UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Criptografia: história, atividades e divulgação científica

Jéssica Shayanne da Paixão

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Jéssica Shayanne da Paixão

Criptografia: história, atividades e divulgação científica

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Rosana Retsos Signorelli Vargas

USP – São Carlos
Outubro de 2020

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

P149c

Paixão, Jéssica Shayanne da
Criptografia: história, atividades e divulgação científica / Jéssica Shayanne da Paixão; orientadora Rosana Retsos Signorelli Vargas. -- São Carlos, 2020.
174 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2020.

1. CRIPTOGRAFIA. 2. DIVULGAÇÃO CIENTÍFICA. 3. DIVULGAÇÃO MATEMÁTICA. 4. ATIVIDADES. I. Vargas, Rosana Retsos Signorelli , orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Jéssica Shayanne da Paixão

Cryptography: history, activities and scientific dissemination

Dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP – in accordance with the requirements of the Professional Master's Program in Mathematics in National Network, for the degree of Master in Science. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Rosana Retsos Signorelli Vargas

USP – São Carlos
October 2020

Dedico este trabalho à minha mãe
Marisa que me ama incondicionalmente,
acredita e confia em mim.

AGRADECIMENTOS

Em primeiro lugar agradeço à minha mãe. Obrigada por seu apoio constante, por acreditar em mim quando eu mesma não acreditava, por me amar mais do que tudo no mundo e sempre ter certeza de me mostrar esse amor. Obrigada pelo seu cuidado, por me levar frutas cortadas só para garantir que eu realmente me alimentaria naqueles dias em que não saía do quarto preparando minhas aulas, estudando ou escrevendo este trabalho. Obrigada por embarcar em cada uma das minhas ideias e ser essa presença constante na minha vida. Sou imensamente grata por ter você! JM sempre.

À Professora Dra. Rosana Retsos Signorelli Vargas por ser, acima de tudo, uma professora humana. Uma professora que entende que a saúde mental do seu estudante é importante e não o pressiona por isso. Obrigada por todas as nossas conversas e discussões, e acima de tudo, por iniciar comigo esse caminho da divulgação científica.

Muito obrigado também a todos os meus professores do PROFMAT. Obrigada por dedicarem seus melhores esforços e seu precioso tempo preparando aulas e se certificando que fizéssemos o nosso melhor. Aprendi algo com cada um de vocês e levarei esse aprendizado para a vida.

Aos meus amigos do PROFMAT que estiveram juntos comigo nessa caminhada. Como foi bom estudar com vocês. Sou grata por nossos almoços divertidos, nossa união organizada e todo conhecimento compartilhado.

Agradeço também aos meus outros amigos que me apoiaram e incentivaram. Obrigada por escutarem as minhas dúvidas e sempre responderem com uma palavra amiga ou um abraço apertado. Cabe aqui um muito obrigado especial à Geisa Ponte que ajudou na minha caminhada pela divulgação científica, tudo poderia ter sido mais difícil sem sua ajuda, serei sempre grata pelo seu acolhimento.

Enfim, ao BTS, meus sete anjos sem asas, vocês não tem ideia de como tocaram a minha história. Obrigada por me ajudarem no momento mais difícil, me ensinar mais sobre gratidão e amor próprio. Essa vitória eu dedico a vocês.

“Se enxerguei mais longe, foi porque
me apoiei sobre os ombros de gigantes.”
(Isaac Newton)

RESUMO

PAIXÃO, J. S. **Criptografia: história, atividades e divulgação científica**. 2020. 174 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

Neste trabalho apresentamos a história da evolução da criptografia desde o período antes da Era Comum até a criptografia RSA, apontando seu importante papel nas duas guerras mundiais e destacando as constantes melhorias nos métodos de cifragem na busca da técnica mais segura. Apresentamos toda a teoria matemática necessária para o entendimento do funcionamento da criptografia RSA passando pelas propriedades dos números inteiros, a divisão nos inteiros, o algoritmo de Euclides, o máximo divisor comum e suas propriedades, os números primos e suas propriedades, o Teorema Fundamental da Aritmética e a congruência. Oferecemos seis propostas de atividades que usam a criptografia como instrumento a fim de contribuir com a contextualização e abstração de certos conteúdos escolares. Usar este tema nas aulas deve estimular a expressão e compreensão do conteúdo. Para finalizar, contamos brevemente a história da divulgação científica no Brasil, explicamos como nos envolvemos com essa área e incluímos nossa contribuição na forma de uma página em uma rede social onde postamos semanalmente textos com conteúdos matemáticos escritos a fim de mostrar a utilidade da matemática bem como aproximar a matéria das discussões da sociedade.

Palavras-chave: Criptografia; Cifra; Divulgação científica; Divulgação matemática.

ABSTRACT

PAIXÃO, J. S. **Cryptography: history, activities and scientific dissemination**. 2020. 174 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

In this paper we present the history of the evolution of cryptography from the period before the Common Era to RSA cryptography, pointing out its important role in the two world wars and highlighting the constant improvements in encryption methods in the search for the most secure technique. We present all the mathematical theory necessary to understand the operation of RSA cryptography through the properties of integers, the division into integers, Euclid's algorithm, the greatest common divisor and its properties, the prime numbers and their properties, the Fundamental Theorem of Arithmetic and congruence. We offer six activity proposals that use cryptography as an instrument in order to contribute to the contextualization and abstraction of certain school content. Using this theme in class should encourage expression and understanding of the content. To conclude, we briefly tell the story of scientific dissemination in Brazil, explain how we get involved in this area and include our contribution in the form of a page on a social network where we post weekly texts with mathematical content written in order to show the usefulness of mathematics as well how to bring the matter closer to society's discussions.

Keywords: Cryptography; Cipher; Scientific dissemination; Mathematics dissemination.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Como professores de matemática, escutamos constantemente a frase “Para que isso serve?” e muitas vezes, nós professores, não conseguimos despertar e instigar a curiosidade matemática do aluno com nossas respostas. O fato de boa parte do ensino ser baseado apenas na reprodução de exercícios pré-determinados empobrece o pensar matemático dos nossos alunos.

Começamos a pensar como poderíamos apresentar a matemática de uma maneira interessante. Da nossa experiência em sala de aula, percebemos que os alunos se sentem mais cativados quando o assunto é tratado também através da parte histórica. Com isso em mente, buscamos dentro da Álgebra, nossa área de estudo, um tema com forte conexão com a história e que estivesse relacionado com a atualidade. Dos temas encontrados, escolhemos a criptografia devido a sua presença em situações cotidianas como transações bancárias, compras *online* e a importância da proteção de nossos dados na rede.

Buscamos referências que contassem a história da criptografia e explicassem a matemática necessária para entendê-la. Em meio a nossas buscas, nos deparamos com a Divulgação Científica, nos interessamos pelo tema, iniciamos nossos estudos na área e aplicamos o que aprendemos criando uma página na internet que falasse de matématica de uma forma menos formal e mais abrangente. Nosso objetivo era “humanizar” a matemática e estimular as pessoas a falarem sobre ela.

Estudamos a história da criptografia e a divulgação científica, porém queríamos oferecer um produto final que incluísse também atividades para a sala de aula, visto que o PROFMAT visa atender professores que buscam aprimoramento em sua formação profissional. Assim surgiram as atividades propostas. Para criá-las, nos apoiamos nos princípios norteadores do Currículo do Estado de São Paulo. Segundo São Paulo (2011, p. 31), devemos ensinar apoiados pelas competências básicas a serem desenvolvidas pelos alunos. Dentro dessas competências, temos três pares complementares que devem nortear a ação educacional, são eles: expressão/compreensão, argumentação/decisão e contextualização/abstração.

O eixo expressão/compreensão é entendido como a capacidade de expressão do eu, por meio das diversas linguagens, e a capacidade de compreensão do outro, que inclui desde a leitura de um texto, de uma tabela, de um gráfico, até a compreensão de fenômenos históricos, sociais, econômicos, naturais.

O eixo argumentação/decisão é entendido como a capacidade de argumentação e análise das informações e relações disponíveis, tendo em vista a viabilização da comunicação, a construção de consensos e a capacidade de elaboração de sínteses de leituras e de argumentações, tendo em vista a tomada de decisões, a proposição e a realização de ações efetivas.

O eixo contextualização/abstração é entendido como a capacidade de contextualização dos conteúdos estudados na escola, e a capacidade de abstração, de consideração de novas perspectivas, de potencialidades para se conceber o que ainda não existe.

Nos dedicamos aos três pares norteadores ao longo deste trabalho, mas concentramo-nos especialmente no par contextualização/abstração. Utilizando o tema criptografia como meio, visamos a introdução e desenvolvimento de determinados conteúdos dos Ensinos Fundamental II e Médio de forma mais significativa.

Segundo Peña (1999), estudar um pouco da história da ciência das comunicações secretas - a criptografia - pode facilitar a percepção de padrões e formação de regras gerais que prenunciam o início da álgebra escolar, por exemplo.

Com essas motivações, nos dedicamos a explorar a história da criptografia contada por Singh (2007) em "O livro dos códigos. A ciência do sigilo - do antigo Egito à criptografia quântica" e Bauer (2013) em "Secret history: the story of cryptology". Norteados pelas histórias contidas em seus livros, buscamos conexões com os conteúdos matemáticos, criamos atividades que podem ser aplicadas em sala de aula e escrevemos textos de divulgação científica que foram publicados em um rede social.

A seguir, explicamos como nosso trabalho está organizado em capítulos.

No Capítulo 2, apresentamos algumas definições, discutimos a diferença entre esteganografia e criptografia, narramos algumas histórias que tiveram seu curso alterado devido a comunicação secreta e analisamos o surgimento da criptoanálise dos árabes, método criado para decifrar uma mensagem codificada. Dedicamos este capítulo aos acontecimentos do período antes da Era Comum (AEC) até o século XIX.

No Capítulo 3, discutimos a papel da criptografia com o surgimento do telégrafo e posteriormente do rádio. Analisamos o processo de quebra da Cifra de Vigenère e entendemos que o desenvolvimento da criptografia no Ocidente foi parte de uma ferramenta valiosa nas duas guerras. Dedicamos este capítulo aos acontecimento do Século XIX até o fim da Segunda Guerra Mundial.

No Capítulo 4, verificamos como a chegada dos computadores programáveis alterou a

forma de se pensar em criptografia. Discutimos o problema das distribuições das chaves e como matemáticos e criptógrafos se dedicaram a resolver essa questão. Dificuldades da criptografia envolveram-se aos conceitos matemáticos e observamos como estas ideias estavam relacionadas. Dedicamos este capítulo aos acontecimentos do período pós Segunda Guerra Mundial.

O Capítulo 5 é dedicado a explicar a teoria necessária para se entender a criptografia RSA. Desta forma, definimos conceitos iniciais, enunciamos e provamos teoremas, corolários e proposições. Dentre os assuntos tratados temos: as propriedades dos números inteiros, a divisão dos números inteiros, o algoritmo de Euclides (incluindo a versão estendida), o máximo divisor comum e suas propriedades, o teorema fundamental da aritmética, a distribuição dos primos, o pequeno teorema de Fermat, congruências e o teorema de Euler.

No Capítulo 6, propomos exercícios para turmas de Ensino Fundamental e Médio usando a criptografia. Oferecemos seis atividades que incluem os seguintes temas: permutação e possibilidades, generalizações e o uso de letras na matemática, análise de frequência, localização de pontos, números primos e fatoração e matrizes. As atividades, em sua maioria, são apresentadas como uma sugestão para uma introdução ao conteúdo, visando instigar a curiosidade e vontade de aprender dos alunos.

O Capítulo 7 surgiu do nosso interesse na divulgação científica. Em 2019 assistimos a palestra "Divulgando ciência: atrair, compartilhar, empolgar" da Luiza Caires (jornalista, mestre em comunicação e editora de Ciências do Jornal da USP) e descobrimos um ambiente que produzia conteúdo para o público em geral, a fim de aproximar a população da universidade e esclarecer a importância das pesquisas. Na palestra conhecemos o perfil de divulgação científica #AstroThreadBR que realiza divulgação científica sobre Astronomia. Entramos em contato com a criadora deste perfil, Geisa Ponte, para conhecer melhor o projeto e ver se seria possível fazer algo semelhante na Matemática. Após este contato inicial que foi bastante frutífero, buscamos materiais sobre o assunto, fizemos um curso online chamado Introdução à Divulgação Científica na Fundação Oswaldo Cruz (Fiocruz) e iniciamos a página #MatThreadBR nas redes sociais. Nosso objetivo é semear a ideia de que a matemática não pertence apenas aos matemáticos e nos propusemos a levar um pouco da matemática para fora dos muros das Instituições de ensino e pesquisa. Esperamos que outros matemáticos sintam-se encorajados a falar sobre matemática de um modo mais acessível, de forma a atrair o público para uma ciência tão linda.

Assim, iniciamos o Capítulo 7 oferecendo uma breve visão do desenvolvimento da divulgação científica no Brasil e, em seguida, apresentamos os textos criados por nós e que foram divulgados nas redes sociais.

Consideramos que o trabalho realizado para fazer as postagens do perfil #MatThreadBR trouxe um resultado diferente de aplicação dos estudos a respeito de números primos e criptografia. Exercitamos um novo olhar sobre estes temas ao pensarmos nos mesmos apresentados em formato de *threads* para a linguagem do *Twitter*.

CAPÍTULO

2

HISTÓRIA DA CRIPTOGRAFIA ATÉ O SÉCULO XIX

Neste capítulo traremos algumas definições que julgamos importante quando se estuda a criptografia. Iniciaremos também uma investigação de fatos cronológicos que antecedem o século XIX, procurando entender quando e como foram utilizados recursos da criptografia para o envio de mensagens secretas e o resultado dessas ações. A parte histórica desse trabalho foi inspirada na leitura do livro 'O livro dos códigos' do autor Simon Singh; assim, as histórias descritas neste e nos dois próximos capítulos terão esta obra como referência.

É conveniente lembrar que enquanto na antiguidade a técnica da criptografia era utilizada para confundir inimigos e transmitir mensagens de forma segura, nos dias de hoje a criptografia é utilizada em compras feitas pela internet, transações bancárias e até em aplicativos de troca de mensagens instantâneas.

2.1 A criptografia antes da Era Comum

Um dos usos mais antigos das 'mensagens ocultas' data de cerca de 2500 anos atrás. Segundo Singh (2007), um dos primeiros relatos desse tipo de mensagem foi feito por Heródoto, um grande historiador, onde ele narra o embate entre Pérsia e Grécia ocorrido no século V AEC.

Naquele tempo, Xerxes, o líder dos persas, enquanto construía a nova capital de seu reino, recebeu presentes de todas as regiões do império, exceto de Atenas e Esparta. Não satisfeito com a hostilidade das cidades-estado, o líder passou metade de uma década planejando um ataque a elas para expandir seu império.

No entanto, seus arranjos de ataque foram vistos por Demarato, um grego exilado na Pérsia. Diante de suas descobertas e de sua fidelidade à pátria, o expatriado resolveu enviar uma mensagem à Esparta para avisar do ataque premeditado. Para isso, ele precisava que seu aviso

não fosse detido pelos guardas. Sua ideia foi ocultar o texto em um par de tabuletas de madeira da seguinte forma: primeiro ele raspou a cera da madeira, em seguida, escreveu a mensagem, e para ocultá-la, ele aplicou novamente a cera na tabuleta. Desta forma, seu aviso passou pelos guardas, que não suspeitaram das tabuletas, chegou ao seu destino e, depois de revelado, ajudou os gregos a se prepararem.

Sem saber que tinha sido descoberto, Xerxes, Rei dos Reis, atacou a Grécia, que cautelosa tinha se preparado com uma armadilha, dizimando os navios persas.

Em seu livro "Histórias" Heródoto narra outro momento em que o envio de uma mensagem camuflada garantiu a entrega de uma informação sem que houvesse desconfiança por parte dos guardas. Segundo ele, a mensagem foi escrita na cabeça de um homem que teve seu cabelo raspado. Depois que o cabelo cresceu, o homem foi enviado ao seu destino e chegando lá, raspou novamente seus cabelos e mostrou o segredo ao seu recebedor.

"A comunicação secreta, quando é obtida através da ocultação da mensagem, é conhecida como *esteganografia*, nome derivado das palavras gregas *steganos*, que significa coberto e *graphein*, que significa escrever." (SINGH, 2007, p. 21, grifo nosso)

Essa técnica foi amplamente usada e tem uma desvantagem clara: se descoberta, a mensagem será revelada de imediato. A fim de reduzir essa desvantagem, o estudo da criptografia foi expandido.

> O estudo da codificação e decodificação de mensagens secretas é denominado **criptografia**. [...] Na linguagem da criptografia, os códigos são denominados **cifras**, as mensagens não codificadas são **textos comuns** e as mensagens codificadas são **textos cifrados** ou **criptogramas**. O processo de converter um texto comum em cifrado é chamado **cifrar** ou **criptografar** e o processo inverso de converter um texto cifrado em comum é chamado **decifrar**. (ANTON; RORRES, 2001, p. 466, grifo nosso)

A esteganografia e a criptografia são ciências diferentes, mas podem ser combinadas a fim de se obter um melhor resultado; um texto codificado e de alguma forma oculto. Um exemplo desta combinação é o microponto, uma técnica que consiste em diminuir a página de algum documento até reduzi-lo a um tamanho inferior a 1 mm de diâmetro e enviá-lo através de uma carta. Quando a técnica foi descoberta e as cartas examinadas, os emissores passaram a cifrar as mensagens a fim de aumentar a segurança; assim, mesmo que o microponto fosse descoberto, a mensagem precisaria ser decifrada.

A criptografia pode ser dividida em dois ramos: transposição e substituição.

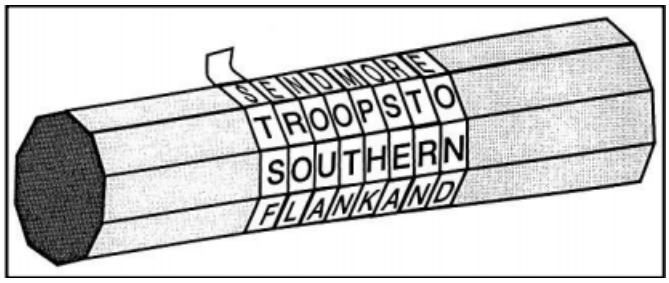
Na criptografia de transposição, as letras são permutadas como num anagrama. Se não houver um sistema de comunicação pré-definido entre emissor e receptor, a criptografia por transposição poderá ser desvantajosa caso o tamanho da palavra seja pequeno, pois há poucas

possibilidades de rearranjo, possibilitando assim que o texto seja decifrado facilmente. Já, se a mensagem for longa, haverá tantas chances de rearranjo que não há tempo no universo para se esgotar todas as possibilidades, logo, o texto se torna indecifrável.

No caso de haver um sistema pré-definido, quem receber a mensagem só precisa desfazer o que foi feito pelo emissor.

Um exemplo do uso da criptografia de transposição é a cítala (bastão) espartana (Figura 1), considerada um dos primeiros aparelhos criptográficos. Na época, para ser usada, tanto o emissor quanto o receptor precisavam dispor de um bastão com dimensões exatamente iguais. Para codificar a mensagem, utilizava-se uma tira de pergaminho ou pedaço de cinto de couro que devia ser enrolado ao longo do bastão e, em seguida, escrevia-se a mensagem ou instrução ao longo do comprimento do objeto. Depois de desenrolado, o assunto do texto não era compreensível. Para desvendar a mensagem, era necessário enrolá-la em um bastão idêntico ao do emissor.

Figura 1 – Cítala espartana



Fonte: Singh (2007, p. 24)

No caso da criptografia de substituição, como o nome indica, cada letra do texto comum é substituída por uma letra diferente. O primeiro documento a utilizar a criptografia de substituição data do primeiro século antes da Era Comum e aparece em *Guerras da Gália* de Júlio César. Segundo este documento, o governante escreveu uma carta trocando as letras do alfabeto romano por letras gregas. Outra mudança utilizada pelo líder consistia na substituição de cada letra do alfabeto por outra que estivesse três posições adiante. Esse método é conhecido como Cifra de César.

Uma forma diferente de rearranjar o alfabeto cifrado seria a escolha de uma palavra-chave ou frase-chave. Desta forma, iniciaríamos o alfabeto cifrado com as letras da palavra/frase-chave, excluindo-se repetições, e depois, seguiríamos a ordem do alfabeto normal com as letras que restaram. Por exemplo, suponha que a palavra-chave escolhida fosse COMANDANTE VALDEZ. Primeiro eliminaríamos as letras repetidas obtendo COMANDTEVLZ. Em seguida, acrescentaríamos o restante das letras do alfabeto na ordem em que aparecem. O resultado é apresentado no Quadro 1.

Os textos cifrados por substituição eram considerados tão confiáveis, que durante anos imaginou-se que eles eram indecifráveis.

Quadro 1 – Exemplo da Cifra de César

Alfabeto normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	**C**	**O**	**M**	**A**	**N**	**D**	**T**	**E**	**V**	**L**	**Z**	B	F	G	H	I	J	K	P	Q	R	S	U	W	X	Y

Fonte: Elaborada pelo autor.

2.2 A criptografia até o século XIX

Foi apenas por volta do século IX que os árabes, que não receberam grande destaque na história da criptografia, mostraram que era possível quebrar as cifras. Eles são considerados os inventores da ciência que permite decifrar uma cifra sem a chave, a criptoanálise. Pessoas que se dedicam a descobrir o conteúdo de um texto cifrado e/ou o método utilizado para cifrar o texto são chamadas criptoanalistas.

Foi através do estudo de várias temáticas, incluindo matemática, estatística e linguística que os árabes, através do entendimento da frequência relativa com que aparecem as letras decifraram as cifras de substituição.

Esse estudo mostra que se conhecermos o idioma a qual o texto cifrado pertence, haverá diversos padrões da língua como as letras que mais aparecem, quais os encontros consonantais mais frequentes, quais letras nunca podem vir seguidas de outras, entre várias outras condições que se manterão após o texto ser criptografado.

Se o texto for pequeno, pode ser mais difícil fazer essas relações, mas com um texto suficientemente grande, a quebra do código pode ser feita dessa maneira.

A criptografia se desenvolveu um pouco mais tarde no Ocidente. O primeiro livro que menciona a criptografia aparece apenas no século XIII, na Europa. No século seguinte, o uso dessa ferramenta estava mais difundido, pois cientistas e alquimistas a usavam a fim de manter suas descobertas em sigilo. No século XV foi usada para fins políticos, uma vez que fornecia uma comunicação secreta. Nessa mesma época, desenvolveu-se a criptoanálise ocidental com o uso da análise de frequência, que não se sabe se foi descoberta de forma independente ou se foi fruto dos estudos árabes, que nessa época já estavam mais difundidos.

A batalha entre criptógrafos e criptoanalistas se iniciava. Quem ainda não dominava a arte de decifrar continuava a confiar cegamente nas cifras de substituição, enquanto aqueles mais avançados no estudo da criptoanálise, já sabiam que esse tipo de cifra não era completamente seguro.

Como a análise de frequência se baseava nos padrões da língua materna, uma forma simples de dificultar a quebra do código era acrescentar os nulos, símbolos que não significavam nada, mas que atrapalhariam na contagem e análise das letras.

> Podemos substituir cada letra por um número entre 1 e 99, o que deixa como sobra 73 números que não representam nada. Estes podem ser espalhados ao acaso por meio do texto cifrado, em variadas frequências. Os nulos não representariam nenhum problema para o receptor da mensagem, que saberia que deveriam ser ignorados. (SINGH, 2007, p. 46)

Em conjunto com os nulos, usar grafia errada sem perda de significado também era uma possível solução, visto que haveria uma quebra nas frequências já conhecidas. Ao invés de escrever CASA, o autor da mensagem poderia escrever a palavra com Z, sem perda de significado, mas alterando a frequência esperada das letras.

É em meio a essa época, em 1586, que por causa da quebra de códigos, Maria, a Rainha da Escócia, foi executada. A história conta que ela foi julgada por traição à rainha da Inglaterra e as provas contra ela foram obtidas através da criptoanálise das cartas que ela enviava e recebia de outros conspiradores. Estes, por acreditarem que sua escrita cifrada era indecifrável, cometeram o erro de colocarem todas as suas informações, incluindo estratégia e o nome dos cavalheiros na correspondência. Às vezes, nenhuma cifra é melhor do que uma cifra fraca; pois esta passa uma falsa sensação de segurança.

O uso da análise de frequência relativa das letras tornou a criptografia de substituição, uma codificação fraca. Os criptógrafos então trabalharam em novas formas de encriptar suas mensagens.

No final do século XVI, é proposto o uso de dois ou mais alfabetos cifrados (Quadro 2), usados alternadamente, para confundir aqueles que tentassem desvendá-lo. A criação desse método é atribuída a Leon Battista Alberti.

Quadro 2 – Exemplo dos dois alfabetos cifrados de Alberti

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado 1	F	Z	B	V	K	I	X	A	Y	M	E	P	L	S	D	H	J	O	R	G	N	Q	C	U	T	W
Alfabeto cifrado 2	G	O	X	B	F	W	T	H	Q	I	L	A	P	Z	J	D	E	S	V	Y	C	R	K	U	H	N

Fonte: Singh (2007, p. 64).

Se quiséssemos, por exemplo, enviar a palavra PROFMAT, procederíamos da seguinte maneira: a primeira letra P seria cifrada usando o alfabeto 1, logo P seria substituída por H, a segunda letra seria cifrada usando o alfabeto 2, logo R seria substituída por S, a terceira letra seria cifrada usando o alfabeto 1, logo O seria substituída por D e assim por diante. Assim, PROFMAT seria escrito como HSDWLGG. A vantagem encontra-se no fato de uma mesma letra cifrada representar letras diferentes no alfabeto original, foi o que aconteceu no exemplo; a letra G representa tanto o A quanto o T. O inverso também ocorre, ou seja, a letra do alfabeto original também é representada por duas letras diferentes no alfabeto cifrado.

É apenas muitos anos mais tarde que a ideia de Alberti é aperfeiçoada por um diplomata francês, Blaise de Vigenère. Sua cifra consiste em não apenas dois alfabetos cifrados, mas vinte e seis deles; o chamado Quadrado de Vigenère (Quadro 4). Para usá-lo é necessário o uso de uma palavra-chave pré-determinada entre emissor e receptor. Para exemplificar, vamos utilizar a palavra-chave PROFMAT e com ele codificar a frase 'hoje vou à faculdade' (Quadro 3).

Primeiro, a palavra chave deve ser escrita acima da mensagem:

Quadro 3 – Exemplo da cifra de Vigenère

Palavra-chave	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R	O
Mensagem original	h	o	j	e	v	o	u	a	f	a	c	u	l	d	a	d	e

Fonte: Elaborada pelo autor.

Quadro 4 – O quadrado de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2007, p. 66).

O texto cifrado será criado assim: para cifrar a primeira letra, H, identificamos a letra da palavra-chave que está acima, no caso, P, que por sua vez, indica uma linha no Quadrado de

Vigenère (linha 15) e é seguindo essa linha que cifraremos a primeira letra, obtendo W; para cifrar a segunda letra, O, identificamos a letra da palavra-chave que está acima, no caso, R, que por sua vez, indica uma linha no Quadrado de Vigenère (linha 17) e é seguindo essa linha que cifraremos a segunda letra, obtendo F; seguiremos fazendo este processo até que terminemos a mensagem e teremos como resultado a mensagem do Quadro 5.

Quadro 5 – Exemplo da cifra de Vigenère – mensagem cifrada

Palavra-chave	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R	O
Mensagem original	h	o	j	e	v	o	u	a	f	a	c	u	l	d	a	d	e
Mensagem cifrada	W	F	X	J	H	O	N	P	W	O	H	G	I	W	P	U	S

Fonte: Elaborada pelo autor.

A Cifra de Vigenère oferece duas grandes vantagens, primeiramente é imune à análise de frequência que era a grande ferramenta da criptoanálise, e depois, oferecia inúmeras chaves para emissor e remetente, visto que qualquer palavra poderia ser usada como palavra-chave, e, tentar todas as possibilidades possíveis seria inviável, uma vez que o número é grande demais.

Embora o Quadrado de Vigenère oferecesse um alto nível de segurança, seu uso só se deu cerca de dois séculos mais tarde devido a sua complexidade e ao esforço necessário para cifrar e decifrar.

No século XVII, os criptógrafos tentavam encontrar uma cifra intermediária; algo mais forte do que a cifra de substituição monoalfabética (que poderia ser decifrada com a análise de frequência) e mais simples do que a cifra polialfabética (que era demasiadamente complicada).

Dentre as cifras que surgiram havia a cifra de substituição homofônica. Com seu uso, pretendia-se eliminar a decodificação através da análise de frequência; para isso, cada letra deveria ser substituída por um conjunto de números aleatórios; o número de elementos em cada conjunto seria determinado pela frequência relativa daquela letra. Se uma letra tem 7% de chance de aparecer num texto, ela deveria ter um conjunto numérico com sete números aleatórios para representá-la. Com esse artifício, se algum criptógrafo fizesse a análise de frequência de cada elemento do texto, chegaria a cerca de 1% para qualquer um deles. Isso não representa o fracasso total da ferramenta de decodificação. Na verdade, como já foi discutido anteriormente, cada língua tem suas peculiaridades e seus padrões; então, se alguém versado nas generalizações da língua estudasse com afinco essa cifra, poderia perceber essas normas, fazer algumas suposições, substituições e poderia chegar à mensagem original.

Outro exemplo de cifra intermediária é a Grande Cifra de Luís XIV, usada pelo rei para codificar suas mensagens e maquinações políticas. A cifra foi inventada pela equipe francesa de pai e filho Antoine e Bonaventure Rossignol. Ambos eram muito eficientes na quebra de códigos

e, por isso, conseguiram criar uma cifra forte que foi estudada por criptoanalistas durante muitos anos. Essa cifra caiu em desuso depois da morte de pai e filho e, logo, detalhes de seu uso foram perdidos, restando apenas os documentos criptografados. Foi apenas no final do século XIX que Victor Gendron, um historiador militar, descobriu uma série nova de cartas escritas com a Grande Cifra. Entregou-as para Étienne Bazeries, um especialista do Departamento Criptográfico francês e este passou os três anos seguintes de sua vida se dedicando a decifrá-las.

As cartas continham milhares de números, mas apenas 587 deles eram diferentes. Bazeries tentou analisar a frequência dos números mais frequentes e depois de muitas tentativas falhas chegou à conclusão de que cada número deveria representar uma sílaba. Acabou descobrindo que o conjunto de números (124-22-125-46-345) que aparecia com frequência significava *'les-en-ne-mi-s'* (os inimigos, em francês), substituiu essas sílabas onde pode e deduziu o significado de outras. À medida que descobria outras relações entre números e sílabas fazia novamente uma substituição com o que já era conhecido e continuava seu trabalho. Passados os três anos, o criptoanalista tinha decifrado todas as cartas de Luís XIV.

Após a leitura de todas as cartas decifradas, a descoberta que mais chamou a atenção dos historiadores foi uma carta que contava a verdadeira identidade do Homem da Máscara de Ferro. Sua identidade sempre foi motivo de alvoroço. O homem foi aprisionado e muitos acreditavam que ele seria algum parente do rei, a teoria mais conspiratória contava que ele era irmão gêmeo de Luís XIV e que fora condenado à prisão para que nunca houvesse dúvidas quanto ao verdadeiro dono do trono. Depois que a carta foi decifrada, descobriu-se que, na verdade, o Homem da Máscara de Ferro tratava-se de Vivien de Bulonde, um comandante que liderava um ataque a uma cidade que fazia fronteira com a França que não manteve sua posição, embora tenha recebido ordens. Preocupado com a chegada de tropas inimigas, o comandante abandonou o posto e deixou para trás suas armas e seus soldados feridos. Por conta disso, foi condenado a prisão e só poderia caminhar durante o dia usando uma máscara de ferro. Mesmo com a decodificação da carta, ainda há muitos que acreditam na história do irmão gêmeo de Luís XIV e afirmam que a carta é uma pista falsa inventada pelo rei.

O século XVIII foi dedicado à decifração de cifras. As potências europeias tinham as chamadas Câmaras Negras, lugares dedicados à decifração de mensagens e reunião de informações, sendo que a mais famosa ficava em Viena. Conta-se a história de que todas as cartas que chegavam na capital destinadas a embaixada eram copiadas e só depois enviadas. As cópias eram entregues aos criptoanalistas para que estes descobrissem o teor das mensagens. Mensagens importantes eram passadas aos imperadores da Áustria que faziam uso próprio das informações ou as vendiam para outros grandes países europeus.

É esse trabalho mais profissional dos criptoanalistas que forçam os criptógrafos a abandonar a cifra de substituição monoalfabética e começar a usar o Quadrado de Vigenère que tinha sido desenvolvido dois séculos antes. O principal objetivo do reforço da proteção das mensagens foi a necessidade de preservar o conteúdo dos telegramas que passaram a ser enviados com o

desenvolvimento do telégrafo. Mas isso será abordado no próximo capítulo.

CAPÍTULO

3

HISTÓRIA DA CRIPTOGRAFIA NO SÉCULO XIX E 2ª GUERRA

3.1 Século XIX

> Embora o telégrafo, junto com a revolução das telecomunicações, tenha surgido no século XIX, suas origens podem ser traçadas até 1753. Uma carta anônima, em uma revista escocesa, descreve como uma mensagem poderia ser enviada, por grandes distâncias, conectando-se 26 cabos entre o emissor e o receptor. Um cabo para cada letra do alfabeto. O emissor então poderia soletrar a mensagem enviando pulsos de eletricidade através de cada cabo. [...] O receptor de algum modo perceberia a corrente elétrica emergido de cada fio e então leria a mensagem. (SINGH, 2007, p. 78)

Mesmo que estivesse descrito na carta ainda no século XVIII, tal objeto só foi construído depois do desenvolvimento de um sistema sensível para captar os pulsos de eletricidade. Por volta de 1839, na Europa, tal aparelho já conseguia enviar mensagens com uma distância de 29 quilômetros e foi altamente elogiado pelo aumento da velocidade na comunicação, desde o anúncio de nascimentos de príncipes até o apoio na prisão de um assassino.

Na América, o responsável pela primeira linha telegráfica foi Samuel Morse. Seu aparelho tinha capacidade de transmitir uma mensagem com cerca de 60 quilômetros de alcance. Ao usar um eletromagneto, ele ampliou o sinal, que chegando ao receptor ainda era forte o suficiente para fazer marcas curtas no papel: pontos e traços. Foi ele também quem desenvolveu o código Morse, que consistia em pontos e traços que representavam as letras do alfabeto (Quadro 6) e o receptor acústico, responsável por emitir *bips* audíveis. Seu telégrafo e código tornaram-se tão populares que passaram a ser utilizados também na Europa. O aparelho ajudou na prisão de criminosos, na divulgação de notícias e até em transações entre empresas distantes.

Quadro 6 – Código Morse internacional

Símbolo	Código	Símbolo	Código
A	·–	W	·––
B	–···	X	–··–
C	–·–·	Y	–·––
D	–··	Z	––··
E	·	1	·————
F	··–·	2	··———
G	––·	3	···––
H	····	4	····–
I	··	5	·····
J	·–––	6	–····
K	–·–	7	––···
L	·–··	8	–––··
M	––	9	––––·
N	–·	0	–––––
O	–––	ponto final	·–·–·–
P	·––·	vírgula	––··––
Q	––·–	ponto de interrogação	··––··
R	·–·	dois pontos	–––···
S	···	ponto e vírgula	–·–·–·
T	–	hífen	–····–
U	··–	barra	–··–·
V	···–	aspas	·–··–·

Fonte: Singh (2007, p. 24).

Mas, como citado no fim do capítulo anterior, com o avanço das mensagens sendo enviadas pelo telégrafo, houve também a necessidade de reforçar a proteção do conteúdo da mensagem. O código Morse não é uma forma de criptografia, os pontos e traços são apenas formas de se representar as letras para a transmissão telegráfica, ou seja, quando alguém decidia enviar uma mensagem, precisava entregar o texto para um especialista em código Morse que, obviamente, leria a nota para transmiti-la. Assim, havia o risco de que esses trabalhadores pudessem ser subornados para passar informações.

A solução encontrada foi cifrar a mensagem antes de entregá-la ao telegrafista e esta opção era boa por dois aspectos: o telegrafista não mais saberia o conteúdo da mensagem e possíveis escutas colocadas no telégrafo não seriam úteis. A melhor alternativa para codificar os telegramas era a Cifra de Vigènere, pois era considerada indecifrável.

É nesse cenário que, ainda no século XIX, surge Charles Babbage, conhecido por ter

desenvolvido o precursor dos computadores modernos. Babbage se interessava por muitas áreas distintas, mas no que concerne a matemática, foi ele quem projetou o "Motor de subtração nº 1" e esboçou o "Motor de subtração nº 2".

O primeiro projeto consistia numa máquina com 25 mil peças de precisão que serviria para fazer cálculos com alto grau de exatidão. O objetivo do britânico era retificar um conjunto de tabelas usadas em alto mar que, devido ao grande número de erros, levava a naufrágios e desastres. Ele recebeu financiamento do governo, mas, mesmo depois de dez anos, não tinha terminado a máquina. Decidiu então abandonar o projeto e dedicar-se ao "Motor de subtração nº 2".

Ao abandonar o primeiro projeto, Babbage perdeu a confiança do governo e também o apoio financeiro, inviabilizando assim a construção do "Motor de subtração nº 2". Se tivesse sido construído, a segunda máquina teria a característica única de ser programável, dependendo das instruções que recebesse. Essa máquina era um esboço dos computadores modernos possuindo memória (chamada de depósito), um processador (triturador) e comandos semelhantes ao SE... ENTÃO... REPITA (usados na computação moderna).

Como não obteve sucesso com a construção das máquinas, dedicou-se a quebra da Cifra de Vigenère, o que fez com sucesso. Para a criptoanálise, esse foi o maior passo dado pela área desde a descoberta da análise de frequência pelos árabes dez séculos antes.

Talvez seja interessante relembrarmos que a Cifra de Vigenère se apoiava em 26 diferentes alfabetos cifrados para criar a mensagem codificada e o uso de uma palavra-chave qualquer, conhecida apenas pelo emissor e receptor da mensagem. Para desvendar a cifra, Babbage apoiou-se na repetição. Inferiu que através da repetição de certos padrões de letras conseguiria descobrir o comprimento da palavra-chave, uma vez que a distância entre palavras iguais devem ocorrer em múltiplos do número de letras da palavra-chave. Analisou então as sequências repetidas, os espaços entre essas sequências e determinou os fatores (tamanhos possíveis de chave) para cada sequência. Ao encontrar um fator comum, descobriu o tamanho da chave.

Sabendo-se o tamanho n da palavra-chave, o texto fica automaticamente dividido em n-partes e cada uma dessas partes foi cifrada usando a palavra-chave que podemos chamar de $L_1L_2L_3 \ldots L_n$, onde cada L_n equivale a uma linha do Quadrado de Vigenère.

Quando analisamos cada um dos L_n's, a *Cifra Indecifrável* torna-se uma cifra monoalfabética e, para este tipo de cifra, aplica-se a análise de repetição de frequências e descobre-se o padrão. Fazendo isso para cada L_n, Babbage determinou com qual letra o alfabeto cifrado se iniciava e com isso desvendou a cifra antes considerada indecifrável.

Acredita-se que a Cifra de Vigenère foi decodificada por Babbage em 1854, mas como esta descoberta não foi publicada, apenas no século XX, quando estudiosos revisaram suas anotações, isto foi revelado. Em 1863, a cifra foi decodificada por Friedrich Wilhelm Kasiski, de forma independente, que publicou suas descobertas em um livro. A técnica para quebrar o código

de Vigenère leva seu nome: Teste de Kasiski. O nome de Babbage comumente é ignorado.

Considera-se que Babbage não tenha publicado sua descoberta devido a sua displicência, uma vez que era conhecido por não terminar projetos ou publicar descobertas; ou ainda, em consequência ao seu possível trabalho com a espionagem britânica, que teria exigido dele segredo absoluto e dado ao seu país uma vantagem de nove anos sobre o mundo.

Descoberta a quebra de código da Cifra de Vigenère, os criptógrafos empenharam-se em criar um novo tipo de cifra que lhes trouxesse segurança, porém, nenhum código apresentou o resultado esperado e assim se seguiu até a segunda metade do século XIX.

Em contrapartida, o interesse do grande público pela criptografia cresceu, principalmente devido à popularização do telégrafo. Pessoas em geral passaram a criar seus próprios tipos de cifras e comunicavam-se, inclusive, através de jornais; jovens casais apaixonados planejando fugas, criptógrafos publicando textos cifrados para desafiar os colegas, entre outros ...

Autores da época inspirados pela criptografia incluíram o tema em seus livros; Júlio Verne em *Viagem ao centro da Terra*, Sir Arthur Conan Doyle em suas histórias sobre o detetive Sherlock Holmes e Edgar Allan Poe considerado por seus leitores "o mais profundo e habilidoso criptógrafo que já vivera"; com seu conto sobre cifras chamado *O escaravelho de ouro*.

No final do século XIX, Guglielmo Marconi, atraído por circuitos elétricos descobriu que "sob certas condições, se um circuito é percorrido por uma corrente elétrica, pode induzir uma corrente em outro circuito isolado, a uma distância do primeiro" (SINGH, 2007, p. 119). Desenvolvendo esta ideia e acrescentando antenas ele criou o rádio, que possuía uma clara vantagem em relação ao telégrafo, não precisava de fios.

3.2 Século XX

O rádio inventado por Marconi atraiu a atenção dos militares, desejosos de coordenarem suas frotas, saberem a localização de seus navios e de terem contato com seus batalhões. Porém, a maior vantagem do rádio era também sua maior fragilidade, uma vez que as ondas emanavam em todas as direções e alcançavam os receptores onde quer que estivessem, não havia como controlar quem receberia as informações passadas através do instrumento, logo, o inimigo seria capaz de interceptar todas as mensagens enviadas. Por esse motivo, era essencial que os informes fossem criptografados.

Essa necessidade aumentou com a chegada da Primeira Guerra Mundial. Criptógrafos esforçaram-se em criar novos tipos de criptografia, mas não obtiveram sucesso; todas foram decifradas.

A cifra mais conhecida dessa época é a ADFGVX usada pelos alemães em 1918. Os criptógrafos da Alemanha julgaram tal cifra como a mais segura e a usaram para transmitir informações de ataque.

Imaginava-se que a cifra ADFGVX ofereceria proteção uma vez que era uma mistura da criptografia de substituição e de transposição.

De modo geral, tal cifra era obtida através de uma matriz de dimensão 6 x 6 com 36 caracteres distintos (26 letras do alfabeto e 10 dígitos de 0 a 9, dispostos de forma aleatória). As linhas e colunas eram nomeadas pelas letras A, D, F, G, V e X e cada letra da mensagem seria substituída de acordo com sua coordenada na grade, obedecendo à ordem do par ordenado (linha, coluna). Veja um exemplo no Quadro 7.

Quadro 7 – Exemplo de matriz para a cifra ADFGVX

\	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

Fonte: Elaborada pelo autor.

Vejamos como a cifra funciona em um exemplo (Quadro 8). Consideremos a seguinte mensagem: **dia 9 vou ao mercado**.

Quadro 8 – Frase-exemplo para a cifra ADFGVX

Mensagem	dia 9 vou ao mercado															
Texto original	d	i	a	9	v	o	u	a	o	m	e	r	c	a	d	o
1ª criptografia	AG	VG	DV	XA	VF	DG	GD	DV	DG	GX	XD	VV	FG	DV	AG	DG

Fonte: Elaborada pelo autor.

A mensagem que obtivemos foi cifrada usando substituição. Para terminarmos o processo vamos cifrar novamente este texto, desta vez, usando uma cifra de transposição. Para isso precisamos de uma palavra-chave (que precisa ser do conhecimento do destinatário), usaremos **PROF**.

Fazemos a transposição da seguinte forma: escrevemos as letras da palavra-chave no topo de uma nova matriz; em seguida, escrevemos o texto já cifrado de forma a preencher as linhas

da matriz, uma a uma, até que não haja mais letras do texto cifrado; por fim, reorganizamos as colunas da matriz de forma que fiquem escritas em ordem alfabética (Quadro 9).

Quadro 9 – Frase final cifrada com a cifra ADFGVX

P	R	O	F
A	G	V	G
D	V	X	A
V	F	D	G
G	D	D	V
D	G	G	X
X	D	V	V
F	G	D	V
A	G	D	G

F	O	P	R
G	V	A	G
A	X	D	V
G	D	V	F
V	D	G	D
X	G	D	G
V	V	X	D
V	D	F	G
G	D	A	G

Fonte: Elaborada pelo autor.

O texto final é obtido seguindo-se cada coluna e escrevendo as letras nessa nova ordem. No caso do exemplo o texto final ficaria: GAGVXVVGVXDDGVDDADVGDXFAGVFDGDGG.

Seria esse o texto transmitido em código Morse, e caberia ao receptor reverter o processo de cifragem para obter a mensagem original.

Prestes a invadir Paris, os alemães enviaram uma mensagem codificada com a cifra ADFGVX pedindo o envio de munições para uma região ao norte da capital. Os alemães não esperavam que o criptoanalista francês Georges Painvin conseguiria decifrar, depois de muito esforço, a mensagem por eles enviada e descobrir o local da invasão, ajudando seu país a reforçar aquela região específica com soldados aliados. Sem o elemento surpresa, os alemães foram obrigados a recuar em uma batalha horrenda que durou cinco dias.

Durante a guerra, o volume de mensagens interceptadas que deveriam ser decifradas aumentou consideravelmente, o que aumentou o trabalho dos criptoanalistas. Dados indicam que apenas os franceses interceptaram cerca de 100 milhões de palavras alemãs naquele período. Porém, o que realmente mudou o rumo da Primeira Guerra Mundial foi a decodificação do telegrama escrito por Zimmermann, ministro das Relações Exteriores alemão.

Até aquele momento, 1916, os Estados Unidos demonstravam neutralidade, tinham esperança de que um acordo seria firmado e esperavam atuar apenas como mediadores. Sua crença no acordo devia-se, especialmente, pela nomeação de Arthur Zimmermann como ministro das Relações Exteriores, que parecia inclinado à diplomacia ao invés da guerra. Eles não poderiam estar mais enganados.

No início de 1917, o ministro enviou um telegrama cifrado para seu embaixador em Washington e, segundo instruções, a mensagem devia ser transmitida também ao embaixador

alemão no México. No telegrama ele propunha um acordo com o presidente mexicano. Para evitar a entrada dos Estados Unidos na guerra, a Alemanha financiaria um ataque do México aos Estados Unidos a fim de reaver estados como o Texas, Novo México e Arizona. Em contrapartida, esperava que o presidente mexicano convidasse o Japão a atacar também o país norte-americano. Zimmermann acreditava que se os Estados Unidos estivessem bastante ocupados com conflitos internos, não tomariam partido da guerra que se desenvolvia naquele momento, por isso iniciariam um ataque total com seus submarinos e forçariam a Inglaterra a assinar o tratado de paz.

Entretanto, Zimmermann não contava que seu telegrama seria interceptado e decifrado pelos ingleses. Estes, com medo de revelar que sabiam decifrar os códigos alemães e perderem sua fonte de informações, decidiram não divulgar o conteúdo do telegrama. Eles confiavam que os Estados Unidos entrariam na guerra após os ataques com submarinos à Inglaterra.

O ataque aconteceu, porém o país norte americano decidiu que continuaria neutro. Assim, os britânicos orquestraram um plano a fim de revelar o telegrama sem mostrar seu envolvimento. Conseguiram uma cópia do telegrama que o embaixador situado em Washington enviou para o embaixador que estava no México e enviaram esta versão decodificada para o presidente americano. Diante do conhecimento do teor desta mensagem o presidente americano não viu alternativa a não ser entrar na guerra.

A entrada dos Estados Unidos alterou a liderança da força para o lado de seus aliados, grupo ao qual a Inglaterra pertencia, e foram eles que acabaram vencendo o conflito.

No tempo posterior a Primeira Guerra, os criptógrafos continuaram a procurar cifras que não pudessem ser decifradas. Pensaram em fortificar a Cifra de Vigenère e revisaram seu ponto fraco: a palavra-chave. Já havia ficado claro com o Teste de Kasiski que a cifra era passível de quebra, uma vez que, descoberta a palavra-chave, a cifra tornava-se cíclica; logo, a fim de consertar essa vulnerabilidade pensaram em tornar a palavra-chave ou frase-chave grande o suficiente, desta forma o Teste de Kasiski não funcionaria.

Inicialmente, pensaram em frases de livros ou até mesmo uma canção, mas, embora a técnica também descoberta por Babbage não funcionasse, ainda era possível decifrar a mensagem, uma vez que a palavra/frase-chave tinha um significado, assim, com alguns testes era possível descobrir alguns segmentos e depois de algumas substituições, descobria-se o conteúdo do texto.

Ainda sem desistir da antes chamada *Cifra Indecifrável*, o diretor da pesquisa criptográfica do exército americano, major Joseph Mauborgne, propôs um modelo de chave aleatória, ela não consistia de palavras com sentido, e sim, de um amontoado de letras escritas de forma aleatória.

O conceito era interessante, produziam-se blocos com centenas de papéis, cada folha com uma chave única formada por letras dispostas ao acaso, imprimiam-se duas cópias, uma para o remente e a outra para o recebedor. Enviava-se a primeira mensagem usando a cifra do primeiro bloco, em seguida, descartava-se tal folha; para a próxima mensagem usava-se a folha

seguinte do bloco e assim por diante. Tal método é conhecido como *bloco de cifras de uma única vez*. Da forma como foi explicada, a cifra tornava-se segura e indecifrável, porém, como milhares de mensagens eram trocadas todos os dias, a ideia não era viável.

Sem outro caminho, os criptógrafos viram-se forçados a abandonar os modelos que já conheciam de cifras, deixar lápis e papel e explorar as novas tecnologias.

3.2.1 Máquinas de Cifragem

O disco de cifras é uma máquina criptográfica inventada por Leon Albertini no século XV. Ela consistia em dois discos de cobre de tamanhos diferentes com o alfabeto escrito neles. Os dois discos eram fixados um no outro através de um eixo, com o disco menor ficando em cima do maior, de modo que fosse possível a rotação. Veja a Figura 2.

Figura 2 – Disco de cifras

Fonte: Singh (2007, p. 144)

Com essa máquina era possível mecanizar a Cifra de César e a Cifra de Vigenère e o aparelho oferecia a vantagem da diminuição de erros humanos no processo da codificação.

No século XX, Scherbius, um inventor alemão, dedicou-se a trabalhar com a tecnologia do século para desenvolver uma máquina que substituísse o uso de papel e lápis, tão necessários na criptografia.

Sua invenção, chamada de *Enigma*, era quase uma versão elétrica da máquina feita por Alberti; composta por três partes principais: um teclado para que se digitasse o texto normal, uma unidade misturadora e um teclado cujas letras podiam ser iluminadas por suas várias lâmpadas que indicava as letras do texto cifrado.

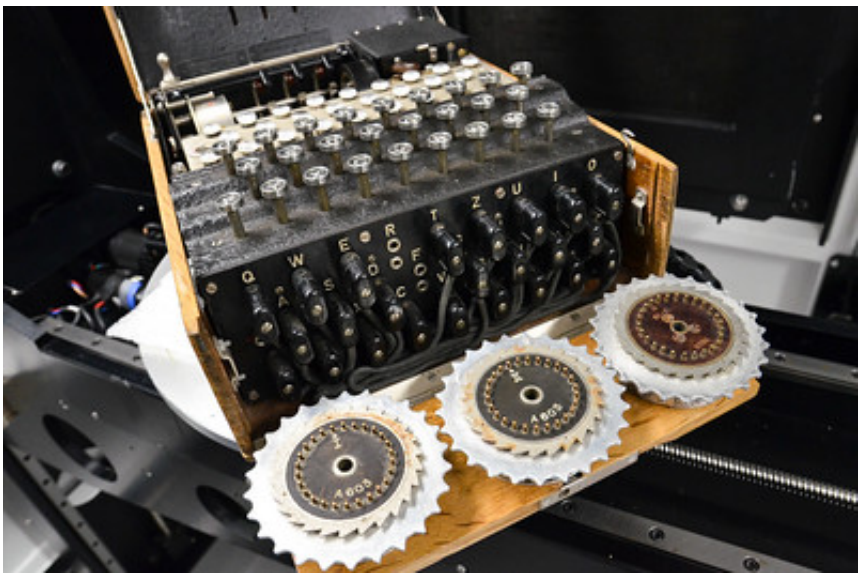
O disco misturador era responsável por traduzir as letras do texto original para o texto codificado e era também a parte mais importante da máquina. A ideia do inventor consistia em um giro de um vinte e seis avos do misturador a cada letra digitada. O problema dessa forma era

que após 26 voltas o disco voltava a sua posição inicial, logo, se o inimigo tivesse acesso a uma das máquinas Enigma, poderia apertar indefinidamente um mesmo botão e depois de 26 vezes o padrão se repetiria; e padrões na criptografia geram cifras inseguras.

Para aumentar a segurança poderia ser adicionada a máquina um segundo misturador, a forma de cifragem seria bastante parecida com a da primeira máquina, sendo que o segundo misturador permaneceria imóvel e só faria sua parte do giro quando o primeiro misturador tivesse completado sua primeira volta completa.

O mecanismo do inventor contava, na verdade, com três misturadores e um refletidor, que permitia desfazer o processo de cifragem usando a própria máquina. Estes três misturadores eram feitos de tal modo que podiam ter seus lugares dentro do engenho alterados e, além disso, havia um painel de tomadas entre o teclado e o primeiro misturador de forma que era possível trocar algumas letras antes delas entrarem no misturador (Figura 3), isso dificultaria o uso da análise de frequências.

Figura 3 – A máquina Enigma



Fonte: Flickr (2018)

Apenas com os três misturadores usando as vinte e seis letras do alfabeto temos $26 \times 26 \times 26 = 17576$ possibilidades de posições iniciais possíveis, e é justamente a posição dos misturadores que determinará a forma como a mensagem será cifrada. Ao colocarmos na conta todos os fatores acima citados teríamos um número acima de 10 quatrilhões de chaves possíveis (são mais de mil bilhões de possibilidades).

As chaves da *Enigma* estavam indicadas em um livro de códigos e uma cópia era dada a todos da comunicação. Cada página indicava as configurações de um dia e serviam tanto para o emissor quanto para o receptor da mensagem, uma vez que para desfazer a cifragem, bastava que o operador fosse digitando a mensagem cifrada na Enigma e o texto decifrado seria iluminado

no painel, tudo isso graças ao uso do refletor.

Em 1918, Scherbius conseguiu sua primeira patente e tentou vender diferentes versões de sua máquina *Enigma* mas o preço alto do equipamento fez com que não fizesse muito sucesso. Encontrou resistência também ao oferecer aos militares, pois estes não acreditavam que precisassem de algo deste tipo; eles ainda não tinham noção do fracasso de sua criptografia, uma vez que não sabiam da verdade sobre o vazamento do telegrama de Zimmermann.

Em outros lugares do mundo, pelo menos outros três inventores criaram algo próximo da *Enigma*, ou seja, um invento que utilizasse misturadores giratórios porém, como aconteceu com Scherbius, suas invenções não tiveram aceitação e portanto suas vendas não prosperaram.

Cerca de 5 anos depois da patente dada a Scherbius, um livro inglês intitulado *A crise mundial* revelou que os britânicos tinham conseguido meios de decifrar as mensagens alemãs durante a Primeira Guerra e que esse fator serviu como grande vantagem para os aliados. Nesse momento, os militares alemães foram convencidos de que precisavam de uma criptografia mais adequada e forte, de forma que não voltassem a cometer os erros da guerra recém-acabada.

Em 1925 iniciou-se a produção em massa de máquinas *Enigma*. Muitos segmentos passaram a utilizá-la, porém o modelo mais completo foi reservado apenas para os militares e governantes. Nos vinte anos seguintes mais de 30 mil máquinas *Enigma* foram compradas pelos militares e o papel que a máquina desempenharia na Segunda Guerra Mundial fez com que alemães dessem como certa a vitória de seu país.

3.2.2 Enigma: impossível de decifrar?

Após a vitória na Primeira Guerra Mundial, Reino Unido, França e Estados Unidos relaxaram em suas áreas de criptoanálise, já que a Alemanha fora derrotada e, na visão deles, não representava ameaça, embora o primeiro país ainda monitorasse as mensagens alemãs.

Para a surpresa deles, em 1926 interceptaram uma mensagem que não conseguiram decifrar, em seguida outra e logo perceberam que não conseguiam decifrar nenhuma das mensagens apanhadas, era a *Enigma* entrando em cena. Depois de várias tentativas de quebrar a nova cifra dos alemães, sentiram-se desestimulados.

Na Alemanha, Hans-Thilo Schmidt, um dos muitos que estava sofrendo no pós-guerra, indignado com as perdas que sofreu em sua família e tendo conseguido um emprego na área das comunicações de seu país, decidiu entregar à França dois documentos que forneciam o modo de usar a *Enigma*.

Embora tivessem a possibilidade de criar uma réplica da máquina, os franceses continuavam com o grande problema de não saber a disposição dos componentes, ou seja, a máquina sem a chave era inútil. Os franceses então compartilharam os documentos alemães com a Polônia, que estava cercada por Rússia e Alemanha e vivia com uma constante ameaça de invasão.

Talvez, guiados pela ameaça, os poloneses debruçaram-se sobre os documentos e iniciaram seu trabalho para desvendá-la. Descobriram que o livro de chaves não fornecia, necessariamente, a chave que seria usada no dia, na verdade ela fornecia uma cifra para a chave do dia, isso aumentava ainda mais a segurança.

Para enfrentar o grande invento, os poloneses tomaram um caminho diferente do que faziam anteriormente. Ao invés de contratar peritos na estrutura da linguagem, pensaram em atacar com mentes científicas e, por isso, convidaram vinte matemáticos fluentes em alemão, já que estudaram em uma universidade polonesa localizada em uma região que antes pertencia à Alemanha.

O mais capaz dentre eles, Marian Rejewski, concentrou todos os seus esforços em desvendar a *Enigma*. Analisou de forma exaustiva a chave da mensagem que era enviada no início do texto, isso porque sabia que a chave utilizada no dia era digitada duas vezes seguidas no início do texto. Por exemplo, se a palavra-chave do livro fosse **JSP** e a mensagem começasse com **MDLPRO** ele saberia que a primeira e a quarta letra representavam a mesma letra, da mesma forma, a segunda e a quinta letra estariam relacionadas e do mesmo modo a terceira e sexta letras.

Isso o levou a uma série de análises, anotações e conclusões; se conseguisse desvendar essa chave diariamente, ele teria vencido a *Enigma*. Depois de conseguir uma réplica do invento e de muito estudo, formulou, ao longo de um ano, um catálogo com todos os ajustes possíveis dos misturadores. Um pouco mais de estudo e descobriu também como funcionava a troca dos fios da máquina, com isso, a *Enigma* tinha sido, finalmente, decifrada e os poloneses usaram isso para manter um olho no que os alemães estavam fazendo.

Mesmo quando os alemães fizeram pequenas alterações na máquina, Rejewski superou as modificações e, ao invés de um novo catálogo, projetou uma versão mecanizada que, de forma automática, revelaria o ajuste dos misturadores. A máquina era composta por seis aparelhos, cada uma representando uma das possíveis disposições dos misturadores.

As boas novas, porém, não duraram muito. Em 1938, a Alemanha passou a contar não mais com três, mas cinco misturadores, que poderiam ser dispostos de qualquer forma segundo o manual. Assim, para que a chave fosse descoberta, os poloneses precisariam de sessenta máquinas de Rejewski. O custo das máquinas ultrapassou até mesmo o orçamento anual do departamento polonês de cifras e, portanto, ficou inviável.

Sem seu mais precioso recurso, a Polônia viu-se incapaz de decifrar as mensagens alemãs. A fim de não deixar sua grande descoberta morrer convidou criptoanalistas franceses e britânicos e entregaram a eles réplicas da *Enigma* e um manual de como reproduzir a máquina polonesa. Apenas duas semanas depois, a Polônia foi invadida pela Alemanha.

3.2.3 A queda da Enigma

Se durante treze anos a máquina *Enigma* foi considerada impossível de decifrar, naquele momento, tendo conhecimento de todos os avanços feitos pelos poloneses, os ingleses tinham agora a certeza de que, embora difícil, a cifra alemã não era perfeita.

A maior lição que tiraram dos poloneses foi a valorosa contribuição que matemáticos e cientistas traziam como decifradores de códigos e por isso passaram a recrutá-los.

Os novos recrutas eram levados para Blentchley Park, na Escola de Cifras e Códigos do Governo em Buckinghamshire. A escola era dividida em várias casas e cada uma tinha sua função: análise das comunicações do exército alemão pela *Enigma*, tradução de mensagens e obtenção de possíveis informações relevantes, especialização na versão naval da *Enigma*, dentre outras.

Em 1939, os cientistas e matemáticos ingleses já tinham dominado as técnicas polonesas e seguiam dia-a-dia a mesma rotina: à meia-noite, os operadores alemães das *Enigmas* mudavam para uma nova chave diária e qualquer avanço feito pelos britânicos no dia anterior era perdido, então, iniciava-se mais uma vez o trabalho para descobrir a chave diária, o que levava horas e, assim que a chave fosse descoberta, eles poderiam decifrar as várias mensagens alemãs que tinham se acumulado durante aquele dia, repassando toda informação para a sede do MI6. Essas informações forneceram um mapa detalhado das operações alemãs.

Depois de dominar as técnicas polonesas, os criptoanalistas passaram a inventar seus próprios atalhos para decifrar a chave do dia. Tiveram ao seu favor erros humanos que aconteciam quando algum operador da *Enigma* escolhia uma chave óbvia demais (como três letras seguidas no teclado) ou acabavam repetindo uma mesma chave (suspostamente as iniciais de uma possível namorada). Isso facilitava o trabalho dos cientistas e matemáticos.

A busca por novas técnicas de decifração era necessária uma vez que a *Enigma* continuou evoluindo durante a guerra. E a união de grandes matemáticos, cientistas, linguistas, especialistas na cultura clássica, mestres de xadrez e viciados em palavras cruzadas fez com que um problema difícil para um pudesse ser passado adiante até que alguém com a competência necessária pudesse resolvê-lo.

Dentre todos, Alan Turing merece destaque por ter atacado de forma impiedosa a máquina *Enigma* e ter vencido a batalha.

Nascido em 1911, Alan Turing foi admitido em King's College, Cambridge, no ano de 1931 numa época onde o campo matemático discutia a existência das questões indecidíveis. Inspirado por esse assunto, ele escreveu seu artigo "Sobre os números computáveis" e nele imaginava uma série de máquinas que efetuariam diversas operações matemáticas, as *máquinas de Turing*. Indo mais longe, "ele imaginou uma máquina cujo funcionamento interno pudesse ser alterado, de modo a fazê-la executar todas as funções de todas as máquinas de Turing concebíveis." (SINGH, 2007, p. 188)

A chamada *máquina universal de Turing* tinha como objetivo responder a qualquer questão que pudesse ser respondida pela lógica, porém, não era possível sempre responder, logicamente, sobre a indecidibilidade de outra pergunta. E, embora não tenha resolvido este problema, a *máquina universal de Turing*, inspirada no Motor Diferencial nº 2 de Charles Babbage, deu aos matemáticos o esquema para a criação do computador moderno programável, mesmo que não houvesse tecnologia para que pudesse ser transformada em realidade.

No ano de 1939 Alan Turing foi recrutado pela Escola de Cifras e Códigos do Governo. Pôs-se a pensar o que aconteceria se os militares alemães percebessem que uma das fraquezas de seu código consistia na repetição da palavra chave (duas vezes) nas mensagens. Se isso acontecesse, as técnicas desenvolvidas, que dependiam dessa repetição, ficariam comprometidas.

Desta forma, Turing passou a dedicar-se a um processo que não dependesse da repetição da cifragem da palavra-chave.

Para isso ele analisou antigas mensagens decifradas e notou que todas seguiam uma estrutura rígida. Notou também que podia prever parte das mensagens enviadas de acordo com o horário e local de onde fora enviada. Sempre que conseguia relacionar um trecho do texto original com o texto cifrado, ele obtinha uma *cola*. Usando essa *cola* ele começou a pensar em como descobrir os ajustes da *Enigma*. Se usasse tentativa e erro teria tantos ajustes possíveis que seria quase impossível de descobrir.

O primeiro problema estava no fato de existirem sessenta combinações diferentes para os misturadores e o segundo era a disposição dos fios no quadro de tomadas. Para diminuir o número de possibilidades ele decidiu primeiro dedicar-se à parte dos misturadores e depois às ligações no quadro de tomadas. Ao invés de uma, usou três máquinas *Enigmas* conectadas por fios elétricos para decifrar os ajustes que levariam a combinação que ele obtivera na *cola*. Quando todos os ajustes estivessem corretos, o circuito se completaria e uma lâmpada acenderia. Se os misturadores demorassem um segundo para mudarem suas orientações, levaria cerca de cinco horas para verificar todas as orientações possíveis. O segundo problema era facilmente resolvido com a digitação e comparação do texto original e cifrado, sendo necessário apenas analisar quais trocas seriam necessárias de acordo com alguns trechos das mensagens.

No início de 1940 o projeto da máquina estava pronto e em março do mesmo ano o primeiro protótipo já estava funcionando, mas os resultados não foram satisfatórios, pois a máquina demorou uma semana para encontrar a chave.

Ajustes foram feitos para aumentar a eficiência da primeira máquina, batizada *Victory*, mas a nova versão só ficaria pronta depois de quatro meses. Nesse meio tempo, os alemães deixaram de usar a repetição da chave e isso resultou na queda do número de mensagens decifradas.

Em agosto, *Agnes*, como foi apelidada a nova máquina, chegou e adequava-se as expectativas de Turing. Em um ano e meio havia mais de quinze máquinas em operação, e se tudo

funcionasse bem, em uma hora uma máquina já teria encontrado a chave da *Enigma*.

Tudo seria mais fácil e a guerra teria acabado mais cedo se os alemães não utilizassem vários sistemas de comunicação, cada um com seu livro de códigos e operadores próprios. A Marinha alemã usava uma versão especial da *Enigma*. Ela contava com oito misturadores, seu refletor podia ser fixado em vinte e seis posições diferentes e seus operadores tinham um cuidado extra ao enviar as mensagens, evitando padrões, o que impossibilitava a obtenção das *colas*. Dessa forma, a comunicação naval era praticamente impenetrável. Se essa situação se estendesse, a Inglaterra perderia a guerra.

A solução encontrada, foi a fabricação de *colas*, ou seja, aviões britânicos lançavam minas sobre um local escolhido e isso obrigava os navios alemães a enviarem avisos a outros navios. Dentre as informações estava a localização, que já era conhecida pela equipe inglesa, logo, a *cola* tinha sido obtida.

Outra solução seria o roubo do livro de códigos, que aconteceu e deu à Inglaterra e seus aliados a vantagem mais uma vez. E eles fizeram uso do livro de forma estratégica (assim como aconteceu com o telegrama de Zimmermann) escolhendo alvos, atacando apenas parte dos comboios, fazendo o necessário para que o lado alemão não suspeitasse que o livro fora roubado e decidissem mudar, mais uma vez, a configuração da *Enigma* que usavam.

Não se pode afirmar ao certo que as descobertas realizadas na Escola de Cifras e Códigos do Governo foi um fator decisivo para a vitória dos aliados, porém, especialistas afirmam que ela decididamente encurtou o período de luta, que teria se estendido até 1948 se o governo britânico não fosse capaz de ler as mensagens da *Enigma*.

Após o fim da guerra, a Escola de Cifras e Códigos do Governo foi fechada e as atividades relacionadas a criptoanálise foram transferidas para o Quartel-General de Comunicações do Governo. A maioria dos criptoanalistas que trabalharam para decifrar a *Enigma* voltaram a sua vida civil e mantiveram tudo o que viveram e descobriram em segredo, pois estavam presos a um juramento de sigilo.

Foi só em 1974, após se certificarem que a *Enigma* tinha caído em desuso, que o segredo terminou e o serviço de informações deu o aval para a publicação do livro *The Ultra Secret* que contou sobre todas as atividades feitas por aqueles intelectuais durante a guerra.

Enquanto os britânicos atacavam a *Enigma*, na América os Estados Unidos atacava a *Púrpura* (máquina de cifras japonesa). Foi graças às mensagens decodificadas que o país americano conseguiu descobrir a localização e matar uma das figuras mais influentes do alto comando japonês, o almirante Isoruko Yamamoto.

Já era sabido então que máquinas como a *Enigma* e a *Púrpura* não eram imunes aos criptoanalistas, logo, as informações que elas passavam eram de conhecimento do inimigo. Além disso, o tempo para produzir uma mensagem cifrada, enviar e esperar que ela fosse decodificada era um ponto negativo, principalmente se a situação exigisse uma resposta rápida. A pergunta

que se fazia era como garantir uma cifra segura e rápida?

Quem ajudou a solucionar esses problemas foi Philip Johnston, um engenheiro de Los Angeles que cresceu nas reservas dos índios navajo. Segundo ele, o idioma falado pelos índios era uma "língua estrangeira" para qualquer um que não fosse familiarizado com o dialeto e seria perfeito para ser usado como código. Seria necessário apenas que se empregassem índios em todas as bases, assim, ao invés de usar uma máquina (onde cada letra seria datilografada, a cifra resultante anotada, a mensagem passada pelo rádio, então, o especialista em cifras escolheria a chave adequada e mais uma vez datilografaria letra por letra da mensagem cifrada e anotaria a mensagem decodificada) eles teriam um índio que passaria a mensagem do comando pelo rádio, em seu idioma nativo, e outro índio que receberia a mensagem e a traduziria para seu comandante.

Algum treinamento foi necessário, palavras que não existiam no vocabulário dos índios foram acrescentadas, mas depois de tudo acertado, mais de 400 navajos ajudaram na comunicação e garantiram o sigilo das informações americanas. A preciosa ajuda deles só foi revelada muitos anos depois e consta na história como um dos poucos códigos que não foi decifrado pelo inimigo.

CAPÍTULO

4

HISTÓRIA DA CRIPTOGRAFIA APÓS A 2ª GUERRA

4.1 A chegada dos computadores

Embora as *bombas de Turing* fossem eficientes, elas só eram capazes de realizar algumas tarefas em alta velocidade, por isso, decifraram apenas a *Enigma*; no entanto, Hitler e seus generais comunicavam-se usando outra máquina, mais complexa, a *Lorenz*.

Para descobrir as informações mais secretas do ditador, os ingleses criaram a máquina de cifragem *Colossus*. Essa foi a máquina que motivou o desenvolvimento da criptografia na segunda metade do século XX.

A máquina britânica foi criada pelo matemático Max Newman que, se baseando na máquina de Turing, criou a *Colossus*, um invento capaz de se adaptar a diferentes problemas, o que na atualidade chamaríamos de computador programável. Porém, *Colossus* foi destruída depois da guerra. Poucos anos depois, dois americanos criaram o ENIAC que, por muito tempo, foi considerado o primeiro computador da história.

O computador ENIAC passou a ser usado tanto por criptógrafos quanto por criptoanalistas e oferecia três vantagens essenciais:

1. Por ser programável, o computador podia criar máquinas de cifragem hipotéticas bastante complexas que dificilmente poderiam ser construídas de forma concreta.

2. A alta velocidade em que operava.

3. O computador mistura números ao invés de letras, uma vez que lidam apenas com números binários.

Embora a cifragem estivesse ocorrendo mais rapidamente, é interessante ressaltar que a forma de cifrar continuou a mesma, os computadores usavam a criptografia de transposição e de substituição.

"Em 1953 a IBM lançou seu primeiro computador e quatro anos depois ela introduziu a Fortran, uma linguagem de programação que permitia que "pessoas comuns escrevessem programas para os computadores"." (SINGH, 2007, p. 272)

Quase 20 anos depois a empresa apresentou *Lucifer*, um algoritmo de cifragem para civis desenvolvido por Horst Feistel. O sistema foi considerado bastante poderoso, por isso, a Agência de Segurança Nacional (NSA) propôs um número limitado de chaves; caso o número não fosse limitado era possível que *Lucifer* permanecesse impossível de decodificar até mesmo para a grande agência.

A versão de chaves limitadas de *Lucifer* foi aceita pela NSA, renomeada como Padrão de Cifragem de Dados (DES) e usada até o início do século XXI como o padrão oficial de cifragem.

A DES oferecia segurança para as empresas fazerem transferências de dinheiro e operações comerciais, mas um problema persistia: como fazer a distribuição das chaves?

4.2 A revolução da criptografia: a distribuição das chaves

Ao longo da história da humanidade vimos como o acesso às chaves derrubou a segurança das mensagens criptografadas. É importante destacar também que a chave precisa ser do conhecimento do emissor e do receptor da mensagem, sem ela, pode ser praticamente impossível decifrar o texto.

Assim, não nos causa espanto, que o principal problema ao final do século XX fosse a segurança da distribuição das chaves. Uma solução possível seria emissor e receptor encontrarem-se pessoalmente para a entrega da chave, mas isso não era viável na maioria dos casos, pois levaria tempo. Outra opção seria o uso de mensageiros, que viajariam entregando as chaves de forma segura.

Bancos durante a década de 70 usavam esse método e o cargo de mensageiro era considerado o de maior confiança na empresa; porém, isso diminuía a força da cifra, já que envolvia uma terceira pessoa e com o aumento da rede de negócios, tornou-se financeiramente inviável.

Em 1960 o Departamento de Defesa dos Estados Unidos financiou a ARPA (Agência de Projetos Avançados de Pesquisa) e um de seus projetos tinha como objetivo conectar computadores militares através de longas distâncias. Os computadores funcionariam independentemente de um deles apresentar problemas. Em 1969, a ARPAnet surgiu e interconectava quatro locais (do inglês, *sites*). Com seu crescimento, em 1982, ela deu origem à Internet. No final da década seu uso foi liberado para não-acadêmicos e não-governamentais.

O matemático Whitfield Diffie acreditava que todos deviam ter sua privacidade assegurada ao usar a internet seja para uma troca corriqueira de e-mails ou uma troca comercial que incluiria dados pessoais como o número do cartão de crédito e isso levava novamente à segurança da distribuição das chaves.

Whitfield Diffie, juntamente com Martin Hellman, criptógrafo, e Ralph Merkle, pesquisador de criptografia, puseram-se a estudar uma forma de eliminar a necessidade da troca de chaves.

Para explicar a ideia geral do trio, convêm utilizar Alice, Bob e Eva, nomes de personagens fictícios comumente usados para facilitar explicações técnicas na criptografia. Vamos supor que Alice deseja enviar uma mensagem a Bob e Eva está tentando ter acesso a essa mensagem. Por questões de segurança, Alice vai enviar a mensagem para Bob dentro de uma caixa de ferro fechada com um cadeado. Ao receber a caixa, Bob não tem como abri-la, uma vez que não tem a chave, então ele coloca outro cadeado e envia de volta para Alice. Ao receber a caixa, agora com dois cadeados, Alice remove seu cadeado e envia de volta para Bob. Agora Bob pode abrir a caixa porque só resta o cadeado que ele tem a chave.

A história parece simples, mas mostra que é possível trocar mensagens secretas sem que aconteça a troca de uma chave. Na criptografia não seria possível seguir o passo a passo de Alice e Bob, uma vez que, diferente dos cadeados, na decodificação a sequência seguida para desfazer a cifra importa. A ideia levou Diffie, Hellman e Merkle a procurarem uma função matemática que fosse fácil de fazer mas bastante difícil de desfazer, que em Ciências da Computação, chamamos de "função de mão única". A aritmética modular proporciona muitas dessas funções.

Em 1976, Hellman encontrou a função que executava o que ele queria: $Y^n \, (mod\, P)$.

Vejamos como funcionaria essa função com nossos personagens fictícios Alice, Bob e Eva. Alice e Bob escolhem o valor de Y e P, desde que Y seja menor do que P, não há necessidade de segredo para esses valores, logo, eles poderiam ser informados até via telefone, observe o que acontece para Y = 7 e P = 11. O passo a passo da conversa e os processos efetuados podem ser acompanhados no Quadro 10.

Desta forma, mostramos que mesmo que Eva tivesse acesso a ligação, e, consequentemente, soubesse os valores de Y, P, α e β ela não seria capaz de descobrir os valores de A e B mantidos em segredo por Alice e Bob. Tudo isso porque a função escolhida por eles é uma função de mão única, logo, desfazer o processo feito por eles é difícil e seria ainda pior se os números escolhidos fossem maiores.

Naquele mesmo ano o trio patenteou sua ideia e provaram aos criptógrafos que não era necessário duas pessoas se encontrarem para trocarem a chave em segurança. A única desvantagem do método Diffie-Hellman-Merkle era o fato de que Alice e Bob precisavam escolher a chave juntos e isso traria inconvenientes caso morassem em lugares com fuso-horários diferentes. Esse seria um novo problema a ser solucionado.

Quadro 10 – Passo a passo da conversa de Alice e Bob – o modo de funcionar da função $Y^n \,(mod\, P)$

	Alice	**Bob**
Fase 1	Alice escolhe um número, digamos 3, e o mantém em segredo. Vamos chamar de A o número dela.	Bob escolhe um número, digamos 6, e o mantém em segredo. Vamos chamar de B o número dele.
Fase 2	Alice introduz o 3 na função de mão única e o resultado de $7^A \,(mod\, 11) : 7^3 \,(mod\, 11) = 343 (mod\, 11) = 2$	Bob introduz o 6 na função de mão única e o resultado de $7^B \,(mod\, 11) : 7^6 \,(mod\, 11) = 117649 (mod\, 11) = 4$
Fase 3	Alice chama o resultado de seus cálculos de alfa e envia seu resultado, 2, para Bob.	Bob chama o resultado de seus cálculos de beta e envia seu resultado, 4, para Alice.
A troca	Normalmente este seria um momento crucial porque Alice e Bob estão trocando informações, e portanto esta é uma oportunidade para Eva escutar e descobrir os detalhes da informação transmitida. Contudo, Eva e Bob podem usar a mesma linha telefônica através da qual escolheram os valores de Y e P, e Eva pode interceptar esses números que estão sendo trocados, ou seja, 2 e 4. Contudo estes números não são a chave, e por isso não importa que Eva os conheça.	
Fase 4	Alice pega o resultado de Bob e calcula a solução de $\beta^A \,(mod\, 11) : 4^3 \,(mod\, 11) = 64 (mod\, 11) = 9$	Bob pega o resultado de Alice e calcula a solução de $\alpha^B \,(mod\, 11) : 2^6 \,(mod\, 11) = 64 (mod\, 11) = 9$
A chave	Miraculosamente Alice e Bob terminaram com o mesmo número 9. Esta é a chave!	

Fonte: Singh (2007, p. 290).

Todos os exemplos de cifragem apresentados até agora usavam uma *chave simétrica*, ou

seja, a chave usada pelo emissor para cifrar a mensagem era a mesma utilizada pelo receptor para decifrar a mensagem. Whitfield Diffie pensou em uma cifra com *chave assimétrica*, ou seja, a chave de cifragem não era a mesma da decifragem.

> Se nós presumirmos que a cifra assimétrica é uma forma de cifragem por computador, então a chave de cifragem de Alice será um número e sua chave de decifragem um outro número diferente. Alice mantém em segredo sua chave de decifragem, de modo que a chamamos de *chave particular* de Alice. Contudo, ela divulga sua chave de cifragem de modo que todos tenham acesso a ela, e é por isso que a chamamos comumente de *chave pública* de Alice. (SINGH, 2007, p. 295)

Desta forma, qualquer um que quisesse enviar uma mensagem cifrada a Alice poderia usar a chave pública dela para cifrar a mensagem e somente ela teria a chave particular para decifrar a mensagem. Voltando a analogia dos cadeados teríamos o seguinte: qualquer um poderia fechar o cadeado, mas só quem pode abri-lo é quem possui a chave.

Essa ideia era muito interessante e pensar no esquema com cadeados fazia parecer fácil, mas encontrar uma função matemática que fizesse isso não era. Diffie publicou suas ideias e outros se juntaram na procura de tal função, porém não tiveram sucesso. Ela foi encontrada cerca de dois anos depois por Ron **R**ivert, Adi **S**hamir e Leonard **A**dleman, três pesquisadores do Instituto de Tecnologia de Massachusetts, Estados Unidos (MIT) e foi batizada de acordo com seus sobrenomes como criptografia RSA.

Baseada na aritmética modular e no pequeno Teorema de Fermat, a criptografia RSA funciona da seguinte forma:

- A chave pública de Alice é dada pelos números N e e. O número N é resultado da multiplicação de dois números primos p e q, escolhidos por ela. O número e é um número que não tivesse divisores comuns com (p - 1) e (q - 1) além do 1.

- Para cifrar uma mensagem para Alice primeiro transformamos a mensagem em um número M. Podemos usar o Código Padrão Americano para Troca de Informações (ASCII) para fazer essa transformação. As letras poderiam ser escritas com dígitos binários e, em seguida, transformadas em números decimais. O texto cifrado C seria produzido assim: $C = M^e \, (mod\, N)$. Esse C seria enviado para Alice.

  Como já ressaltamos, a função escolhida é uma função de mão única, logo, qualquer um que quisesse decifrar a mensagem a partir de C, encontraria muita dificuldade. Vale ressaltar que uma rede bancária, por exemplo, usa um N com cerca de 10^{308} algarismos, logo devemos escolher primos suficientemente grandes para garantir a segurança da cifra.

- Quando Alice receber a mensagem e for decifrá-la, ela precisará calcular o número d que é a chave de decifragem. Só ela pode calcular esse número, visto que apenas

ela conhece os valores de p e q. Tal número é calculado da seguinte forma: $e \times d = 1\,(mod\,(p-1) \times (q-1))$.

- Para decifrar a mensagem Alice usa $M = C^e\,(mod\,N)$

Para entender melhor o leitor pode consultar um exemplo do sistema acima no Capítulo 7, *Thread #15* na página 113.

Desta forma, se alguém quisesse decifrar a mensagem enviada a Alice, precisaria descobrir os valores de p e q, assim, a segurança da cifra RSA depende de quão difícil é a fatoração do número N.

A RSA mostrou ser uma cifra quase inquebrável. O trio que descobriu essa criptografia até mesmo lançou um desafio que teria como prêmio 100 dólares para quem quer que desvendasse os dois primos usados para gerar o "número RSA 129", um número de 129 algarismos. Demorou 17 anos, mas um grupo de 600 voluntários descobriu os dois valores.

Por ser uma cifra tão forte, a RSA precisava de computadores poderosos para rodá-la, logo, ela era usada apenas pelo governo, militares e grandes empresas.

Phil Zimmermann, graduado em física e ciência da computação, acreditava que todos deviam ter acesso a privacidade ao se comunicar na internet. Ele foi o responsável pela criação do *Pretty Good Privacy* (PGP), um algoritmo de cifragem para as massas inspirado na RSA.

Cifrar e decifrar uma mensagem usando o RSA poderia levar tempo se estivéssemos usando um computador comum. Para aumentar essa velocidade, Zimmermann mesclou as ideias de chaves assimétrica e simétrica. Assim, quando alguém fosse enviar uma mensagem usando o *software* PGP a codificaria usando uma cifra simétrica e, quando fosse enviar a chave para decodificar, usaria a RSA para cifrar essa chave simétrica. O PGP também criaria, aleatoriamente, chaves públicas e particulares para seus usuários. Também garantiria a assinatura digital de e-mails, uma técnica que utiliza criptografia para conferir segurança e integridade às mensagens enviadas.

Este *software* não era uma ideia original, outros já tinham pensado em mesclar chave simétrica e assimétrica e em assinaturas digitais, porém Zimmermann foi quem colocou todas as ideias em um produto que fosse de uso fácil e que rodasse em um microcomputador com potência moderada. Houve muita polêmica com a distribuição desse *software*. Muitos acreditavam que ele garantiria privacidade para a sociedade, outros imaginaram o que grupos como o crime organizado, os traficantes de drogas, os terroristas e os pedófilos poderiam fazer com ele.

Com a possibilidade de usar números tão grandes quanto se queira e a dificuldade de fatorá-los, garantir a insegurança da RSA viria por dois meios: um salto teórico no campo matemático, como a descoberta de um método rápido e eficaz para a fatoração de números ou um salto tecnológico que garantiria a criação de computadores potentes e capazes de fazer muitas operações matemáticas em um número bastante reduzido de tempo.

CAPÍTULO

5

FUNDAMENTAÇÃO TEÓRICA

Os capítulos até aqui desenvolveram a parte histórica da criptografia mostrando que ela foi amplamente usada para segredos militares e fins políticos, porém o desenvolvimento da criptografia moderna é motivada pela utilização massiva de computadores por pessoas comuns. Dentre os temas tratados no último capítulo, discutimos o problema da troca de chaves entre correspondentes e vimos como os norte-americanos Whitfield Driffie, Martin Hellman e Ralph Merkle provaram que era possível uma troca de chaves sem um intermediário.

É nesse momento que a Teoria dos Números começa a entrar no campo da criptografia através da noção de congruências. Mais tarde , Ronald Rivest, Adi Shamir e Leonard Adleman implementam um sistema criptográfico com chaves assimétricas (RSA) e fazem isso utilizando números primos, fatoração e outros elementos da Teoria dos Números. Por isso, neste capítulo estudaremos os elementos necessários para entender a matemática envolvida nesses conceitos. O conteúdo deste capítulo teve como fonte o livro Aritmética do Hefez (2014).

5.1 Propriedades do Números Inteiros

A nossa abordagem será essencialmente axiomática, ou seja, a partir de uma lista pequena de propriedades básicas dos números inteiros e das duas operações, vamos mostrar como podem ser obtidas as outras propriedades.

1. A adição e a multiplicação são *bem definidas*:

   Para todos $a, b, a', b' \in \mathbb{Z}$ se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

2. A adição e a multiplicação são *comutativas*:

   Para todos $a, b \in \mathbb{Z}, a + b = b + a$ e $a \cdot b = b \cdot a$.

3. A adição e a multiplicação são *associativas*:

Para todos $a,b,c \in \mathbb{Z}, (a+b)+c = a+(b+c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

4. A adição e a multiplicação possuem *elementos neutros*:

   Para todo $a \in \mathbb{Z}, a+0 = a$ e $a \cdot 1 = a$.

5. A adição possui *elementos simétricos*:

   Para todo $a \in \mathbb{Z}$, existe $b(=-a)$ tal que $a+b=0$.

6. A multiplicação é *distributiva* com relação à adição:

   Para todos $a,b,c \in \mathbb{Z}$, tem-se $a \cdot (b+c) = a \cdot b + a \cdot c$.

   Admitiremos que em $\mathbb{Z}$ também valem as seguintes propriedades:

7. *Fechamento* de $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos $a,b \in \mathbb{N}$, tem-se que $a+b \in \mathbb{N}$ e $ab \in \mathbb{N}$.

8. *Tricotomia:* Dados $a,b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

   i) $a = b$;

   ii) $b-a \in \mathbb{N}$;

   iii) $-(b-a) = a-b \in \mathbb{N}$.

9. *Princípio da Boa Ordenação:* Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

5.2 Divisão nos Inteiros

Definição 1. Dados dois números a e b, diremos que *a divide b*, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a ou, se $b \neq 0$, que b é divisível por a.

A divisão euclidiana nos garante sempre ser possível efetuar uma divisão entre dois números inteiros, mesmo quando não existe uma relação de divisibilidade entre tais números, neste caso podemos efetuar uma "divisão com resto pequeno". Esse fato, considerado um resultado central na obra de Euclides, é responsável por muitas propriedades dos inteiros que serão exploradas a seguir.

Teorema 1. (Divisão Euclidiana) Sejam a e b dois números inteiros com b $\neq 0$. Existem dois únicos números inteiros q e r tais que

$$a = bq + r, \text{ com } 0 \leq r < |b|.$$

Demonstração. Considere o conjunto $S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Existência: Existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade: Suponha que $a = bq + r = b'q' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b||q - q'| = |r - r'| < |b|,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$. □

5.3 Algoritmo de Euclides

5.3.1 Máximo Divisor Comum

Definição 2. Sejam dados dois números a e b, distintos ou não. Um número inteiro d será dito um *divisor comum* de a e b se $d|a$ e $d|b$.

Definição 3. Diremos que um número inteiro $d \geq 0$ é um *máximo divisor comum* (mdc) de a e b, se possuir as seguintes propriedades:

i) d é um divisor comum de a e b, e

ii) d é divisível por todo divisor comum de a e b.

A condição (ii) pode ser reenunciada como segue:

ii') Se c é um divisor comum de a e b, então $c|d$.

Denotando o mdc de a e b, quando existe, como (a,b), apresentaremos a seguir o Lema 1, que será utilizado para provar a existência do máximo divisor comum de dois inteiros não negativos.

Lema 1. Sejam $a, b, n \in \mathbb{Z}$. Se existe $(a, b - na)$, então, (a,b) existe e $(a,b) = (a, b - na)$.

Demonstração. Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c|d$. Isso prova que $d = (a,b)$. □

Quando não existe nenhum número inteiro c tal que $b = ca$, denotaremos $a \nmid b$. A seguir, será apresentada a prova construtiva da existência do mdc dada por Euclides. Tal algoritmo é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios.

Algoritmo de Euclides: Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b|a$, já vimos que $(a,b) = a$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão eucliana, podemos escrever

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

Temos duas possibilidades:

a) $r_1|b$. Em tal caso, $r_1 = (b, r_1)$ e pelo Lema 1, temos que

$$r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b),$$

e o algoritmo termina.

b) $r_1 \nmid b$. Em tal caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

a') $r_2|r_1$. Nesse caso, $r_2 = (r_1, r_2)$ e novamente pelo Lema 1,

$$r_2 = (r_1, r_2) = (r_1, b - q_2 r_1) = (r_1, b) = (a - q_1 b, b) = (a, b),$$

e paramos, pois termina o algoritmo .

b') $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Continuamos esse procedimento até que pare. Isto sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $B > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n|r_{n-1}$, o que implica que $(a,b) = r_n$.

Exemplo 1. A fim de visualizar e compreender melhor o funcionamento do Algoritmo de Euclides vamos calcular o mdc de 162 e 48.

Neste caso temos $a = 162$ e $b = 48$. Vamos escrever esses valores de acordo com a divisão euclidiana da seguinte forma: $a = bq_1 + r_1$, com $0 < r_1 < b$.

Assim, $162 = 48 \cdot 3 + 18$. Como $18 \nmid 48$ efetuaremos nova divisão.

Obtendo, $48 = 18 \cdot 2 + 12$. Como $12 \nmid 18$ efetuaremos nova divisão.

Logo, $18 = 12 \cdot 1 + 6$.

Como $6|12$, temos que $6 = (12,6) = (18,12) = (48,18) = (162,48)$.

Além disso, através do uso do Algoritmo de Euclides de trás para frente, podemos escrever $6 = (162,48)$ como múltiplo de 162 mais um múltiplo de 48. Obtendo

$$6 = 162 \cdot 3 + (-10) \cdot 48.$$

O Algoritmo de Euclides nos fornece um meio de escrever o mdc de dois números como a soma de múltiplos desses dois números em questão. Quando utilizarmos o Algoritmo de Euclides para expressar (a,b) na forma $ma+nb$, com $m,n \in \mathbb{Z}$, vamos nos referir a ele como *Algoritmo de Euclides Estendido*.

Precisamos de um método mais prático para determinar os inteiros m e n tais que $(a,b) = ma+nb$. Para isso precisaremos das propriedades a seguir.

5.3.2 Propriedades do Máximo Divisor Comum

Sejam $a,b \in \mathbb{Z}$. Definimos o conjunto

$$I(a,b) = \{xa+yb; x,y \in \mathbb{Z}\}.$$

Note que se a e b não são simultaneamente nulos, então $I(a,b) \cap \mathbb{N} \neq \emptyset$. De fato, temos que $a^2+b^2 = a \cdot a + b \cdot b \in I(a,b) \cap \mathbb{N}$.

A seguir utilizaremos a notação

$$d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}.$$

O Teorema 2 nos dará outra demonstração da existência do mdc de dois números a e b e da existência dos inteiros m e n tais que $(a,b) = ma+nb$. Porém, ao contrário da prova de Euclides, não nos fornecerá um meio prático para achar o mdc dos dois números, nem os inteiros m e n.

Teorema 2. Sejam $a,b \in \mathbb{Z}$, não ambos nulos. Se $d = min\, I(a,b) \cap \mathbb{N}$, então

i) d é o mdc de a e b; e

ii) $I(a,b) = d\mathbb{Z}$.

Demonstração. (i) Suponha que c divida a e b, logo c divide todos os números naturais da forma $xa+yb$. Portanto, c divide todos os elementos de $I(a,b)$, e, consequentemente, $c|d$.

Agora vamos mostrar que d divide todos os elementos de $I(a,b)$. Seja $z \in I(a,b)$ e suponha, por absurdo, que $d \nmid z$. Logo, pela divisão euclidiana,

$$z = dq + r, \text{ com } 0 < r < d. \quad (1)$$

Como $z = xa + yb$ e $d = ma + nb$, para alguns $x, y, m, n \in \mathbb{Z}$, segue-se de (1) que

$$r = (x - qm)a + (y - qn)b \in I(a,b) \cap \mathbb{N},$$

o que é um absurdo, pois $d = min\, I(a,b) \cap \mathbb{N}$ e $r < d$. Em particular, $d|a$ e $d|b$.

Assim, provamos que d é o mdc de a e b.

(ii) Dado que todo elemento de $I(a,b)$ é divisível por d, temos que $I(a,b) \subset d\mathbb{Z}$. Por outro lado, para todo $ld \in d\mathbb{Z}$, temos que

$$ld = l(ma + nb) = (lm)a + (ln)b \in I(a,b)$$

e, portanto, $d\mathbb{Z} \subset I(a,b)$. Em conclusão, temos que $I(a,b) = d\mathbb{Z}$. □

A seguir, a Proposição 1 estabelece uma relação importante entre as estruturas aditiva e multiplicativa dos números naturais, o que permitirá provar, entre vários outros resultados, o importante teorema conhecido como Lema de Gauss.

Proposição 1. Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.

Demonstração. Suponha que a e b são primos entre si. Logo, $(a,b) = 1$. Pelo Teorema 2, temos que existem números inteiros m e n tais que $ma + nb = (a,b)(= 1)$, segue a primeira parte da proposição.

Reciprocamente, suponha que existam números inteiros m e n tais que $ma + nb = 1$. Se $d = (a,b)$, temos que $d|(ma + nb)$, o que mostra que $d|1$, e, portanto, $d = 1$. □

Teorema 3 (Lema de Gauss)**.** Sejam a, b e c números inteiros. Se $a|bc$ e $(a,b) = 1$, então $a|c$.

Demonstração. Se $a|bc$, então existe $e \in \mathbb{Z}$ tal que $bc = ae$.

Se $(a,b) = 1$, então, pela proposição anterior, temos que existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = mac + nbc.$$

Substituindo bc por ae nesta última igualdade, temos que

$$c = mac + nae = a(mc + ne)$$

e, portanto, $a|c$. □

5.3.3 Algoritmo de Euclides Estendido

A versão estendida do algoritmo de Euclides calcula o mdc de dois números inteiros a e b e determina quais são os números inteiros m e n tais que $(a,b) = ma + nb$.

Suponhamos $a \geq b$. Para calcular o mdc de a e b montamos a matriz

$$A = \begin{bmatrix} b & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$$

O primeiro passo do algoritmo consiste em subtrair da segunda linha q_1 vezes a primeira linha, onde q_1 é o quociente da divisão de a por b, obtendo a matriz

$$A_1 = \begin{bmatrix} b & 1 & 0 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} b & 1 & 0 \\ r_1 & -q_1 & 1 \end{bmatrix},$$

onde r_1 é o resto da divisão de a por b.

Em seguida, na matriz A_1, subtraímos da primeira linha q_2 vezes a segunda linha, onde q_2 é o quociente da divisão de b por r_1, obtendo a matriz

$$A_2 = \begin{bmatrix} b - q_2 r_1 & 1 + q_1 q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} r_2 & 1 + q_1 q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix},$$

onde r_2 é o resto da divisão de b por r_1.

O algoritmo prossegue reproduzindo o Algoritmo de Euclides para determinação do mdc de a e b, efetuado, porém, sobre as duas linhas da matriz, obtendo no final do processo uma matriz B.

A linha (d,n,m) da matriz B que contém o elemento não nulo da primeira coluna será tal que $d = (a,b)$. Os inteiros m,n obtidos, são tais que

$$(a,b) = ma + nb.$$

5.4 Números Primos

Como já citamos na introdução deste capítulo, o princípio das chaves assimétricas baseia-se na relativa facilidade em encontrar números primos grandes e, ao mesmo tempo, na enorme dificuldade prática em fatorar o produto de dois desses números.

Assim, estudaremos nesta seção os números primos e algumas de suas propriedades a fim de melhorar nossa compreensão da criptografia RSA.

5.4.1 Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética nos garante que os números primos são suficientes para gerar todos os números naturais, logo, todos os inteiros não nulos. Para entender este teorema precisamos definir as propriedades que fazem um número ser primo.

Definição 4. Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de *número primo*.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

i) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) Se $p \nmid a$, então $(p,a) = 1$.

De fato, se $(p,a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Definição 5. Um número maior do que 1 e que não é primo será dito *composto*.

A seguir, estabelecemos um resultado fundamental de Euclides, chamado Lema de Euclides.

Proposição 2 (Lema de Euclides)**.** Sejam $a,b,p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que $(p,a) = 1$, e o resultado segue-se do Teorema 3, também conhecido como Lema de Gauss. □

Para provar o Teorema Fundamental da Aritmética precisaremos do Corolário 1 a seguir:

Corolário 1. Se $p, p_1, \ldots, p_n$ são números primos e, se $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \ldots, n$.

Demonstração. Demonstra-se o resultado por indução sobre n. Se $n = 2$, o resultado vale pela Proposição 2. Como hipótese de indução suponha que o resultado vale para $n-1$. Agora se, $p|p_1 \cdots p_n$ tem-se que $p|p_1 \cdots p_{n-1}$ ou $p|p_n$. Se $p|p_n$ o resultado segue. Se $p \nmid p_n$ então $p|p_1 \cdots p_{n-1}$ e, pela hipótese de indução $p = p_i$ para algum $i = 1, \cdots, n-1$. □

Teorema 4. (Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração. Usaremos a segunda forma do Princípio da Indução. Se $n = 2$, o resultado é verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, qie n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n - n + 1n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Vamos provar a *unicidade* da escrita. Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 \cdots q_s$, pelo Corolário 1, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. □

5.4.2 Distribuição dos Números Primos

Para demonstrar a existência de infinitos números primos, apresentaremos a prova elaborada por Euclides, através de uma demonstração por absurdo.

Teorema 5. Existem infinitos números primos.

Demonstração. Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural

$$n = p_1 p_2 \cdot p_r + 1.$$

Pelo Teorema 4 (Fundamental da Aritmética), o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \cdot p_r$. Mas isto implica que p divide 1, o que é absurdo. □

Um dos métodos mais antigos para a construção de uma tabela de primos é o *Crivo de Eratóstenes*, que permite determinar todos os números primos até a ordem que se desejar. Embora a técnica funcione, não é muito eficiente para determinar números primos de ordem muito elevada.

Faremos a seguir a construção do *Crivo de Eratóstenes* até o número 120. Para isso, será interessante usarmos o lema a seguir.

Lema 2. Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração. Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então, $n = qn_1$, com $q \leq n_1$. Segue daí que $q^2 \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo. □

Para a construção da tabela escrevemos todos os números naturais de 2 a 120. Riscam-se, de modo sistemático, todos os números compostos da tabela, seguindo o roteiro abaixo.

Risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo.

O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3, pois esses não são primos.

O terceiro número não riscado que aparece é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5, pois esses não são primos.

O quarto número não riscado que aparece é 7, que é primo. Risque todos os múltiplos de 7 maiores do que 7, pois esses não são primos.

Não necessitamos ir além do número primo 7, pois, segundo o Lema 2 temos que o próximo número primo seria o 11, cujo quadrado supera 120.

Tabela 1 – Crivo de Eratóstenes

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~

Fonte: Hefez (2014, p. 151).

5.4.3 Pequeno Teorema de Fermat

Os chineses, desde 500 anos antes da Era Comum, já sabiam que, se p é um número primo, então $p|2^p - 2$. Coube a Pierre Fermat, no século XVII, generalizar esse resultado, enunciando um pequeno mas notável teorema.

Lema 3. Seja p um número primo. Os números $\begin{pmatrix} p \\ i \end{pmatrix}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração. O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$. Nesse caso, $i!|p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i!|(p-1)\cdots(p-i+1)$, e o resultado segue, pois $\begin{pmatrix} p \\ i \end{pmatrix} = p\dfrac{(p-1)\cdots(p-i+1)}{i!}$. □

Teorema 6. (Pequeno Teorema de Fermat) Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração. Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par. Suponhamos ímpar. Nesse caso, claramente basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo válido para a, iremos prová-lo para $a+1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a.$$

Como, pelo Lema 3 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado se segue. □

O Corolário 2 também será chamado de *Pequeno Teorema de Fermat*.

Corolário 2. Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Demonstração. Como, pelo Pequeno Teorema de Fermat (Teorema 6), $p|a(a^{p-1} - 1)$ e como $(a, p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$. □

É importante ressaltar que o Pequeno Teorema de Fermat nos fornece um teste de não primalidade. De fato, dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

5.5 Congruências

Nesta seção apresentaremos uma aritmética com os restos da divisão euclidiana por um número fixado. Essa aritmética foi usada para resolver o problema da distribuição das chaves.

5.5.1 Aritmética dos Restos

Definição 6. Seja m um número natural. Diremos que dois números inteiros a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b \bmod m$.

Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b *não são congruentes,* ou que são *incongruentes,* módulo m. Escreveremos, nesse caso, $a \not\equiv b \bmod m$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão eucliana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 3. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \bmod m$ se, e somente se, $m|b-a$.

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m|b-a$, já que $|r - r'| < m$. □

Proposição 4. Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que

i) $a \equiv a \bmod m$,

ii) se $a \equiv b \bmod m$, então $b \equiv a \bmod m$,

iii) se $a \equiv b \bmod m$, e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Demonstração. (i) $a \equiv a \bmod m$:

$m|0 \Longrightarrow m|a-a \Longrightarrow a \equiv a \bmod m$.

(ii) se $a \equiv b \bmod m$, então $b \equiv a \bmod m$:

$a \equiv b \bmod m \Longrightarrow m|b-a$. Logo, existe um $k \in \mathbb{Z}$ tal que $mk = b-a$. Usando a propriedade dos números inteiros, garantimos a existência do elemento simétrico a k, o $-k$. Assim, $m(-k) = -(b-a) = a-b$ o que implica $m|a-b$ e, portanto, $b \equiv a \bmod m$.

(iii) se $a \equiv b \bmod m$, e $b \equiv c \bmod m$, então $a \equiv c \bmod m$:

Como $a \equiv b \bmod m$, e $b \equiv c \bmod m$, temos $m|b-a$ e $m|c-b$, logo, existem $k, k' \in \mathbb{Z}$ tais que

$$(1) \quad mk = b - a \quad \text{e}$$

$$(2) \quad mk' = c - b \, .$$

De (1) temos que $b = mk + a$. Substituindo em (2) temos $mk' = c - (mk + a)$. Portanto,

$$mk' + mk = c - a \Longrightarrow m(k + k') = c - a$$

Assim, $m|c - a$ e, portanto, $a \equiv c \bmod m$. □

O que torna a noção de congruência útil e poderosa é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 5. Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.

Demonstração. Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, temos que $m|b - a$ e $m|d - c$.

(i) Basta observar que $m|(b - a) + (d - c)$ e, portanto, $m|(b + d) - (a + c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m|bd - ac$. □

Corolário 3. Para todos $n \in \mathbb{N}, a, b \in \mathbb{Z}$, se $a \equiv b \bmod m$, então tem-se que $a^n \equiv b^n \bmod m$.

Demonstração. Faremos a demonstração por indução sobre n. Se $n = 1$ o resultado é válido pela hipótese.

Como hipótese de indução suponhamos que o resultado vale para n, ou seja, $a^n \equiv b^n \bmod m$. Queremos provar que vale para $n + 1$. Basta observar que

$$b^{n+1} - a^{n+1} = b^n b - a^n a$$

Como $a \equiv b \bmod m$ e $a^n \equiv b^n \bmod m$, pela hipótese, temos pela Proposição 5 item ii, o resultado desejado. □

A Proposição 6 nos diz que, para as congruências, vale o cancelamento com relação a adição.

Proposição 6. Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que

$$a + c \equiv b + c \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Demonstração. Se $a \equiv b \bmod m$, segue-se imediatamente da Proposição 5 que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$.

Reciprocamente, se $a+c \equiv b+c \bmod m$, então $m|b+c-(a+c)$, o que implica que $m|b-a$ e, consequentemente, $a \equiv b \bmod m$. □

Temos a seguir um resultado relacionado com o cancelamento multiplicativo.

Proposição 7. Sejam $a,b,c,m \in \mathbb{Z}$, com $m > 1$. Temos que

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$

Demonstração. Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são primos entre si, temos que

$$ac \equiv bc \bmod m \Leftrightarrow m|(b-a)c \Leftrightarrow \frac{m}{(c,m)}|(b-a)\frac{c}{(c,m)} \Leftrightarrow \frac{m}{(c,m)}|b-a \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$ □

Logo, o cancelamento multiplicativo $ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod m$ será válido sempre que $m > 1$ e $(c,m) = 1$.

5.6 Teorema de Euler

Um *sistema reduzido de resíduos* módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que

a) $(r_i, m) = 1$, para todo $i = 1, \ldots, s$;

b) $r_i \not\equiv r_j \bmod m$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $(n,m) = 1$, existe i tal que $n \equiv r_i \bmod m$.

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma importante função

$$\varphi : \mathbb{N} \to \mathbb{N},$$

chamada *função fi de Euler*.

Pela definição, temos que $\varphi(m) \leq m-1$, para todo $m \geq 2$.

Além disso, se $m \geq 2$, então $\varphi(m) = m-1$ se, e somente se, m é um número primo.

Exemplo 2. Se $n = kd$, com $k,d \in \mathbb{N}$, então a quantidade de números naturais m tais que $1 \leq m \leq n$ e $(n,m) = d$ é $\varphi(k)$.

Teorema 7 (Euler)**.** Sejam $m,a \in \mathbb{Z}$ com $m > 1$ e $(a,m) = 1$. Então, $a^{\varphi(m)} \equiv 1 \bmod m$.

Demonstração. Para demonstrar o Teorema de Euler, vamos seguir o mesmo roteiro do Teorema 6 (Pequeno Teorema de Fermat). Primeiramente, é fácil ver que, se $r_1, r_2, \ldots, r_{\varphi(m)}$ formarem um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ também formará um sistema reduzido de resíduos módulo m, com $(a,m) = 1$. Ou seja, podemos fazer uma relação biunívoca entre os dois conjuntos, em congruência, e daí chegamos em

$$ar_1 ar_2 \ldots ar_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \bmod m$$

ou seja

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \bmod m.$$

Pela Proposição 7, temos então, que $a^{\varphi(m)} \equiv 1 \bmod m$ e isso completa a demonstração. □

Usando-se a congruência podemos enunciar o Pequeno Teorema de Fermat da seguinte maneira:

Corolário 4. (Pequeno Teorema de Fermat) *Sejam $a \in \mathbb{Z}$ e p um número primos tais que $(a,p) = 1$. Tem-se que*

$$a^{p-1} \equiv 1 \; mod \; p.$$

Demonstração. Basta observar que, sendo p primo, $\varphi(p) = p - 1$. □

Da versão acima do Pequeno Teorema de Fermat, obtém-se a formulação do Teorema 6:

$$a^p \equiv a \bmod p, \text{ para todo } a \in \mathbb{Z}.$$

De fato, se $(a,p) = 1$, o resultado segue do Corolário 4, multiplicando ambos os membros da congruência $a^{p-1} \equiv 1 \bmod p$.

No caso em que $(a,p) \neq 1$, segue-se que $p|a$ e, consequentemente, $p|a^p - a$, o que ainda garante que $a^p \equiv a \bmod p$.

CAPÍTULO

6

SUGESTÃO DE ATIVIDADES PARA A SALA DE AULA

Neste capítulo vamos propor sugestões de atividades com o tema da criptografia e criptoanálise que podem ser desenvolvidas em sala de aula. As atividades estão profundamente ligadas à parte histórica anteriormente descrita aqui.

Muitos assuntos podem ser trabalhados usando-se a criptografia e a criptoanálise como meios. Ao falarmos da criptografia de transposição e o disco de cifras usamos a permutação e o cálculo de possibilidades, se a criptografia for de substituição há a chance de usarmos as funções e suas inversas. Lembremos que um dos primeiros métodos da criptoanálise usava a análise de frequência, já a cifra ADFGVX pode ser usada na introdução das matrizes e seus elementos e a criptografia RSA instiga o estudo dos números primos, fatoração dos números e estudo dos tipos de funções.

Acreditamos que, numa sociedade onde o jovem é apresentado a uma imensidão de estímulos, apresentar a ele conteúdos que estejam relacionados a temas atuais, como a segurança de dados, pode dar sentido ao conhecimento matemático que ele desenvolve na escola.

> Quando o aluno estuda técnicas para criptografar mensagens, palavras, frases ou textos através de permutações, funções, matrizes, entre outros, ele visualiza situações reais e consegue chegar mais facilmente a um resultado, além de estimular a aprendizagem, a utilização da criptografia também é um meio de concretizar esses saberes. (GANASSOLI; SCHANKOSKI, 2015, p. 23)

Segundo o Currículo do Estado de São Paulo: Matemática e suas tecnologias

> Quando os contextos são deixados de lado, os conteúdos estudados deslocam-se sutilmente da condição de meios para a de fins das ações docentes. E, sempre que aquilo que deveria ser apenas meio transmuta-se

> em fim, ocorre o fenômeno da mediocrização. (SÃO PAULO, 2011, p. 30)

Ao usarmos o contexto histórico da criptografia e da criptoanálise para ensinar alguns conteúdos mostramos aos alunos que certos assuntos na Matemática se desenvolvem atendendo a necessidade do momento e fortalecemos a motivação do uso da História da Matemática.

Segundo os Parâmetros Curriculares Nacionais

> A História da Matemática pode oferecer uma importante contribuição ao processo de ensino e aprendizagem [...]. Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor cria condições para que o aluno desenvolva atitudes e valores mais favoráveis diante desse conhecimento. (BRASIL, 1998, p. 42)

6.1 Permutação e possibilidades

Ao falarmos da criptografia de transposição podemos trabalhar o conceito de permutação e contagem de possibilidades. "Permutar é sinônimo de trocar. Intuitivamente, nos problemas de contagem, devemos associar a permutação à noção de misturar." (DANTE, 2005, p. 273)

Esse assunto é aprofundado no Ensino Médio, mas é trabalhado por alguns autores de livros didáticos já no 6º ano do Ensino Fundamental. Nesse contexto utilizaremos a criptografia como motivação e introdução ao conteúdo.

Objetivos: Introduzir a ideia de permutação simples e contagem de possibilidades.

Série indicada: 6º ano do Ensino Fundamental II

Materiais: Um objeto cilindrico por aluno (podem ser utilizados: rolo de papel higiênico, alumínio, filme, lápis ou caneta, copo, entre outros). E tiras de papel.

Atividade:

1. Iniciar a aula discutindo com os alunos se eles já escreveram mensagens codificadas e qual o método utilizado por eles.

   Abordar os conhecimentos prévios do aluno reforça o aprendizado de forma significativa. Segundo Daher (2006, p. 4)

> a apropriação do conhecimento não pode partir do nada, mas sim do conhecimento prévio, dos interesses e das experiências dos alunos. A aprendizagem torna-se significativa quando o novo conteúdo é incorporado às estruturas de conhecimento dos alunos passando a adquirir significado para ele ao manter relação com a sua vivência.

2. Compatilhar as histórias em que o uso de mensagens secretas culminou no sucesso ou fracasso de um plano. Seria interessante usar algumas das narrativas apresentadas nos capítulos 2, 3 e 4.

3. Propor a construção e o uso de uma cítala.

   A orientação dada para o uso deve manter-se simples. Instrua os alunos a enrolarem a tira de papel no cilindro e escreverem a mensagem ao longo do comprimento do cilindro. É esperado que os alunos percebam que não será possível desvendar a mensagem se os cilindros não forem iguais.

4. Observar a tira e tentar desvendar (sem o cilindro) qual a mensagem enviada.

   Discutir as dificuldades da permutação para um grande número de letras.

5. Solicitar que os alunos escrevam uma palavra e a codifiquem trocando a ordem das letras da forma que preferirem. Em seguida, pedir a outro aluno que decodifique o texto.

   Discutir a insegurança do método para textos curtos.

6. Debater com os alunos sobre o número de possibilidades para cada mensagem.

Introduzir, da maneira que for mais compreensível ao entendimento dos alunos, o Princípio Fundamental da Enumeração: "Se uma decisão d_1 pode ser tomada de x maneiras e se, uma vez tomada a decisão d_1, a decisão d_2 puder ser tomada de y maneiras então o número de maneiras de se tomarem as decisões d_1 e d_2 é xy." (MORGADO *et al.*, 2006, p. 18)

6.2 Generalizações e o uso de letras na matemática

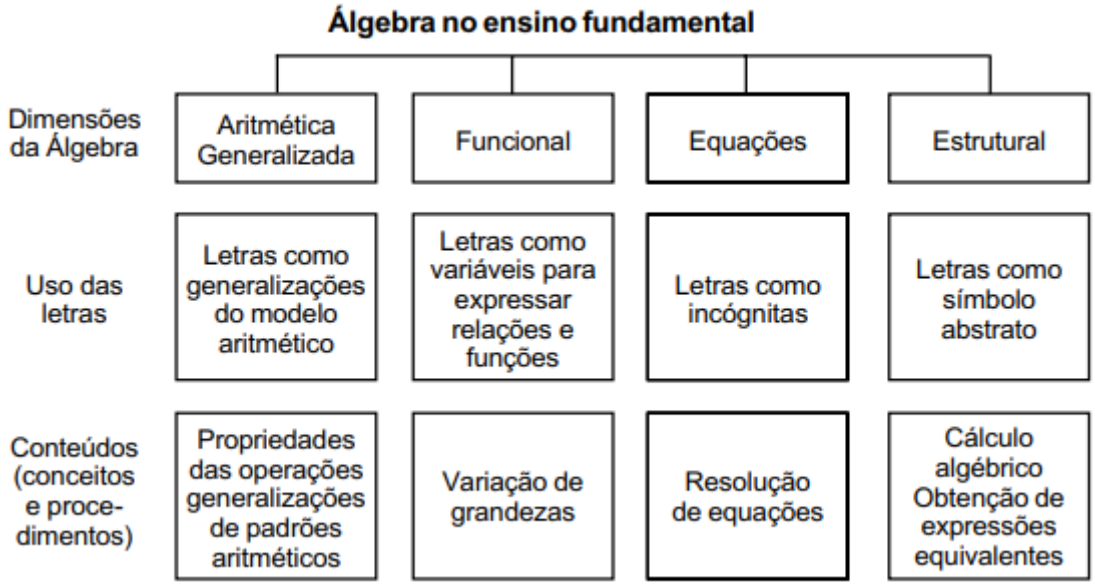
> O pensamento algébrico ou o raciocínio algébrico envolve formar generalizações a partir de experiências com números e operações, formalizar essas ideias com o uso de um sistema de símbolos significativos e explorar os conceitos de padrão e de função. Longe de ser um tópico de pouco uso no mundo real, o pensamento algébrico penetra toda a Matemática e é essencial para torná-la útil na vida cotidiana. (VAN DE WALLE, 2009, p. 287)

Segundo os Parâmetros Curriculares Nacionais (PCN) de matemática existem diferentes interpretações da álgebra escolar e diferentes funções das letras (veja o Quadro 11).

A atividade proposta encaixa-se na primeira dimensão, visto que nosso objetivo é usar a álgebra para generalizar um modelo.

Exercícios que estimulam a formação do pensamento algébrico podem estar presentes desde os anos iniciais do Ensino Fundamental, porém esse conteúdo é estudado de forma mais sistematizada a partir do 7º ano, desta forma, a atividade a seguir tem esses alunos como grupo-alvo.

Quadro 11 – Concepções da Álgebra



Fonte: Brasil (1998, p. 116).

Objetivos:

- Fazer uso de letras para expressar uma lei de formação.
- Perceber regularidades em padrões e generalizá-los.

Série indicada: 7º ano do Ensino Fundamenal II

Materiais: Quadros com cifras monoalfabéticas, seguindo o modelo da Cifra de César. Modelos disponíveis no Anexo A.

Atividade:

1. Iniciar a atividade fazendo referência ao uso de mensagens codificadas ao longo da história. Falar sobre a Cifra de César e como ela foi pensada.

2. Distribuir as cifras previamente construídas. Se o número de alunos permitir, distribuir cifras diferentes para cada um.

3. Pode ser interessante pedir que todos os alunos cifrem uma mesma frase, por exemplo, HOJE É DIA DE MAT. Assim, eles podem se familiarizar com o processo. Dependendo do entusiasmo da turma, pedir que eles escrevam pequenas frases e as codifiquem usando a cifra que receberam.

4. Socilitar que respondam as indagações abaixo:

   - Com base na cifra recebida, explique com suas palavras como você procede para determinar por qual letra do alfabeto cifrado você trocará o alfabeto original, ou seja, escreva a regra de formação da cifra.
   - Vamos escrever de forma simplificada a regra de formação que você criou. Utilizaremos **C** para nos referirmos ao alfabeto cifrado e **O** para o alfabeto original.
   - Escreva, usando essas letras, como obter um alfabeto cifrado a partir do alfabeto original.
   - Agora faça o contrário, escreva, usando essas letras como obter o alfabeto original a partir do alfabeto original.

5. A fim de discutir os resultados do item anterior o professor pode transcrever algumas respostas da frase-exemplo HOJE É DIA DE MAT de alunos que tenham cifras diferentes.

   É possível que descrever a regra de formação usando símbolos seja uma tarefa mais complicada para alguns alunos, e uma discussão aberta entre os alunos pode aumentar o entendimento do que está sendo feito.

6. Discutir com a turma quantas cifras monoalfabéticas diferentes podem ser construídas.

Se o professor achar interessante, ele pode citar o disco de cifras apresentado no capítulo 3 e construí-lo com os alunos seguindo as instruções do Anexo B.

6.3 Análise de frequência

> No mundo das informações no qual estamos inseridos, torna-se cada vez mais "precoce" o acesso do cidadão a questões sociais e econômicas em que tabelas e gráficos sintetizam levantamentos; índices são comparados e analisados para defender idéias. Dessa forma, faz-se necessário que a escola proporcione ao estudante, desde os primeiros anos da escola básica, a formação de conceitos que o auxiliem no exercício de sua cidadania. (LOPES, 2008, p. 60)

Segundo o PCN Brasil (1997) devem ser trabalhados desde os anos iniciais do Ensino Fundamental conteúdos que permitam o tratamento de informações. Assim é esperado que alunos nos anos finais do Ensino Fundamental já tenham aprendido a ler e interpretar gráficos e tabelas.

Nosso interesse com essa atividade é usar a criptoanálise como um meio de ensinar a construção de tabelas e o cálculo da frequência relativa. Vamos aproveitar que esses conteúdos podem ser trabalhados de maneira mais ampla e interdisciplinar e por isso utilizaremos o conto 'O escaravelho de ouro' de Edgar Allan Poe.

Segundo Bauer (2013) Edgar Allan Poe fez sua primeira referência à criptografia em 1839 e convidou os leitores do periódico *Alexander's Weekly Messenger* a enviarem suas mensagens escritas com cifras de substituição monoalfabéticas que ele decifraria a todas. Seus leitores queriam saber qual o segredo de suas habilidades em decifrar mensagens, e o autor revela seu método no conto do escaravelho.

Esse conto geralmente é trabalhado no 8º ou 9º ano do Ensino Fundamental e está disponível no Anexo C.

Objetivos:

- Construir tabelas de distribuição de frequências.
- Utilizar os diferentes tipos de frequência em uma tabela.

Série indicada: 8º ano do Ensino Fundamental II

Materiais: Calculadora.

Atividade:

1. Iniciar a atividade fazendo referência ao uso de mensagens codificadas ao longo da história. Comentar sobre as cifras monoalfabéticas e como durante séculos pensou-se que elas eram indecifráveis, até que os árabes descobriram que podiam decifrar a mensagem se fizessem uma análise de frequência das letras.
2. O professor pode solicitar que a leitura seja feita em casa ou conversar com o(a) professor(a) de Língua Portuguesa a fim de conciliar a leitura do conto de forma que possa ser trabalhado simultaneamente nas duas disciplinas. Como o texto cifrado é apresentado em inglês, incluir o professor desta disciplina seria enriquecedor à discussão.
3. Analisar a cifra apresentada por Legrand, tabular os resultados apresentados por ele (usando a Tabela 2), explicar e calcular a frequência relativa e a porcentagem.

Cifra de Legrand:

53%%+305))6*;4826)4%.)4%);806*;48+8&60))85;1%(;:%*8+83(88)5*+;46(;
88*96*?;8)*%(;485);5*+2:*%(;4956*2(5*-4)8&8*;4069285);)6+8)4%%;1(%9
;48081;8:8%1;48+85;4)485+528806*81(%9;48;(88;4(%?34;48)4%;161;:188;%?;

Tabela 2 – Tabela de frequências

Código	Frequência	Frequência relativa	Porcentagem
8			
;			
4			
%			
)			
*			
5			
6			
(			
+			
1			
0			
9			
2			
:			
3			
?			
&			
-			
.			

Fonte: Elaborada pelo autor.

Talvez aqui seja interessante apresentar aos alunos uma tabela (ver Tabela 3) com as frequências das letras na língua inglesa a fim de que eles comparem os resultados obtidos.

Embora a criptografia do texto *O escaravelho de ouro* esteja escrita na língua inglesa, apresentamos também a Tabela 4 que possui a frequência relativa das letras da língua portuguesa do Brasil. Se possível, discuta a tabela com os alunos.

Tabela 3 – Exemplo das estatísticas da língua inglesa

Letra	Frequência relativa (%)	Letra	Frequência relativa (%)
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.3	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.2	W	2.4
K	0.8	X	0.2
L	4.0	Y	2.0
M	2.4	Z	0.1

Fonte: Bauer (2013, p. 24, tradução nossa).

Tabela 4 – Exemplo das estatísticas da língua portuguesa brasileira

Letra	Frequência relativa (%)	Letra	Frequência relativa (%)
A	14.63	N	5.05
B	1.04	O	10.73
C	3.88	P	2.52
D	4.99	Q	1.20
E	12.57	R	6.53
F	1.02	S	7.81
G	1.30	T	4.34
H	1.28	U	4.63
I	6.18	V	1.67
J	0.40	W	0.01
K	0.02	X	0.21
L	2.78	Y	0.01
M	4.74	Z	0.47

Fonte: Tkotz (2005).

6.4 Localização de pontos

No Ensino Fundamental, mais especificamente no 6º ano, trabalhamos a localização de pontos. É nessa época que apresentamos aos alunos o sistema de coordenadas cartesianas e explicamos que qualquer ponto P poderá ser descrito de acordo com suas coordenadas da seguinte maneira: P = (a, b), onde a representa o valor lido no eixo horizontal e b representa o valor lido no eixo vertical.

Propomos que a atividade seguinte seja aplicada antes da formalização do conceito do ponto e suas coordenadas a fim de que a convenção de leitura eixo horizontal/eixo vertical seja melhor explorada.

Objetivos: Introduzir o conceito de coordenadas.

Série indicada: 6º ano do Ensino Fundamental II

Materiais: Quadros 7 x 7 como o do modelo apresentado no Quadro 12.

Quadro 12 – Quadro para cifra ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A						
D						
F						
G						
V						
X						

Fonte: Elaborada pelo autor.

Atividade:

1. Iniciar a atividade fazendo referência ao uso de mensagens codificadas ao longo da história. Fazer referência a parte histórica da Cifra ADFGVX que pode ser lida no capítulo 3.

2. Entregar o Quadro 12 para os alunos e pedir que eles o completem usando todas as letras do alfabeto e os numerais de 0 a 9 na ordem que preferirem. Fica a critério do professor decidir se o quadro a ser criado valerá para toda a sala ou se cada aluno produzirá seu próprio quadro.

3. Peça que os alunos criem frases pequenas. O primeiro passo será localizar as letras do texto comum no quadro e substituí-las pelas letras que rotulam sua fileira e coluna. Dê destaque a ordem com que escrevemos as letras codificadas aqui, explique que se a codificação for feita em outra ordem, a mensagem obtida será diferente. Deixe claro que convenções matemáticas servem como um grande combinado entre matemáticos e que isso permite que nossa disciplina avance.

4. Para terminarmos o processo vamos cifrar novamente este texto, desta vez, usando uma cifra de transposição. Para isso, escolha a palavra-chave. Pode ser qualquer palavra desde que não tenha letras repetidas.

5. Crie um novo quadro tendo a palavra-chave como conteúdo da primeira linha. Reescreva o texto cifrado completando linha por linha. Para mais detalhes, veja um exemplo no capítulo 3.

6. Rearranje as colunas do quadro de forma que as letras da palavra-chave fiquem em ordem alfabética.

7. A mensagem cifrada é conseguida seguindo-se cada coluna e então escrevendo as letras nesta nova ordem.

8. Para decifrar a mensagem, basta que o receptor tenha em mãos a mensagem codificada, conheça a palavra-chave e saiba detalhes do quadro que foi criado no início da atividade.

6.5 Números primos e a fatoração

Os números primos são usualmente trabalhados no 6º ano do Ensino Fundamental. Geralmente o conteúdo é apresentado através da definição do número, uma série de procedimentos para a determinação dos fatores primos de um número e a aplicação no cálculo do mínimo múltiplo comum (mmc) e do máximo divisor comum (mdc).

Sem uma contextualização histórica ou suas aplicações práticas, esse conceito parece "inútil" aos alunos, muitos ficam com a impressão de que é um tema que inicia e termina em si.

Sobre os números primos Brasil (1998, p. 66, grifo nosso) afirma:

> Conceitos como os de "múltiplo" e "divisor" de um número natural ou o conceito de "número primo" podem ser abordados neste ciclo como uma ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores [...] Além disso, **é importante que tal trabalho não se resuma à apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum** sem compreender as situações-problema que esses conceitos permitem resolver.

Pensando em uma abordagem prática e com exemplos de aplicações no cotidiano, propomos o ensino dos primos vinculado a criptografia RSA, de forma que mostremos como números com características 'simples' são capazes de feitos tão poderosos, como a segurança dos nossos dados na rede.

Esclarecer que a nomenclatura não tem a ver com grau de parentesco, contar que os primos foram escolhidos como a base do código que teria maior chance de ser entendido por eventuais seres inteligentes de outros mundos, entre outras curiosidades pode aumentar o interesse por parte dos alunos. Algumas dessas curiosidades serão abordadas no capítulo 7 nas *Threads* #8 a #12.

Objetivos:

- Identificar um número primo.
- Decompor um número não primo em fatores primos.

Série indicada: 6º ano do Ensino Fundamental II

Materiais: Calculadora (opcional).

Atividade:

1. Iniciar a aula perguntando aos alunos se eles sabem como os dados que eles inserem na internet permanecem seguros.
2. Discutir as respostas deles e falar sobre a criptografia RSA - de forma geral, estamos interessados em deixá-los saber que a segurança dos nossos dados na rede está baseada na dificuldade em se descobrir quais números primos foram utilizados na multiplicação que dá origem à chave pública, essa será nossa motivação para o estudo dos números primos (por se tratar de um grupo-alvo jovem, as informações devem ser repassadas de forma simplificada de modo a facilitar o entendimento. Recomenda-se a leitura da *Thread #14* do capítulo 7; as ilustrações podem ajudar o entendimento.)
3. Usar a história da matemática, contar quem foi Eratóstenes (veja *Thread #9* do capítulo 7), comentar suas constribuições e apresentar seu Crivo. O crivo pode ser construído de forma individual no caderno seguindo orientações da professora, de forma coletiva na lousa ou também pode ser apresentado através de um recurso visual como a animação[1] que mostra o passo-a-passo da construção do Crivo na internet.
4. Abordar o processo prático para a verificar se um número é primo ou não.
5. Explorar os vários processos para a determinação dos fatores primos de um número.
6. Estimular a fatoração de alguns números e usar algum valor grande, por exemplo, 907, como desafio. Depois disso, retomar a discussão da criptografia RSA e discutir como é possível que essa seja a ferramenta que proporciona proteção de senhas e transações bancárias, uma vez que eles acabaram de resolver exercícios onde descobriam os números primos que compunham determinado número.

[1] Disponível em: <https://upload.wikimedia.org/wikipedia/commons/8/8c/New_Animation_Sieve_of_Eratosthenes.gif>

7. Finalmente, deixá-los saber que os números primos usados na RSA são bastante grandes (cerca de 100 algarismos) e que mesmo que sejam usados computadores, a tarefa de decompor números muito grandes leva bastante tempo.

Os alunos do 6º ano já aprenderam potenciação, assim, é possível apresentar a eles o maior número primo conhecido da atualidade $2^{82589933} - 1$ com 24 862 048 dígitos. Esse número foi descoberto em 7 de Dezembro de 2018 pelo projeto de pesquisa mundial Great Internet Mersenne Prime Search (GIMPS).

6.6 Matrizes

Segundo consultas às obras aprovadas do Programa Nacional do Livro Didático (PNLD) a introdução às matrizes ocorre no Ensino Médio. Segundo Oliveira (2017) embora as matrizes sejam objeto de estudo na Educação Básica e na Educação Superior e de estarem relacionadas a diversas aplicações na Matemática, Engenharia, Computação Gráfica, e Economia, por exemplo, no Ensino Médio elas são abordadas de maneira superficial, mecânica e subjetiva.

Sugerimos que o professor mostre aplicações práticas desse conteúdo a fim de despertar e incentivar seu aprendizado. Escolhemos trabalhar com a Cifra de Hill (mesmo que ela não tenha sido apresentada no contexto histórico) pois é um assunto que possui muitos conteúdos possíveis de serem trabalhados no Ensino Médio. Introduzir um contexto interessante aos olhos dos jovens como a criptografia poderá motivá-los a entender o tema, uma vez que eles enxergarão uma utilidade na matéria aprendida.

Para uma explicação completa sobre como cifrar e decifrar mensagens usando a Cifra de Hill veja o Anexo D.

Objetivos:

- Efetuar multiplicação de matrizes.
- Cálculo de determinante.
- Conceito de matriz inversível.
- Introduzir uma noção básica de aritmética modular.

Série indicada: 2º ano do Ensino Médio

Atividade:

1. O professor pode iniciar a atividade discutindo com os alunos sobre a criptografia e sua importância nos dias de hoje, pode contar histórias mostrando como partes da nossa história podem ser descritas através do enfrentamento entre criptógrafos e criptoanalistas.

   Nesse contexto, introduzir a Cifra de Hill e convidar os alunos a cifrar uma mensagem (frases curtas).

2. Num primeiro momento seria interessante apresentar a eles a matriz para a codificação. Abaixo temos alguns exemplos.

   $$A = \begin{bmatrix} 6 & 11 \\ 3 & 5 \end{bmatrix} \; B = \begin{bmatrix} 11 & 2 \\ 5 & 3 \end{bmatrix} \; C = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

   As três matrizes respeitam os pré-requisitos, ou seja, são inversíveis e seus determinantes não possuem fatores primos comuns com 26.

3. Proceda com os passos 2, 3 e 4, como mostrado no Anexo D, ressaltando as técnicas para multiplicação das matrizes.

4. Para decifrar a mensagem será necessário trabalhar o inverso multiplicativo e o conceito inicial da aritmética modular. O quanto você aprofundará no assunto dependerá da resposta da turma, veja como eles reagem aos conceitos iniciais e adapte o que for necessário.

CAPÍTULO

7

DIVULGAÇÃO MATEMÁTICA

Neste capítulo discutiremos brevemente a história do desenvolvimento da divulgação científica no Brasil. Contaremos o processo de criação da nossa página MatThreadBR na rede social Twitter, que tem por objetivo contribuir com a divulgação na área da matemática. Apresentaremos os textos produzidos para a página que tiveram como tema a criptografia e, por fim, escreveremos um guia a fim de conduzir, ao menos inicialmente, aqueles que desejarem seguir por esse caminho.

7.1 A divulgação científica no Brasil

A divulgação científica no Brasil tem pelo menos duzentos anos. Ela se iniciou com a chegada da Corte portuguesa ao nosso país, passou por diversos momentos e finalidades de acordo com o interesse e o período em que aconteceu.

No século XVIII boa parte da população brasileira era não letrada e estava sobre a orientação dos jesuítas. Os conhecimentos científicos adquiridos nessa época provinham, geralmente, de algum estudo no exterior. O investimento dos portugueses à ciência no Brasil acontecia apenas se houvesse utilidade, como desenvolvimento de alguma necessidade técnica ou militar.

Em 1772 surgiu a Academia Científica do Rio de Janeiro que tinha por objetivo se dedicar à física, química, história natural, medicina, farmácia e agricultura. A academia fechou e pouco tempo depois reabriu com o nome de Sociedade Literária do Rio de Janeiro, mas não passou muito tempo operante, uma vez que seus membros foram aprisionados, acusados de conspirações pró-independência.

Com a chegada da Corte ao país, no início século XIX, surgiram as primeiras instituições de ensino superior com interesse na ciência e foi criada a Imprensa Régia, responsável por publicar, mesmo que em pequena escala, manuais para o ensino de engenharia e medicina. Surgiram também os primeiros jornais, com destaque para *O Patriota*, que apesar de ter tido

apenas dois anos de circulação, teve nele vários artigos de cunho científico publicado.

Durante o agitado período entre a Independência e o Segundo Império, houve uma diminuição nas atividades da divulgação científica.

Em meados do século XIX, como consequência da segunda revolução industrial na Europa, as atividades ligadas à divulgação científica foram intensificadas. Essa atividade foi desenvolvida aqui por estrangeiros residentes ou de passagem e brasileiros que tiveram ensino em institutos estrangeiros. O interesse pelo assunto cresceu entre o público e foi fomentado também pelo grande interesse em ciências do imperador D. Pedro II. Cresceu o número de periódicos, sobretudo no Rio de Janeiro, e artigos tanto nacionais quanto estrangeiros foram publicados.

A partir de 1874, com a ligação telegráfica do Brasil, os jornais passaram a divulgar notícias mais atualizadas sobre descobertas científicas. Nos vintes anos seguintes surgiram várias revistas com a intenção de difundir a ciência. Algumas contavam com temas controversos para a época, já outras traziam ilustrações para explicar o tema, e também haviam revistas que utilizavam linguagem de difícil compreensão para os que não fossem da área.

No início do século XX houve um aumento das atividades de divulgação científica no Rio. Este aumento

> está ligado ao surgimento de um pequeno grupo de pessoas que participaram intensamente de várias atividades que buscaram traçar um caminho para a pesquisa básica e para a difusão mais ampla da ciência no Brasil. Eles são professores, cientistas, engenheiros, médicos e outros profissionais liberais, ligados às principais instituições científicas e educacionais do Rio de Janeiro, que tinham como estratégia o desenvolvimento da pesquisa científica. Formava-se, ali, um embrião da comunidade científica brasileira que, em um movimento organizado, tentava criar condições para a institucionalização da pesquisa no país. (MASSARANI; MOREIRA, 2002, p. 51)

No início do século XX criou-se a Academia Brasileira de Ciências (ABC) e a Rádio Sociedade do Rio de Janeiro, considerada a primeira rádio brasileira. A rádio tinha como objetivo divulgar informações e temas educacionais. Em 1925, Einstein fez um breve discurso na rádio apoiando a difusão cultural e científica através do uso do rádio.

Nessa época, surgiram revistas que tinham por objetivo a divulgação científica, jornais abriram espaço para notícias científicas cobrindo, principalmente, a visita de cientistas estrangeiros e muitos livros do tema foram publicados.

Nos 40 anos seguintes foram criadas aqui no Brasil as primeiras faculdade de ciências e institutos de pesquisas como o Centro Brasileiro de Pesquisas Físicas, o Instituto de Matemática Pura e Aplicada (IMPA) e o Instituto Nacional de Pesquisas da Amazônia. Nos anos 50 criou-se o Conselho Nacional de Pesquisa (CNPq), uma agência pública de incentivo a pesquisa.

> Entre as atividades de divulgação científica [...] destacou-se a produção de filmes pelo Instituto Nacional do Cinema Educativo (INCE) [...] esse instituto produziu mais de uma centena de filmes curtos (em geral, com duração entre 3 e 30 minutos), voltados para a educação em ciências, para a divulgação de temas científicos e tecnológicos ou para a difusão de informações sobre algumas das principais instituições científicas do país. (MASSARANI; MOREIRA, 2002, p. 57)

Entre os autores da época destacavam-se Monteiro Lobato e o matemático Júlio César de Mello e Souza. O primeiro escreveu *Sítio do Pica-Pau Amarelo* onde a ciência tinha presença constante, e o segundo escreveu *O homem que calculava* sob o pseudônimo de Malba Tahan que contava histórias e curiosidades matemáticas.

Destacava-se também José Reis, médico, economista e divulgador científico que escreveu livros sobre ciência para crianças e adolescentes, fez programas em rádios sobre o assunto e até o final de sua vida escreveu uma coluna destinada a ciência no jornal Folha de São Paulo. Ele também foi um dos criadores da Sociedade Brasileira para o Progresso da Ciência (SBPC) que tinha como objetivo ampliar a popularização da ciência. Sua contribuição à divulgação científica foi tamanha que em 1978 a CNPq criou o Prêmio José Reis de Divulgação Científica que premia quem desenvolve trabalhos significativos na área.

Nos anos 80, seções sobre ciência foram criadas em jornais diários, surgiram programas de televisão como *Nossa Ciência* e *Globo Ciência* e a revista *Ciência Hoje* foi elaborada com o objetivo específico de divulgar e aproximar o conhecimento do público.

Na mesma época foram criados vários centros de ciência que, junto aos museus, empenharam-se em disseminar a ciência. A questão é que, ainda hoje, esses centros atingem pouco a população geral, possuem como visitantes principais os estudantes que os conhecem, sobretudo, em passeios escolares. Parece que não criamos aqui em nosso país uma cultura de consumo de ciência.

Na atualidade contamos com Núcleos de Divulgação Científica em muitas universidades, textos em revistas e jornais, podcasts, programas de TV e redes sociais.

É preciso que a ciência adentre a esfera pública e lá seja discutida. Se faz necessário que a sociedade se aproprie do conhecimento científico e faça uso dele para tomar decisões. E para que isso aconteça precisamos de mais pessoas dispostas a falar sobre ciência.

7.2 Usando a internet na divulgação matemática

Segundo pesquisa da TIC[2] Domicílios - 2018, cerca de 70% da população brasileira tem acesso à internet.

Com o advento da internet o conhecimento está a um clique de distância e todos podem se informar sobre qualquer assunto.

[2] TIC: tecnologias da informação e comunicação

Algumas áreas já estão fazendo uso dessa ferramenta e se unindo às redes sociais para disseminar o conhecimento científico. Dentre as iniciativas citamos a #AstroThreadBR criada pela astrônoma Geisa Ponte.

> A #AstroThreadBR é um projeto de divulgação científica que usa uma hashtag do Twitter pra reunir em esforço coletivo dezenas de astrônomos profissionais e amadores para estreitar os laços entre a população, cientistas e seu trabalho, além de advogar pela conscientização da importância dos investimentos em ciência de base e da educação acessível e de qualidade para todos. (PONTE, 2018)

Ao ver o interesse por sua página crescer, a autora convidou outras áreas a participar. Aceitamos o convite, iniciamos a página #MatThreadBR e colocamos como objetivo divulgar conteúdos matemáticos. Nosso foco inicial foram nossos estudos sobre a criptografia.

No *Twitter* existem os *tweets* que são postagens com no máximo 280 caracteres e existem as *threads*, um encadeamento dessas postagens. Ao usar uma *hashtag* (#) você classifica um termo ou palavra e facilita sua exibição na busca da plataforma. Ao clicar em uma *hashtag* o site mostra todos os *tweets* que a possuem. A *hashtag* é, portanto, uma forma de reunir informações de um mesmo tema mas de autores diferentes.

Nossa intenção com a abertura da página foi participar do processo de divulgação científica na rede social, apoiando e convidando outros a se juntarem a ele. Escolhemos o *Twitter* pois há, nos dias de hoje, um aumento no consumo de textos rápidos e essa plataforma tem como principal característica os textos curtos. Além disso, a #AstroThreadBR possui grande engajamento e nos apoiou desde o início, depois que a página divulgou a #MatThreadBR o número de seguidores e de engajamentos com a nossa página aumentou.

Inicialmente escolhemos temas dentro de nosso estudo e montamos *threads* semanais, com o fim do conteúdo da criptografia (pelo menos no que se refere ao que estudamos ao longo da dissertação), passamos a postar textos de conteúdos matemáticos diversos. A linguagem dos textos não é formal e tentamos nos valer ao máximo de recursos visuais como o uso de imagens, gifs (um tipo de imagem que exibe movimento) e vídeos.

7.2.1 As threads

Acreditamos que o tema criptografia podia gerar curiosidade, por isso, usamos sua parte histórica como material para nossas *threads*. De modo geral, cada postagem teve início e fim nela mesmo, ou seja, não era necessário nenhum conhecimento prévio do assunto para acompanhá-las. Alguns temas por serem maiores ganharam mais de uma postagem e, eventualmente, fizemos referência a postagens anteriores.

Iniciamos as postagens no mês de Outubro e nele se comemora o *Ada Lovelace Day*. Usamos a *hashtag* do evento a fim de atrair outras pessoas interessadas no tema para nossa

página.

Escrevemos dezessete *threads* falando sobre criptografia e temas relacionados a ela. O Quadro 13 resume todas as postagens do tema:

Quadro 13 – Data de postagem e conteúdo das *threads*

Data	Conteúdo
31.10.2019	História e contribuições de Ada Lovelace
07.11.2019	Esteganografia: o que é e algumas histórias
14.11.2019	Microponto: como foi utilizado
21.11.2019	Criptografia e a cítala
28.11.2019	Cifra de substituição
05.12.2019	Histórias: Maria, Rainha da Escócia e o telegrama de Zimmermann
12.12.2019	2ª Guerra Mundial: a máquina Enigma
19.12.2019	Números primos: denifição, origem do nome e o teorema fundamental da Aritmética
26.12.2019	Números primos: encontrando números primos e o Crivo de Eratóstenes
02.01.2020	Números primos: como descobrir se um número é primo
09.01.2020	Números primos: prova da infinitude dos primos
16.01.2020	Números primos: para que servem? (aritmética dos relógios)
23.01.2020	Criptografia: chave-pública (é possível contar um segredo através de uma conversa pública?)
30.01.2020	Criptografia RSA: explicação
06.02.2020	Criptografia RSA: explicação matemática
13.02.2020	Criptoanálise: análise de frequência no conto de Edgar A. Poe
20.02.2020	A Cifra de Vigènere

Fonte: Elaborada pelo autor.

Nas páginas a seguir, apresentaremos os textos criados para a nossa página. Infelizmente não é possível copiar o formato exato das postagens, uma vez que não podemos incluir os gifs ou os vídeos que dão maior fluidez a leitura do texto. Cada parágrafo do texto representa um *tweet*.

Thread #1 31.10.2019

O primeiro programa de computador da história foi criado por uma mulher! Venha conhecer um pouco de Ada Lovelace [4]. #MatThreadBR #AdaLovelace

Nascida em 1815, filha de uns dos principais poetas da Inglaterra com uma estudiosa da matemática, Ada foi criada próxima dos números.

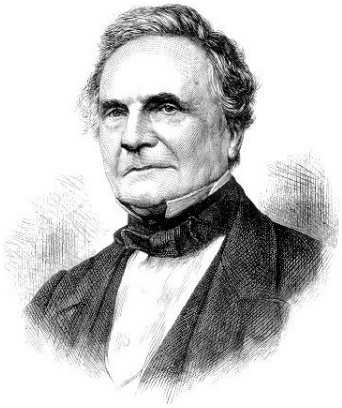
Junto ao cientista Charles Babbage [5] participou do projeto sobre a Máquina Analítica que foi criada para executar e imprimir cálculos matemáticos e percebeu o grande potencial de programação da máquina concluindo que ela era capaz de fazer mais do que seu criador

imaginava.

Figura 4 – Retrato em aquarela de Ada Lovelace por Alfred Edward Chalon por volta de 1840

Fonte: Chalon (c1840).

Figura 5 – Retrato de obituário de Charles Babbage



Fonte: Hook e Norman (2002, p. 161)

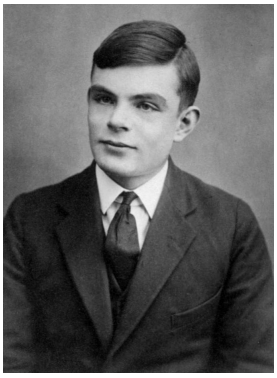
A pedido do cientista, Ada traduziu um artigo sobre o funcionamento da máquina. Enquanto o traduzia incluiu várias notas pessoais para exaltar as capacidades da máquina. Ao fim, sua tradução ficou três vezes maior do que o texto original.

Dentre as observações escritas por Ada, havia um algoritmo para a Máquina Analítica computar a Sequência de Bernoulli. Esse foi considerado o primeiro programa de computador já criado, inventado antes mesmo da existência concreta de um computador.

Ada não recebeu reconhecimento enquanto estava viva. Seu reconhecimento como iniciadora da computação só surgiu após Alan Turing ter feito referência a seu trabalho.

Turing [6], conhecido como ‘o pai da computação moderna’, foi um matemático e cientista da computação britânico responsável por formalizar o conceito de algoritmo criando a Máquina de Turing, que abriu as portas para a invenção dos computadores que utilizamos hoje em dia.

Figura 6 – Foto do passaporte de Alan Turing aos 16 anos



Fonte: WikimediaCommons (1928).

Depois de 100 anos, o material de Ada foi republicado; a Máquina Analítica foi reconhecida como o primeiro computador e as anotações da jovem foram reconhecidas como a descrição de um computador e de um software.

Mais tarde, o Departamento de Defesa dos Estados Unidos criou um código de linguagem e o batizou de ADA em homenagem a ela. Essa linguagem pode ser utilizada para softwares de aviação, por exemplo.

Além disso, toda segunda terça-feira de outubro comemora-se o "Ada Lovelace Day", um dia que tem como objetivo celebrar o legado de Ada e de outras mulheres das áreas de tecnologia, matemática e engenharia, além de incentivar mais mulheres a trilhar esses caminhos.

Não teríamos tanta tecnologia como os smartphones e os computadores se Ada não tivesse elaborado o primeiro programa da história o que permitiu que outros cientistas desenvolvessem seus conceitos e criassem essas novas tecnologias.

Thread #2 07.11.2019

Mensagens secretas podem ser muito interessantes. Às vezes aparecem em filmes e quando desvendadas nos deixam boquiabertos.

Sabia que existe um nome para a 'arte de escrever mensagens ocultas'?! Já ouviu falar da ESTEGANOGRAFIA?

Se liga na thread que eu conto mais. #MatThreadBR

Essa técnica vem sendo usada a mais de 2500 anos e foi capaz de mudar o rumo de alguns acontecimentos na história, pois confundia inimigos e transmitia mensagens de forma segura.

Um dos primeiros relatos foi feito por Heródoto, pai da história, lá no século 5 a.C..

Ele narra o conflito entre a Pérsia e a Grécia. Segundo ele foi a arte da escrita secreta que

salvou a Grécia de ser conquistada por Xerxes, o líder dos persas.

Enquanto esse líder construía a nova capital de seu reino, recebeu presentes de todas as regiões do império, menos de Atenas e Esparta. Não contente com a afronta, ele passou os 5 anos seguintes planejando um ataque as duas cidades para expandir seu império.

No entanto, seus planos de ataque foram vistos por Demarato, um grego exilado na Pérsia. Diante de suas descobertas e de sua fidelidade à pátria, ele resolveu enviar uma mensagem à Esparta para avisar do ataque. Era necessário que seu aviso não fosse detido pelos guardas.

Sua ideia para ocultar a mensagem foi raspar a cera de algumas tábuas de madeira, escrever o que Xerxes pretendia fazer e depois cobrir a tábua novamente com a cera. Assim, seu aviso passou pelos guardas, que não suspeitaram das 'tábuas em branco' e chegou ao seu destino.

Depois que a mensagem foi descoberta e compartilhada, os gregos começaram a se armar. Sem saber que tinha sido descoberto, Xerxes, Rei dos Reis, atacou a Grécia, que tinha uma armadilha planejada e destruiu os navios persas.

Heródoto escreve sobre outro momento em que o envio de uma mensagem oculta garantiu a entrega de uma informação sem que houvesse desconfiança por parte dos guardas. Segundo ele, rasparam o cabelo de um homem, escreveram a mensagem em sua cabeça e esperaram até que seu cabelo crescesse de novo. Com o cabelo comprido, o homem foi enviado ao seu destino e chegando lá, raspou novamente seus cabelos e mostrou ao destinatário a mensagem.

Deu para perceber que naquela época, tempo não era um problema. . . Como será que a esteganografia se desenvolveu? Vocês conhecem alguma técnica para ocultar mensagens?

Thread #3 14.11.2019

Gosta de filmes de ação e espionagem? Já assistiu Missão Impossível 3? No filme o agente Ethan Hunt descobre um MICROPONTO em um cartão postal enviado por uma colega de trabalho, nele existe um vídeo. O filme é de 2006, mas a técnica existe desde 1870. Olha a thread$\sim$ #MatThreadBR

No filme, sua colega de agência, oculta um vídeo em um microponto para mostrar o envolvimento do diretor da unidade com um traficante de armas. É possível esconder também páginas de documentos. Mas como isso funciona? #DivulgaçãoCientífica

A ideia era encolher uma foto com texto ou imagem até um tamanho muito pequeno (o tamanho de um ponto final) para facilitar a transmissão e prevenir a detecção; então era escondida em meio de um texto normal, sendo colocada como ponto final, ou como o pingo do i ou do jota.

Podiam ser escondidas também embaixo do selo de cartas como foi feito no filme. Na época, muitos espiões usavam a Minox Câmera [7] para fotografar documentos secretos e utilizavam a técnica para reduzir o tamanho até cerca de 1mm e enviar a informação.

Figura 7 – Câmera sub-miniatura de espionagem Minox C

Fonte: Halicki (2016).

Conta-se que durante a 2ª Guerra Mundial um agente duplo contou ao FBI que os alemães dominavam a técnica do microponto e a utilizavam amplamente. Demorou cerca de 1 ano para que os americanos conseguissem identificar o primeiro microponto num envelope.

A quantidade de informações roubadas era enorme, e incluía plantas de edifícios, esquemas táticos, estatísticas de produção, informação sobre urânio... E essa é a principal desvantagem do uso do microponto, se descoberta, a informação não está protegida.

Para aumentar a segurança, passaram a codificar as mensagens, assim, mesmo se descobertas, demorariam a serem decifradas. Escrever uma mensagem em códigos é o objeto de estudo da CRIPTOGRAFIA.

Com a criação do computador e o aumento do uso da internet, milhões de dados são transmitidos diariamente; e ficou mais fácil esconder um texto numa foto, por exemplo. Você pode ver orientações de como fazê-lo no site: Esconder texto em uma imagem[3]

Se tiver mais interesse pelo assunto:

Uso do microponto pela CIA[4]

Site usa esteganografia para esconder mensagens em textos públicos[5]

Thread #4 21.11.2019

Na internet provavelmente já viu uma mensagem explicando que o conteúdo de determinado site era criptografado. Criptografia na internet é sinal de segurança. Quer conhecer o 1º aparelho criptográfico? Vem comigo∼ #MatThreadBR

Escrever um texto em códigos ou desvendar um texto escrito em códigos é o que faz a

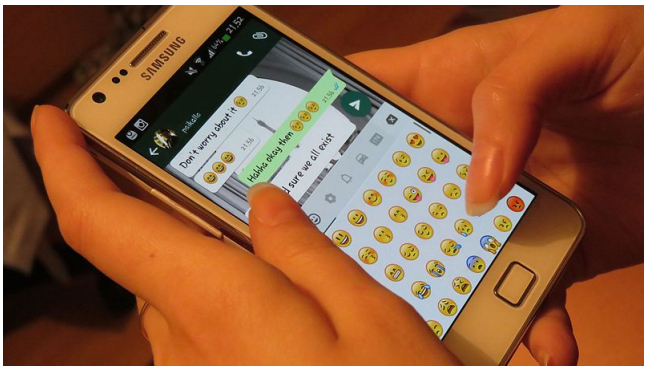
[3] Disponível em: <https://pt.wikihow.com/Esconder-Texto-em-uma-Imagem>

[4] Disponível em <https://www.smithsonianmag.com/videos/category/history/microdots-the-cias-tiny-secret-message-holders/>

[5] Disponível em <https://canaltech.com.br/espionagem/Site-usa-esteganografia-para-esconder-mensagens-em-textos-
>

criptografia. Você provavelmente a tem na palma de sua mão, naquele aplicativo de mensagens instantâneas (sim, aquele mesmo que você está pensando). [8]

Figura 8 – Enviando mensagens no whatsapp



Fonte: Lukats (2015).

A cítala (bastão) espartana é considerada o primeiro aparelho de criptografia. Seu uso era bastante simples. Eram necessários dois bastões idênticos um para quem enviaria a mensagem e outro para quem receberia. #DivulgaçãoCientífica

Para codificar a mensagem utilizava-se uma tira de pergaminho ou de couro que devia ser enrolado ao longo do bastão, depois se escrevia a instrução ao longo do comprimento do objeto. [9] #Matemática

Figura 9 – Cítala

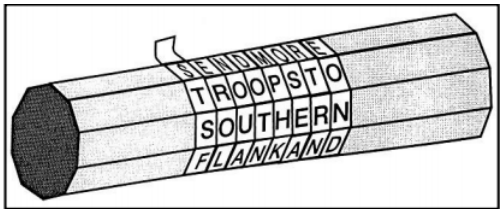
Fonte: WikimediaCommons (2007).

Depois de desenrolado, o assunto do texto não era compreensível. Para desvendar a mensagem, era necessário enrolá-la no bastão idêntico que estava com o recebedor. *tradução da figura [10]: envie mais tropas para o lado sul e...

O interessante desse método é que a tira de couro podia ser usada como cinto e passaria despercebida caso quem levasse a mensagem fosse revistado por guardas. E foi o que aconteceu em 404 a.C. em mais um confronto Esparta-Pérsia.

Um mensageiro espartano, o único sobrevivente de um grupo de cinco soldados, chegou todo ensanguentado e entregou seu cinturão a Lisandro um estrategista espartano que ao enrolar em torno de seu citale descobriu o ataque e o bloqueou.

Figura 10 – Cítala



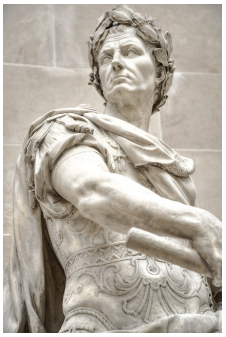
Fonte: Singh (2007, p. 24)

Thread #5 28.11.2019

Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são criptogramas. #MatThreadBR #DivulgaçãoCientífica #Matemática

O primeiro documento a utilizar a criptografia de substituição data do primeiro século antes de Cristo e aparece no texto Guerras da Gália de Júlio César [11] um dos maiores comandantes militares da história.

Figura 11 – Estátua de mármore de Júlio César



Fonte: Skitterphoto (2017).

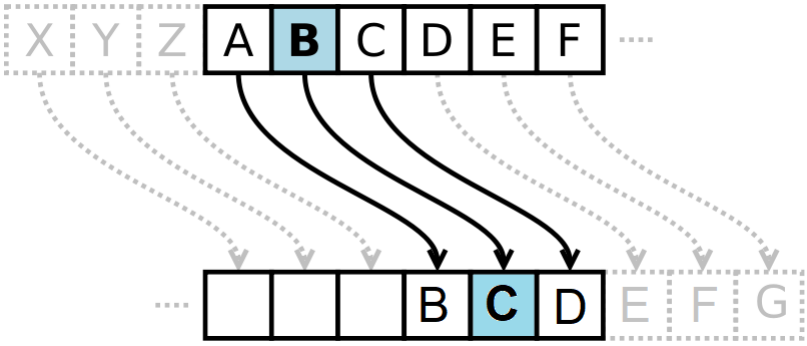
O governante escreve uma carta trocando as letras do alfabeto romano por letras gregas. Outra mudança foi a substituição de cada letra do alfabeto por uma que estivesse três posições adiante, esse método é conhecido como Cifra de César. [12]

Dessa forma, se a mensagem normal fosse: PRECISAMOS DE AJUDA ENVIE SOLDADOS, a mensagem criptografada ficaria: SUHFLVDPRV GH DMXGD HQYLH VROGDGRV.

Usando essa fórmula, podemos gerar 25 tipos diferentes de cifra [13], basta mudarmos, uma a uma, as letras que substituirão a letra A e, a partir disso, escrever o resto das letras em ordem alfabética. Cada linha do quadro abaixo representa um novo alfabeto cifrado.

Os textos cifrados assim eram considerados tão confiáveis que durante anos imaginou-se que eles eram indecifráveis, porém, se o texto for longo, haverá a repetição de padrões, e em criptografia, repetição é sinônimo de código fraco.

Figura 12 – Cifra de César com uma deslocação de 3



Fonte: Cepheus (2016).

Figura 13 – As 25 diferentes cifras

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Singh (2007, p. 66)

Esse problema seria contornado com a escolha de uma palavra/frase-chave. Iniciaríamos o alfabeto cifrado com as letras da palavra/frase, excluindo-se repetições, e depois, seguiríamos a ordem do alfabeto normal com as letras que restaram.

Você pode criar sua Cifra: 1º escolha a palavra-chave: COMANDANTE VALDEZ, 2º elimine letras repetidas: COMANDTEVLZ, 3º complete com o restante do alfabeto excluindo as letras que já apareceram no passo 2: BFGHIJKPQRSUWXY. [14] Está pronto!

Figura 14 – Exemplo de cifra

Alfabeto normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	**C**	**O**	**M**	**A**	**N**	**D**	**T**	**E**	**V**	**L**	**Z**	B	F	G	H	I	J	K	P	Q	R	S	U	W	X	Y

Fonte: Elaborada pelo autor.

Vamos deixar um desafio. Tentem decifrar essa mensagem. Usamos um dos 25 alfabetos cifrados, a frase pertence a um famoso físico e matemático e sua obra é considerada uma das mais influentes na história da ciência.

AM MC DQ UIQA TWVOM, NWQ XWZ MABIZ AWJZM WUJZWA LM OQOIVBMA - QAIIK VMEBWV. As duas últimas palavras referem-se ao nome do físico.

Pense nas letras que mais se repetem em nossa língua e compare-as com as letras que mais se repetem no texto, tente fazer algumas substituições para ver se alguma palavra se revela. Se quiser use esse site: Codifica[6].

Resposta: Se eu vi mais longe, foi por estar sobre ombros de gigantes - Isaac Newton

Thread #6 05.12.2019

Muitas histórias tiveram um fim inesperado depois que o conteúdo de alguma mensagem secreta foi descoberto. Na thread de hoje conto duas dessas histórias: uma sobre Maria, a Rainha da Escócia e outra sobre a 1ª Guerra Mundial. #MatThreadBR

Em 1586, Maria, a Rainha da Escócia [15] foi executada por tramar o assassinato da Rainha Elizabeth da Inglaterra. A vida de Maria foi marcada por dificuldades; não teve sorte como herdeira, nem com os maridos.

Figura 15 – Maria, rainha da Escócia (Nicholas Hilliard, 1578)

Fonte: Hilliard (1578).

[6] Disponível em <http://www.codifica.ibict.br/>

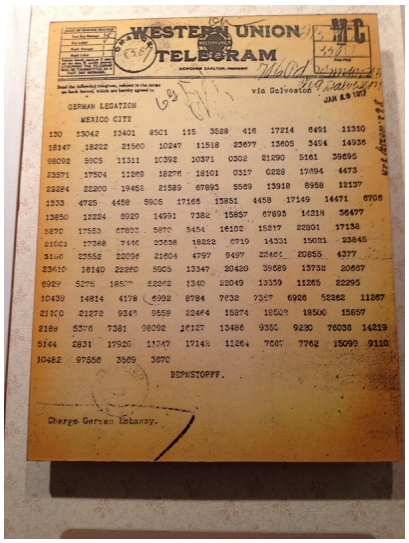
Depois de ser aprisionada por seu povo descontente, ela fugiu para a Inglaterra pedindo apoio a sua prima Elizabeth I. O que encontrou foi outra prisão, uma vez que ela oferecia risco à coroa de sua prima.

Após 18 anos de prisão ela recebeu uma carta de seus simpatizantes e o conteúdo revelava não só um plano para libertá-la como uma trama para matar a atual rainha.

As cartas trocadas eram codificadas e por acreditarem que eram indecifráveis, cometeram o erro de colocarem suas informações, incluindo estratégia e o nome dos cavalheiros na correspondência. Descoberta a conspiração, Maria foi decapitada.

Sobre a 1ª Guerra Mundial, poucos conhecem o telegrama de Zimmermann [16], ministro das Relações Exteriores alemão. Em 1916, os Estados Unidos mantinham a neutralidade, a espera de que um acordo fosse firmado e onde atuassem só como mediadores.

Figura 16 – O Telegrama Codificado de Zimmerman



Fonte: Levine (2012).

Em 1917, o ministro alemão enviou um telegrama codificado que tinha por objetivo uma união com o México a fim de atacar os Estados Unidos. Ele acreditava que se houvesse conflito interno o suficiente o país americano ficaria fora da guerra.

Entretanto, eles não contavam que seu telegrama seria interceptado e decifrado pelos ingleses. Depois que os ingleses enviaram uma cópia do telegrama para o presidente americano ele não viu alternativa a não ser entrar na guerra.

Sua entrada afetou o rumo do conflito e junto com seus aliados venceram a guerra.

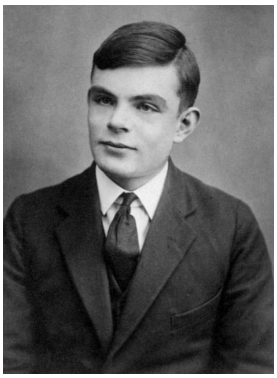
Moral da história: Às vezes, nenhuma cifra é melhor do que uma cifra fraca; pois esta passa uma falsa sensação de segurança e pode voltar para te assombrar.

Thread #7 12.12.2019

Na 1ª Guerra Mundial os criptoanalistas tiveram um grande papel, pois decifraram cartas escritas em códigos, durante a 2ª Guerra não foi diferente. Você assistiu ao filme "O jogo da imitação"? Conhece a Enigma? Confira a thread. #MatThreadBR

O filme conta a história de Alan Turing [17], um importante matemático que criou uma máquina capaz de decifrar a máquina Enigma que representou por 13 anos a grande vantagem da Alemanha, uma vez que suas mensagens eram consideradas indecifráveis.

Figura 17 – Foto do passaporte de Alan Turing aos 16 anos



Fonte: WikimediaCommons (1928).

A máquina Enigma foi uma invenção do alemão Scherbius que desejava substituir o uso de papel e lápis na hora de escrever uma mensagem em códigos, a vantagem do aparelho era a diminuição de erros humanos no processo da codificação.

A máquina [18] era composta por 3 partes: um teclado para digitar o texto normal, uma unidade misturadora (para traduzir as letras do texto original para o texto codificado) e um teclado que indicava as letras do texto codificado.

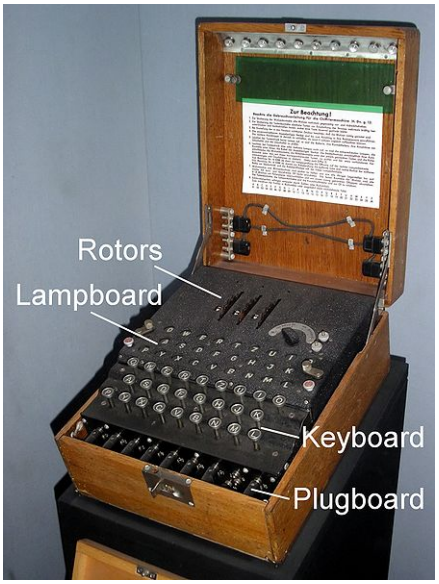
Havia várias versões da Enigma. As usadas pelos militares contavam com 3 ou mais misturadores (veja na foto [19] os três discos em frente à máquina). Quanto mais misturadores, mais difícil a tarefa de decodificar a mensagem interceptada.

Todos os dias os alemães determinavam uma configuração e uma palavra-chave para a máquina e enviavam suas mensagens de forma segura, uma vez que havia mais de 10 quatrilhões (10 com mais 15 zeros) de chaves possíveis.

Decididos a vencer, os ingleses recrutaram matemáticos, cientistas, linguistas, especialistas na cultura clássica, mestres de xadrez, viciados em palavras cruzadas. Todos foram levados para a Escola de Cifras e Códigos do Governo.

Depois de 2 anos de estudo e inspirado nos conhecimentos dos poloneses sobre a Enigma, Alan Turing e sua equipe construíram uma máquina [20] capaz de testar todas as possibilidades de chave e foram capazes de decifrar as mensagens dos alemães.

Figura 18 – Máquina Enigma no Museu Imperial da Guerra, Londres



Fonte: Sperling (2004).

Figura 19 – Máquina Enigma

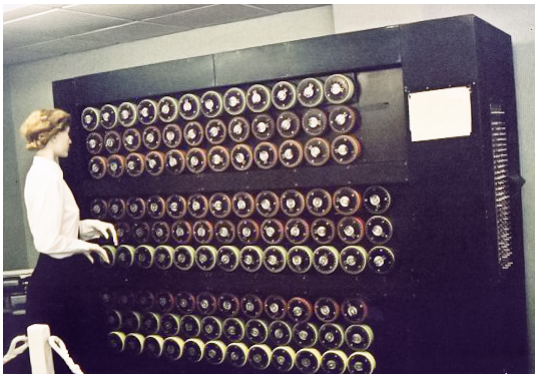
Fonte: Flickr (2018).

Sabendo quais seriam os próximos passos do inimigo a Inglaterra planejou a melhor estratégia para lidar com os ataques e a guerra terminou com a derrota da Alemanha. Especialistas afirmam que a conquista inglesa decididamente encurtou o período de luta, que teria se estendido até 1948 se o governo britânico não fosse capaz de ler as mensagens da Enigma.

Thread #8 19.12.2019

Vamos falar um pouco sobre os números primos. Quando se trata deles as perguntas são várias: o que são?, por que tem esse nome?, são infinitos?, como descobrimos se um nº é ou não primo?, servem para quê? O assunto é extenso, mas vamos abordar alguns tópicos hoje.

Figura 20 – Modelo de uma Bomba de Turing em Bletchley Park



Fonte: Hartwell ().

#MatThreadBR

Números que surgiram de forma espontânea e natural através da contagem de animais, por exemplo, são chamados números naturais. São eles: $1, 2, 3, 4, \ldots$ Quando estamos entre eles, a expressão ***dividir por*** é o mesmo que ***estar na tabuada de***.

Número primo é todo número maior do que 1, que pode ser dividido apenas por dois números: o 1 e ele mesmo. Os primeiros números primos são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ... Se um número tem outros divisores além desses é chamado de número composto.

Ao contrário do que muitos pensam os primos não receberam este nome por terem relação com parentesco. O nome primo vem de um conceito pitagórico antigo. Para eles os números naturais se dividiam em: o número 1, os números primários e os números secundários.

Os números primários (em grego: *protoi arithmói*) correspondem aos números que chamamos de primos. Eles receberam esse nome quando o romano Boethius traduziu para o latim o termo grego que resultou em: ***numerus primus***.

Todo número que não é primo pode ser escrito como a multiplicação de números primos. Essa característica tão básica é conhecida como o Teorema Fundamental da Aritmética. Assim, os números primos são aqueles que constroem os outros números com a ajuda da multiplicação.

Por essa condição os números primos foram escolhidos como a base do código que teria maior chance de ser entendido por eventuais seres inteligentes de outros mundos. A primeira nave espacial a sair do sistema solar levou mensagens gravadas num disco de ouro e cobre que continha: mensagens em línguas diferentes, músicas, sons de pássaros, imagens de um homem e uma mulher, imagens da Terra indicando a nossa localização, a sequência dos primeiros primos... A sequência foi considerada o que teria a maior probabilidade de ser compreendido.

Responderemos as outras perguntas na próxima thread então fiquem de olho... E já que semana que vem já é Natal, aproveitamos para desejar a todos vocês um Feliz Natal com uma

árvore enfeitada com os primeiros números da sequência de primos. [21] Tchau, tchau.

Figura 21 – Árvore de Natal com a sequência dos primeiros números primos

Fonte: Elaborada pelo autor.

Thread #9 26.12.2019

Na thread da semana passada iniciamos nossa conversa sobre os números primos e discutimos algumas questões. Vamos continuar falando sobre eles e ver quais surpresas esses números nos reservam. #MatThreadBR

Tendo uma definição tão "simples": número primo é todo número natural que pode ser dividido apenas por dois números o 1 e ele mesmo, nos parece que a busca por números dessa natureza é uma tarefa fácil, não é? Eratóstenes foi o matemático que mostrou uma forma de consegui-los.

Nascido em Cyrene, na Líbia em 276 a.C, Eratóstenes [22] foi um filósofo, astrônomo, matemático, geógrafo, historiador... Por um tempo foi chefe da Biblioteca de Alexandria e lá passava horas lendo sobre tudo.

Atribuímos a ele descobertas em diversas áreas: o diâmetro da Terra, o cálculo da distância entre a Terra e o Sol, um catálogo com 675 estrelas, a proposta da inclusão de um dia a mais no calendário que resultou no ano bissexto e o Crivo de Eratóstenes, objeto de nosso interesse.

O chamado Crivo de Eratóstenes é um método simples para descobrir números primos num intervalo. O primeiro passo consiste em criar uma lista indo do 2 até o número desejado, por exemplo, 120. Em seguida, vamos riscar todos os números que estiverem na tabuada do 2. (1 não é primo)

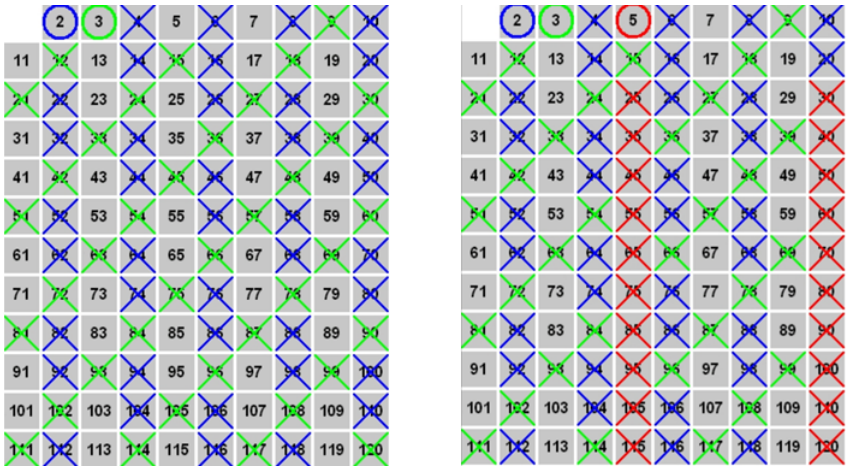
O nº 3, primeiro nº que não foi riscado é primo. Vamos riscar todos os nºs que estiverem na tabuada dele. O nº 5, é o próximo nº que não foi riscado, é primo. Então, vamos riscar todos

Figura 22 – Eratóstenes

Fonte: WikimediaCommons (a).

os n^{o}s que estiverem na tabuada dele [23]. Repetindo o processo, todo número não riscado é primo.

Figura 23 – Crivo com os múltiplos de 3 e 5 riscados



Fonte: Elaborada pelo autor.

A animação[7] a seguir mostra o passo a passo do que descrevemos. Esperamos que observá-la torne o entendimento do método algo mais fácil.

E aqui finalizamos a última thread do ano. Aproveitamos para desejar a todos um excelente ano novo. Que 2020 nos traga muitas descobertas importantes, não só na matemática, mas em todas as áreas do conhecimento. Até o ano que vem.

Thread #10 02.01.2020

Ano novo chegou e desejamos que vocês o tenham iniciado com ótima energia e muita

[7] Disponível em <https://upload.wikimedia.org/wikipedia/commons/8/8c/New_Animation_Sieve_of_Eratosthenes.gif>

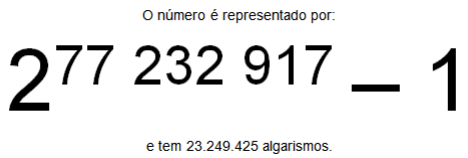
vontade de aprender. Que 2020 lhe inspire gentileza e que seja um ano de realizações. Vamos a primeira thread do ano?! Como determinamos se um número é primo? #MatThreadBR

Discutimos na thread anterior o Crivo de Eratóstenes. Essa ferramenta que data do período antes de Cristo nos ajudou a descobrir quem eram os números primos até um número limite.

Muitos matemáticos se dedicaram a criar tabelas com os números primos. E graças ao esforço de muitos no início do ano 1700 todos os números primos até o número 10 mil eram conhecidos. Em 1800 esse valor tinha crescido para todos os primos até 1 milhão.

Segundo o IMPA (Instituto de Matemática Pura e Aplicada) em 2017 foi encontrado o maior nº primo JÁ CATALOGADO [24] por matemáticos e ele tem mais de 23 milhões de algarismos! Se você escrevesse 5 dígitos por segundo, demoraria 54 dias para escreve-lo todo e usaria 118 km de papel.

Figura 24 – Maior número primo descoberto



Fonte: Elaborada pelo autor.

A pergunta que queremos responder: como é possível determinar se um número dado é primo ou não? Há um método que nos ajude? A resposta é sim!

Acompanhe o passo a passo com o exemplo: 907 é primo?

Se quiser acompanhar o cálculo, pegue sua calculadora ;) 1º passo: determine a raiz quadrada do número. A raiz quadrada de 907 é aproximadamente 30,17.

2º passo: verifique se o número pode ser dividido por algum primo menor do que a raiz. [25] 907 pode ser dividido por algum nº primo menor do que 30 (2, 3, 5, 7, 11, 13, 17, 19, 23, 29)? Faça os cálculos e veja se existe alguma divisão exata.

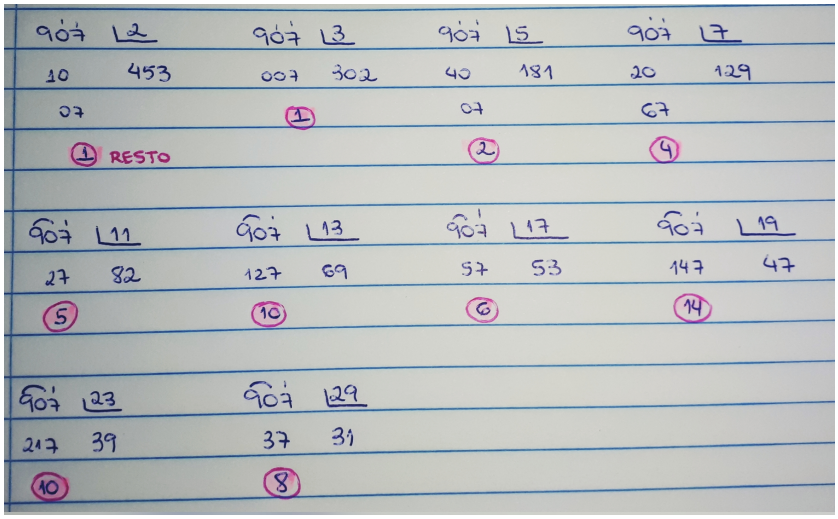
3º passo (conclusão): Se todas as divisões não forem exatas o nº é primo. Caso contrário, ele é um nº composto. Nenhum dos primos divide 907, logo ele é primo.

E aí, acha que consegue descobrir se um número é ou não primo? Então, vamos ao desafio!

DESAFIO: Verifique se o número 1091 é primo. Se tiver dúvida, entre em contato, pergunte. A resposta do desafio será postada na semana que vem.

Descobrindo se 1091 é primo: [26] 1º calcule sua raiz quadrada; 2º verifique quais são os nºs primos menores do que a raiz; 3º efetue as divisões de 1091 pelos nºs primos. Se nenhuma divisão for exata, o número é primo. Para ver as contas, olhe a imagem.

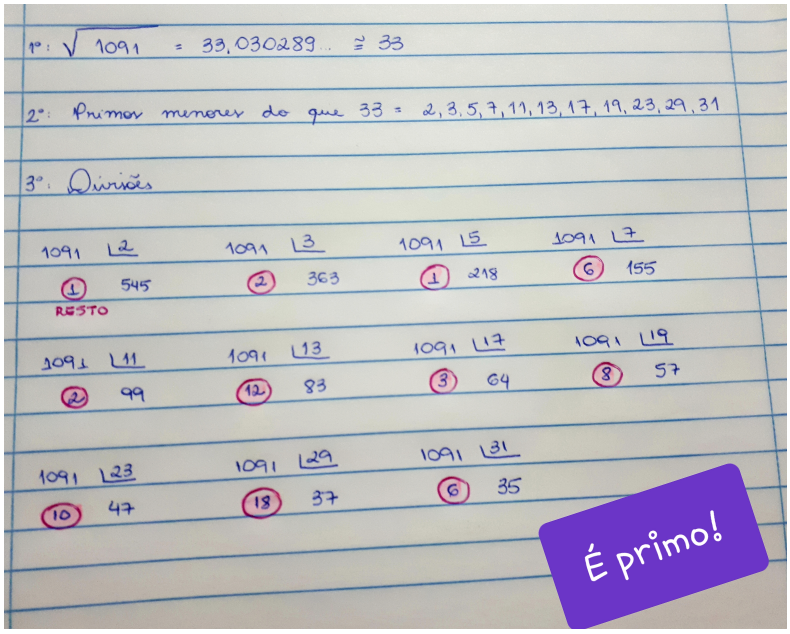
Figura 25 – Verificação do 2º passo



Fonte: Elaborada pelo autor.

1091 é o 182º número primo!

Figura 26 – Resolução do desafio



Fonte: Elaborada pelo autor.

Thread #11 09.01.2020

Na thread da semana passada falamos sobre a descoberta do maior número primo já conhecido pelo IMPA. Um nº com mais de 23 milhões de algarismos. Essa semana responderemos a pergunta: os nºs primos são infinitos? #MatThreadBR

Se analisarmos a sequência dos nºs primos perceberemos que eles não seguem um padrão. Ora eles estão bastante próximo uns dos outros ora estão distantes. Dá a impressão de que o nº de primos vai diminuindo até acabar, mas isso não é verdade. E dá para provar!

As 'provas matemáticas' são a base que os matemáticos usam para mostrar que as coisas são verdade. Não basta falar ou mostrar exemplos. Matemáticos da Grécia antiga já provavam teoremas e entre eles podemos citar Tales, Eudoxo, Aristóteles, Euclides... [27]

Figura 27 – Papiro de Rhind

Fonte: WikimediaCommons (b).

Euclides (300 a.C.) [28] merece atenção especial por ter reunido o conhecimento matemático acumulado por anos em seu livro 'Os Elementos'. O livro destaca-se não só por ser uma coleção de definições, axiomas, teoremas, mas pelas provas que o matemático apresentou para os teoremas.

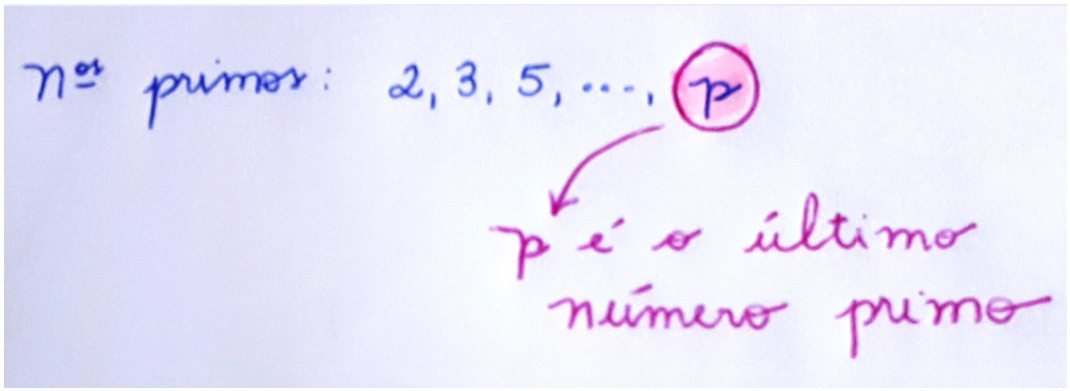
Figura 28 – Euclides de Alexandria

Fonte: WikimediaCommons (2005).

Existem várias técnicas para provar um teorema. Uma delas é a prova por contradição também conhecida por 'redução ao absurdo'. Vamos usá-la para provar que existem infinitos primos.

Vamos considerar que em algum momento os números primos acabam, ou seja, existe uma quantidade limitada de números primos. [29]

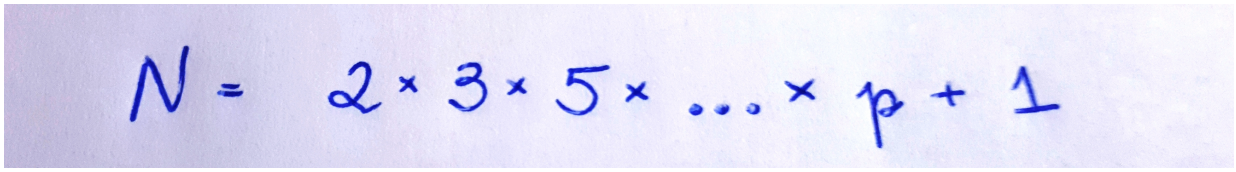
Figura 29 – Prova da infinitude dos números primos



Fonte: Elaborada pelo autor.

Vamos criar um número e chamá-lo de N. [30]

Figura 30 – Número N



Fonte: Elaborada pelo autor.

Por causa desse 1 que somamos ao nº N, sabemos que $2, 3, 5, \ldots, p$ não podem dividir o N (sempre sobrará resto 1). Logo, nenhum dos primos existentes divide esse nº que criamos.

Assim, há duas conclusões possíveis: (^{1}) N é um nº primo, (^{2}) N é divisível por um primo maior do que o p.

Se (^{1}) acontece, significa que encontramos um novo nº primo que não estava na lista. Se (^{2}) acontece, provamos que existe um primo maior do que o p. Nos dois casos mostramos que a ideia inicial de que os nºs primos são finitos estava errada. Logo, existem infinitos nºs primos.

Tcharaaaaam! Deu pra entender? Sei que pode parecer meio difícil. Sinceramente, algumas provas são complexas até pra gente que é da área. Porém com uma leitura cuidadosa, atenção às definições e vontade de entender a gente domina o assunto. Restaram dúvidas? Entre em contato.

Thread #12 16.01.2020

De todas as perguntas sobre números primos levantadas por nós do #MatThreadBR a única que ainda não foi respondida foi: para que servem? Uma das aplicações mais importantes

está ligada ao desenvolvimento da criptografia moderna, ou seja, a transmissão segura de dados em rede.

Antes de explicarmos como essa transmissão segura funciona, precisamos conhecer a "aritmética do relógio", conhecida pelos matemáticos como aritmética modular. Ela e os números primos terão um papel fundamental na criptografia.

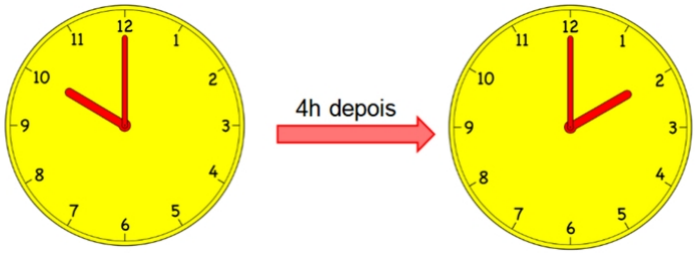
O matemático suíço Leonhard Euler foi o primeiro a abordar o tema em 1750. Cerca de 50 anos mais tarde o matemático alemão Carl Gauss desenvolveu o tema em seu livro Disquisitiones Arithmeticae. Foi contribuição de Gauss a ideia da calculadora-relógio. [31]

Figura 31 – Euler e Gauss

Fonte: Elaborada pelo autor.

A calculadora-relógio é realmente uma ideia, não havia meios de construí-la porque ela foi feita para trabalhar com números muito grandes. E ela funciona como um relógio comum. Se um relógio comum marca 10h e adicionarmos 4h, o ponteiro das horas avança até 2h. [32]

Figura 32 – Exemplo da soma na calculadora-relógio



Fonte: Elaborada pelo autor.

Assim, olhando para o relógio, temos: 10 + 4 = 2. Sabemos que 14h é igual à 2h. Fazemos esse tipo de cálculo todos os dias sem nem perceber ou nos surpreender. Os matemáticos generalizaram o conceito e encontraram outras aplicações para ele.

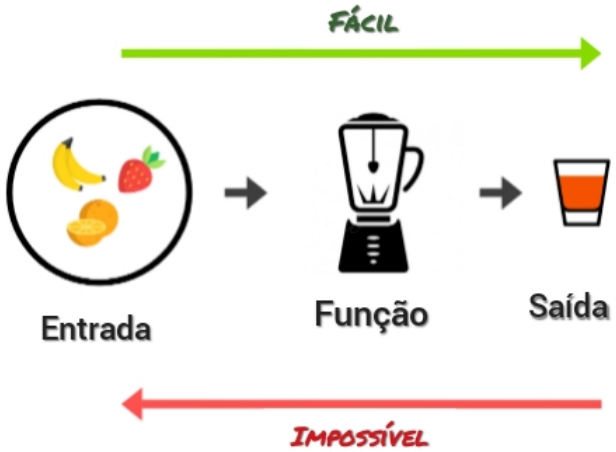
Podemos continuar a fazer somas nessa calculadora-relógio, tudo o que precisamos fazer é efetuar a adição e descobrir o valor do resto após a divisão por 12. Voltando ao nosso exemplo,

14 dividido por 12 tem resto 2, por isso, dizemos que $14 = 2$[8] (módulo 12).

Gauss percebeu que não era necessário usar apenas o relógio convencional de 12 horas. Ele poderia fazer cálculos com qualquer valor de "hora". Outro matemático, Fermat, descobriu propriedades interessantes se o "número de horas"escolhido fosse um número primo.

Funções calculadas com essa aritmética tem uma característica que em Ciência da Computação chamamos de função de mão única [33]: uma função que é fácil de calcular, dado um valor encontro um resultado; porém é difícil de inverter, dado o resultado é quase impossível descobrir o valor.

Figura 33 – Metáfora da função de mão única



Fonte: DataSeries (2019).

A segurança da nossa rede vem dessas duas ideias simples: os números primos e cálculos envolvendo a aritmética do relógio. A forma como isso é feito, fica para a próxima semana. Até lá∼

Thread #13 23.01.2020

Na thread anterior iniciamos a discussão segurança de dados na internet. Nossa intenção hoje é aprender um pouco sobre o desenvolvimento da criptografia de chave pública um dos métodos mais utilizados da criptografia atualmente em uso. #MatThreadBR

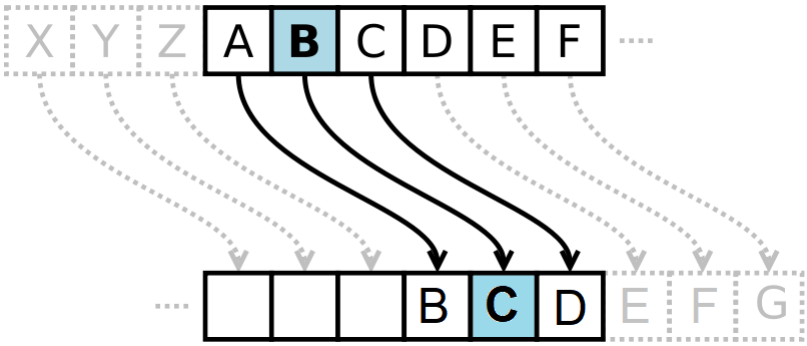
Vamos lembrar que na criptografia se queremos codificar uma mensagem precisamos contar a quem receberá a mensagem a forma como codificamos, é isso que chamamos de *chave*. E é este elemento que permite que a mensagem seja decifrada.

Num exemplo [34] bem simples, se eu resolvo enviar uma mensagem em que cada letra

[8] Note que aqui foi utilizado o símbolo de igual (=) ao invés do símbolo de congruência (≡), pois esse texto foi criado com finalidade de divulgação. Usar símbolos pouco conhecidos que necessitariam de mais explicações não se alinham com a nossa proposta.

do alfabeto foi trocada pela letra seguinte, eu preciso contar (de forma segura) essa informação para aquele que vai receber a mensagem, assim ele poderá desfazer o que eu fiz e ler a mensagem original.

Figura 34 – Cifra de César com uma deslocação de 3



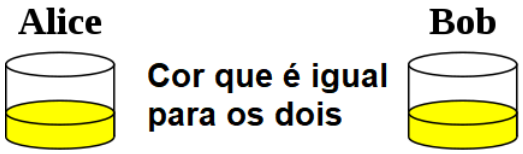
Fonte: Cepheus (2016).

Acontece que a troca da chave é uma das partes mais sensíveis do sistema, pois se descoberta por outra pessoa, permite que ela decodifique e entenda a mensagem. Seria possível fazer a troca da chave de forma segura sem que fosse pessoalmente?

Na década de 70 o matemático Diffie juntou-se aos criptógrafos Hellman e Merkle para pesquisar uma maneira de fazer isso. Vamos usar personagens fictícios: Alice, Bob e Eva e cores para explicar de uma maneira simples.

Suponha que Alice e Bob queiram combinar uma chave e Eva esteja decidida a descobri-la. Alice e Bob escolhem uma cor pública qualquer, ou seja, uma informação que Eva também pode descobrir: amarelo. [35]

Figura 35 – Ilustração da ideia da troca de chaves Diffie-Hellman - passo 1



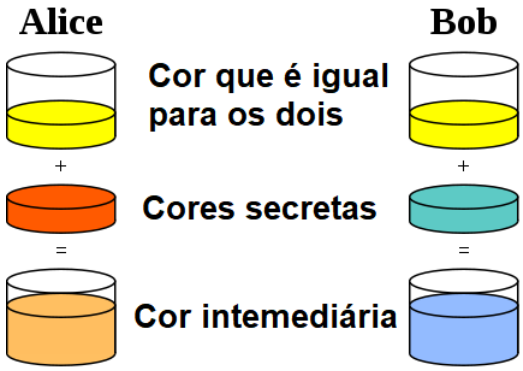
Fonte: Vinck (2011, tradução nossa).

Depois, cada um escolhe uma cor secreta. Alice escolhe laranja e Bob escolhe azul. Agora, eles misturam a cor secreta com o amarelo. Alice obtém um balde de tinta laranja claro e Bob azul claro[9] [36]

Eles trocam essas misturas por um meio não seguro. Depois, acrescentam a cor secreta que possuem a mistura que receberam. Pronto, eles conseguiram uma cor secreta, que só eles dois conhecem. [37]

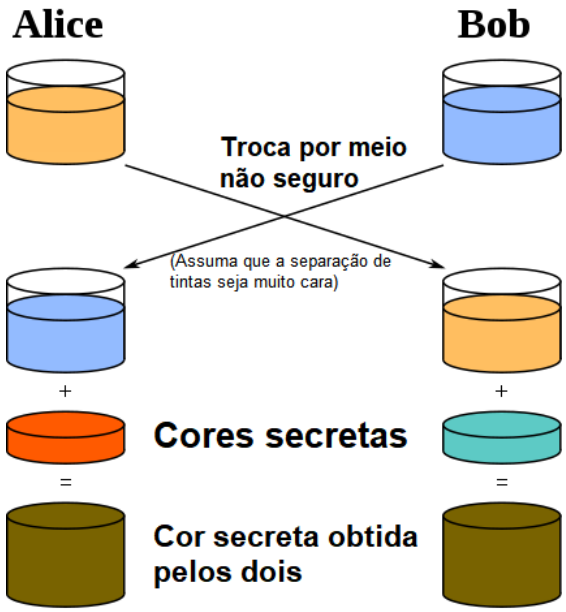
[9] A mistura de amarelo e azul resulta em verde. Deixamos azul claro no texto a fim de facilitar a relação com a figura.

Figura 36 – Ilustração da ideia da troca de chaves Diffie-Hellman - passo 2



Fonte: Vinck (2011, tradução nossa).

Figura 37 – Ilustração da ideia da troca de chaves Diffie-Hellman - passo 3



Fonte: Vinck (2011, tradução nossa).

Essa seria a chave privada que eles obtiveram, ainda que utilizando um meio não seguro. Mesmo que Eva consiga colocar as mãos na mistura intermediária, como ela não conhece as cores de Alice e Bob não é possível que ela descubra a cor final.

Na realidade o esquema das cores foi substituído por uma função matemática [38] que era fácil de fazer e difícil de desfazer. O esquema ficou conhecido como Diffie-Hellman-Merkle e provou que era possível que Alice e Bob combinassem um segredo através de uma conversa pública.

Era necessário agora uma forma de distribuição das chaves. Neste ponto faltava pouco para a criptografia RSA. Falaremos sobre ela na semana que vem.

Para quem quiser saber mais: Esse vídeo explica o passo a passo de Alice e Bob para a

Figura 38 – Função Y^n

Função: Y^n (mod P)

A função escolhida funciona de
acordo com a aritmética do
relógio citada na thread anterior

Fonte: Elaborada pelo autor.

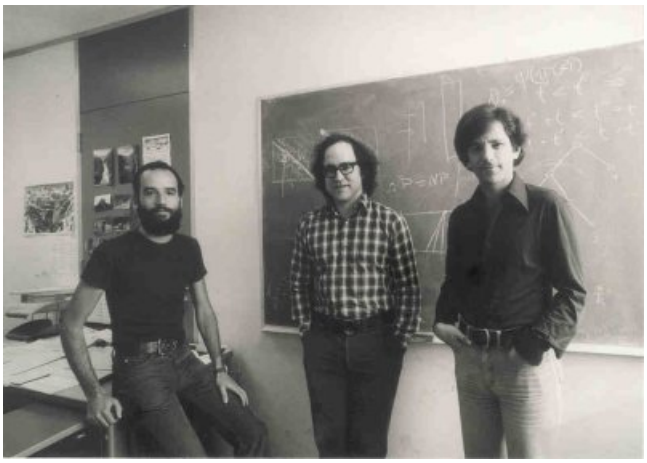
mistura das tintas: Secret Key Exchange (Diffie-Hellman) - Computerphile[10]

Thread #14 30.01.2020

Tornou-se cada vez mais comum compartilharmos nossas informações pessoais em situações diárias: transações bancárias, compras pela internet, cartões, senhas, caixas eletrônicos. Confiamos que o ambiente é seguro. Mas o que garante que nossos dados estejam protegidos? #MatThreadBR

Na década de 70 os matemáticos Ron Rivert, Adi Shamir e Leonard Adleman [39], pesquisadores do Instituto de Tecnologia de Massachusetts (MIT) foram em busca de um método que garantisse a privacidade no uso da internet e foi assim que desenvolveram o algoritmo RSA.

Figura 39 – Adi Shamir (1952-), Ron Rivest (1947-), e Len Adleman (1945-)



Fonte: Bauer (2013, p. 408).

O algoritmo RSA pode ser chamado de criptografia assimétrica uma vez que usa duas chaves: uma para codificar (chamada chave pública) e outra para decifrar (chamada chave privada).

Exemplo: A loja MaT decidiu vender online e vai usar o RSA para proteger os dados dos clientes. A loja cria sua chave pública e sua chave privada. A chave pública será distribuída

[10] Disponível em <https://www.youtube.com/watch?v=NmM9HA2MQGI>

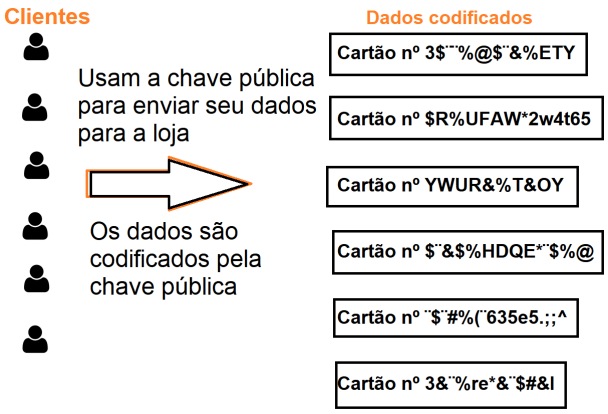
para os clientes, todos que comprarem na loja usarão a mesma chave pública para enviar as informações. [40]

Figura 40 – Ilustração da chave pública

Fonte: Elaborada pelo autor.

Usando a chave pública da loja o cliente codifica seus dados (nome completo, cpf, número do cartão de crédito, endereço) e envia as informações para a loja. [41]

Figura 41 – Ilustração da codificação através da chave pública



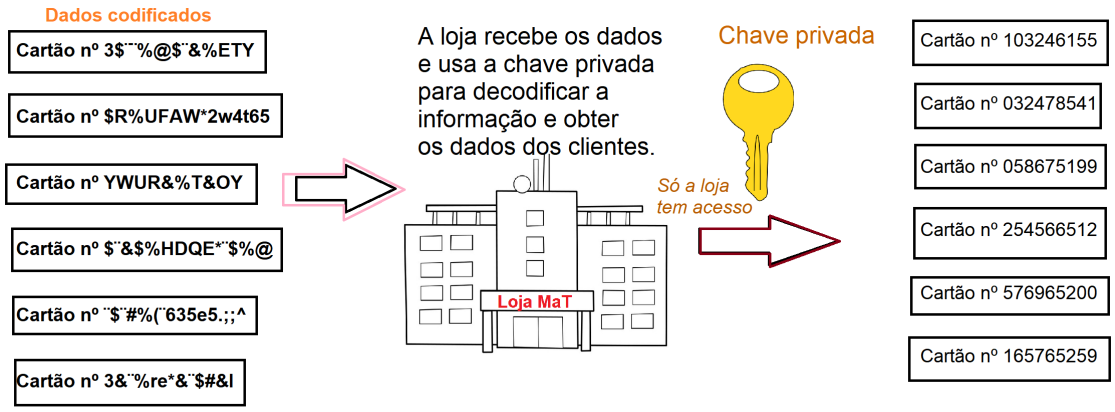
Fonte: Elaborada pelo autor.

A loja decifra as informações recebidas usando sua chave privada. Como ela é a única que tem acesso à chave privada, mesmo que as informações do cliente sejam interceptadas no meio da transação, serão necessários cálculos extremamente demorados para que os dados sejam decifrados. [42]

Com o algoritmo RSA a chave de codificação para qualquer destinatário pode ser tornada pública. Lojas, bancos, qualquer um pode divulgar sua chave pública e receber mensagens codificadas por ela de forma que só serão decifradas depois do uso da chave particular que é secreta.

A matemática envolvida nesse algoritmo incrível fica para a próxima semana. Até lá.

Figura 42 – Ilustração do uso da chave privada



Fonte: Elaborada pelo autor.

Thread #15 06.02.2020

Hoje é dia de explicar a matemática envolvida no algoritmo de chave pública, RSA. Os principais conceitos são os nºs primos e a 'aritmética do relógio/dos restos'. Voltemos a loja MaT p/ responder: como são criadas as chaves pública e privada? #MatThreadBR

Primeiro a loja MaT escolhe dois nºs primos (suficientemente grandes), vamos chamá-los de p e q e os multiplica. O resultado dessa multiplicação é a chave pública, vamos chamá-la de X. O valor X será publicado, os valores de p e q serão de conhecimento apenas da loja.

Qualquer pessoa/empresa pode usar a chave pública X da loja MaT para codificar uma informação. Entretanto, sem conhecer os valores de p e q, ninguém será capaz de decifrar a mensagem. Vamos acompanhar o passo a passo com um exemplo. Usaremos p = 2 e q = 5. [43]

Depois de calculado X (X = 10), a loja escolhe um número E que não tenha fatores comuns com $(p-1)\cdot(q-1)$. Pelos cálculos abaixo, escolhemos E = 3.

p - 1 =	q - 1 =
2 - 1 =	5 - 1 =
1	4

Assim, $(p-1)\cdot(q-1) = 1\cdot 4 = 4$

E não pode ter fatores comuns com 4. Vamos escolher E = 3.

Para cifrar uma mensagem ela primeiro precisa ser transformada em número. Vamos usar a tabela de conversão abaixo. Queremos enviar a mensagem AMORAS, transformando-a em código numérico temos 3 7 8 6 3 1 (isso é o que vamos codificar) [5]

Para codificar usamos a chave pública X = 10 e o E = 3, da seguinte forma: Vamos elevar todos os números usando o expoente E = 3, e calcular o resto da divisão por X = 10

Figura 43 – Ilustração do uso da chave pública

Fonte: Elaborada pelo autor.

Tabela 5 – Exemplo de tabela de conversão

S	O	A	E	C	R	M	O	V
1	2	3	4	5	6	7	8	9

Fonte: Elaborada pelo autor.

(na matemática o cálculo do resto da divisão por qualquer número é chamado congruência ou aritmética dos restos). [44]

Logo, 7 3 2 6 7 1 é a mensagem cifrada que será enviada. Para decifrar a mensagem, a loja MaT precisará da chave privada, vamos chamá-la de D. Os cálculos para se chegar ao valor de D estão na figura abaixo. D = 3.

$$E \cdot D \equiv 1(mod(p-1)\cdot(q-1))$$

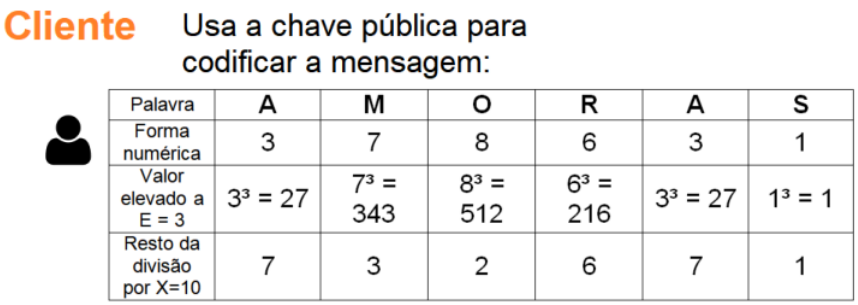
$$3 \cdot D \equiv 1(mod4)$$

Procuramos um número que ao ser multiplicado por 3 e depois dividido por 4 tenha resto 1. O número 9 dividido por 4 tem resto 1. Assim, $D = 3$.

Decifrando: Vamos elevar todos os números usando o expoente E = 3 (foi uma coincidência o valor de D e E serem iguais ;)), e calcular o resto da divisão por X = 10. [45]

A segurança da RSA está no fato de que é mto difícil descobrir os valores de p e q, uma vez que geralmente são escolhidos primos com mais de 100 algarismos, o que resulta em uma chave pública X com uns 200 algarismos. Fatorar um nº grande requer tempo, mesmo usando um computador.

Figura 44 – Ilustração de codificação usando a chave pública



Palavra	A	M	O	R	A	S
Forma numérica	3	7	8	6	3	1
Valor elevado a E = 3	$3^3 = 27$	$7^3 = 343$	$8^3 = 512$	$6^3 = 216$	$3^3 = 27$	$1^3 = 1$
Resto da divisão por X=10	7	3	2	6	7	1

Fonte: Elaborada pelo autor.

Figura 45 – Ilustração de decodificação usando a chave privada

Texto cifrado	7	3	2	6	7	1
Valor elevado a D = 3	$7^3 = 343$	$3^3 = 27$	$2^3 = 8$	$6^3 = 216$	$7^3 = 343$	$1^3 = 1$
Resto da divisão por X=10	3	7	8	6	3	1
Texto DECODIFICADO	**A**	**M**	**O**	**R**	**A**	**S**

Fonte: Elaborada pelo autor.

Em 1977, os criadores da RSA lançaram um desafio. Eles publicaram na Scientific American uma chave pública com 129 algarismos e desafiaram os leitores a descobrirem p e q. Dezessete anos depois, uma equipe de 600 voluntários anunciaram os valores de p e q.

X = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541

p = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577

q = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533

O que vocês acharam??

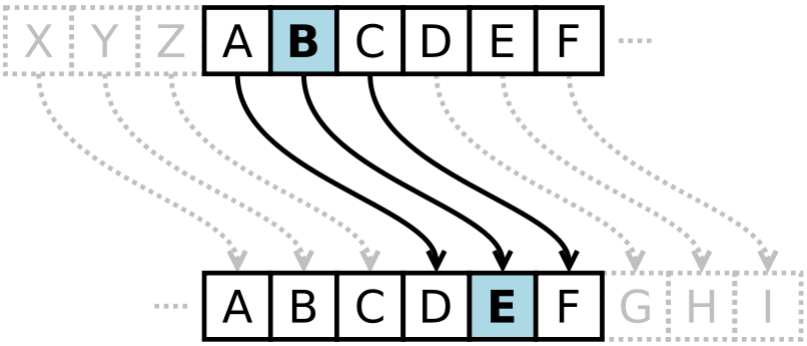
Thread #16 13.02.2020

Na thread de hoje vamos falar um pouquinho de criptoanálise que é a arte de tentar descobrir o que está escrito em um texto codificado sem conhecer a chave que o decodifica. #MatThreadBR #Matemática #DivulgaçãoCientífica

Durante muito tempo as pessoas usaram a criptografia de substituição achando que ela era um meio seguro de comunicação. Nesse tipo de criptografia, você troca as letras do alfabeto

original por outra do alfabeto cifrado. A cifra de César é um exemplo. [46]

Figura 46 – Cifra de César com uma deslocação de 3



Fonte: Cepheus (2016).

A cifra de César data do período antes de Cristo e apenas no século IX que os árabes mostraram que era possível quebrar esse exemplo de cifra. Foram eles que criaram a criptoanálise e apresentaram a análise de frequência das letras, a ferramenta que quebra a cifra de substituição.

Segundo seus estudos, se conhecermos o idioma do texto cifrado, haverá diversos padrões da língua como as letras que mais aparecem, os encontros consonantais mais frequentes, letras que não podem vir seguidas de outras, entre outros que se manterão após o texto ser criptografado.

Assim, se um criptoanalista estudar o texto codificado de seu interesse, ele pode calcular a porcentagem com que aparecem cada uma das letras e comparar com a porcentagem do alfabeto original. Na figura abaixo temos a frequência das letras na língua inglesa. [47]

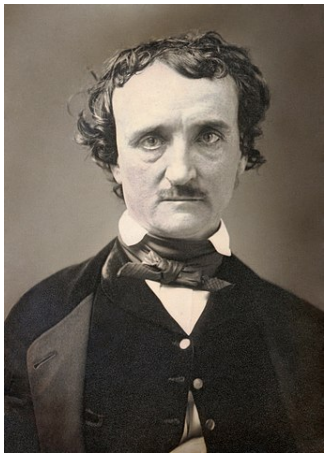
Figura 47 – Exemplo das estatísticas da língua inglesa

Letra	Frequência relativa (%)	Letra	Frequência relativa (%)
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.3	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.2	W	2.4
K	0.8	X	0.2
L	4.0	Y	2.0
M	2.4	Z	0.1

Fonte: Bauer (2013, p. 24, tradução nossa).

O escritor Edgar Allan Poe [48] usou a análise de frequência das letras para fascinar seus leitores. Em 1839, publicou um artigo explicando a cifra de substituição e desafiou os leitores do jornal a enviarem qualquer mensagem usando a cifra que ele decifraria todas. E assim ele fez!

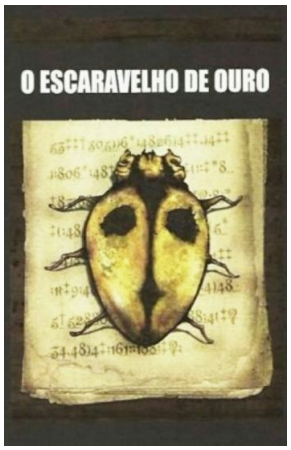
Figura 48 – Edgar Allan Poe



Fonte: WikimediaCommons (1849).

Ele foi chamado por seus fãs de ‘o mais profundo e habilidoso criptógrafo que já vivera’. Todos queriam saber como ele desvendava as cartas enviadas; então, em 1843, Poe escreveu um conto que explicava seu segredo: “O escaravelho de ouro”. [49]

Figura 49 – Capa do livro



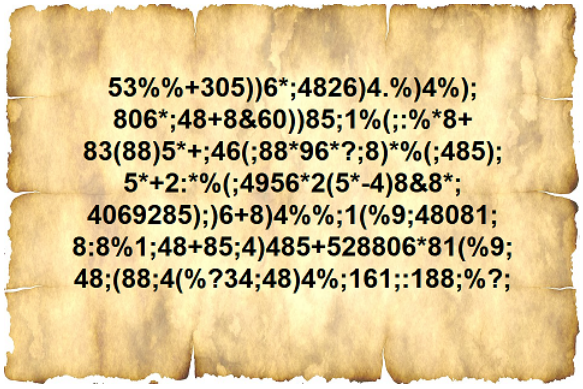
Fonte: VDocuments (2014).

Criptógrafos profissionais consideram este o melhor exemplo de literatura de ficção sobre o assunto. O conto narra a história de Legrand que descobre um escaravelho e ao apanhá-lo acaba se envolvendo em uma aventura de caça ao tesouro. [50]

Ele descobre um texto codificado e para entendê-lo, usa a análise da frequência das letras. No conto o autor descreve o passo a passo utilizado para decifrar as instruções que levaram Legrand a um tesouro de grande valor.

Nossa história é marcada pelo conflito incessante entre fazedores e quebradores de código. Quando um tem a vantagem o outro se supera e retorna a cena, mais forte. “A ingenuidade humana não pode inventar uma cifra que a ingenuidade humana não pode resolver” – Poe.

Figura 50 – Pergaminho com a mensagem criptografada



Fonte: Elaborada pelo autor.

Thread #17 20.02.2020

Já falamos sobre a cifra de substituição, que é trocar as letras do alfabeto original por outras do alfabeto cifrado. Contamos também que os árabes, através da análise da frequência das letras, conseguiram decifrar cifras desse tipo. Que tipo de cifras vieram depois? #MatThreadBR

Naquela época, todas as cifras de substituição usavam apenas um alfabeto cifrado. Leon Battista Alberti propôs o uso de dois ou mais alfabetos cifrados, usados de maneira alternada, de modo a confundir criptoanalistas em potencial. Veja um exemplo abaixo [51]:

Figura 51 – Exemplo da cifra de Alberti

Alfabeto Normal	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Alfabeto Cifrado 1	C	Q	M	Y	N	D	S	E	V	L	Z	B	F	G	H	I	J	K	P	O	R	T	U	W	X	A
Alfabeto Cifrado 2	S	D	F	G	H	J	K	L	P	O	I	U	Y	T	M	N	B	R	V	E	C	W	X	A	W	Q

Fonte: Elaborada pelo autor.

Para codificar a mensagem ENVIE TROPAS faríamos assim: a 1ª letra seria cifrada usando o alfabeto 1, a 2ª seria cifrada usando o alfabeto 2, a 3ª usaria o alfabeto 1, para a 4ª letra usaríamos o alfabeto 2 e assim continuaríamos até terminarmos a mensagem [52].

A vantagem do sistema criado por Alberti é que letras repetidas na mensagem cifrada podem representar letras diferentes no alfabeto original. No exemplo, a letra T representa tanto N quanto V; o mesmo ocorre com a letra P que representa I e S.

Embora essa cifra representasse um avanço, Alberti não conseguiu desenvolver sua ideia e torna-la um sistema de cifras. Coube a Blaise de Vigenère examinar as ideias de Alberti e criar uma nova cifra, bastante poderosa.

O método é conhecido como ‘quadrado de Vigenère’ [53] e usa 26 diferentes alfabetos cifrados para criar a mensagem codificada. Cada alfabeto cifrado é criado deslocando-se uma

Figura 52 – Exemplo de uso da cifra de Alberti

Mensagem	**E**	**N**	**V**	**I**	**E**	T	R	O	P	A	S
Cifra 1	N		T		N		K		I		P
Cifra 2		T		P		E		M		S	
Mensagem cifrada	N	T	T	P	N	E	K	M	I	S	P

Fonte: Elaborada pelo autor.

letra em relação ao alfabeto anterior.

Figura 53 – Quadrado de Vigenère

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2007, p. 66).

Podemos usar esse método de forma semelhante ao que fizemos com Alberti e tomar a 1ª letra no alfabeto 1, a 2ª no alfabeto 2 e assim por diante. Se quisermos podemos inventar outra ordem e, por exemplo, tomar a 1ª letra no alfabeto 5, a 2ª no alfabeto 15...

Ao usarmos o alfabeto de forma aleatória, teríamos um problema na hora de decodificar a mensagem, seria difícil para o receptor 'adivinhar' quais os alfabetos foram usados. Por isso, podia-se usar junto ao quadrado de Vigenère uma palavra-chave.

Vamos cifrar a mensagem ENVIE TROPAS usando a palavra chave VISTO. Primeiro devemos escrever a palavra-chave repetidamente em cima da mensagem original. [54]

Figura 54 – Usando o quadrado de Vigenère - passo 1

Palavra-chave	**V**	**I**	**S**	**T**	**O**	**V**	**I**	**S**	**T**	**O**	**V**
Mensagem original	**E**	**N**	**V**	**I**	**E**	T	R	O	P	A	S

Fonte: Elaborada pelo autor.

Codificando: a 1ª letra da mensagem é E, olhando a palavra chave E deve ser codificado usando o alfabeto que começa com V, logo E vira Z. A próxima letra é N, observando a palavra-chave, N deve ser codificado usando o alfabeto que começa com I, logo N vira V. E assim por diante. [55]

Figura 55 – Usando o quadrado de Vigenère - passo 2

Palavra-chave	**V**	**I**	**S**	**T**	**O**	**V**	**I**	**S**	**T**	**O**	**V**
Mensagem original	**E**	**N**	**V**	**I**	**E**	T	R	O	P	A	S
Mensagem cifrada	Z	V	N	B	S	O	Z	G	I	O	N

Fonte: Elaborada pelo autor.

O quadrado de Vigenère, também conhecido como Cifra Indecifrável, era imune a análise de frequência das letras e como possuía um enorme nº de palavras-chaves tornava a tarefa do criptoanalista praticamente impossível, uma vez que o nº de opções é grande demais.

Embora o sistema fosse forte e garantisse segurança, ele não foi adotado pelos secretários de segurança da Europa depois de criado. Cifrar e decifrar mensagens usando essa cifra era muito trabalhoso e levava tempo. Essa cifra só viria a ser usada cerca de dois séculos depois.

Vejo vocês na semana que vem∼

7.2.2 Escrevendo threads para a MatThreadBR

Neste espaço vamos expor a forma como escrevemos nossas postagens. Ressaltamos que isso não é, de jeito algum, um guia definitivo de como se fazer uma *thread*; as observações aqui descritas apenas refletem a nossa experiência.

Vale lembrar que essas postagens podem ser feitas por qualquer pessoa, não é necessário ter formação em matemática para escrever sobre algum conteúdo ou curiosidade que ache interessante, mas é fundamental consultar referências confiáveis antes de publicar.

- *Sobre o tema das postagens:* Aqui cabe qualquer tema que você julgue interessante. É válido explorar tópicos que mostrem a aplicação da matemática em outros campos ou procurar conexões com algum assunto que esteja sendo bastante discutido pela sociedade no momento e que tenha a ver com a matemática. Postagens que mostrem a utilidade da matéria são pertinentes.

- *Sobre a escrita do texto:* Escreva seu texto em um editor de texto e só depois o estruture no *Twitter*. Escrever dessa forma facilita edições caso necessário. Você pode usar a ferramenta 'contar palavras/caracteres' para não ultrapassar o limite de 280 caracteres.

- *Sobre o tamanho da thread:* A *thread* não pode ser muito longa, pois o *Twitter* foi projetado para postagens curtas. Nessa plataforma, se a publicação ficar muito longa o leitor pode perder o interesse e abandonar a leitura. Em nossa experiência, escrevemos *threads* com cerca de 10 *tweets*. Usar muito mais do que isso pode indicar que você está se alongando demais, escreva de forma simples e objetiva.

- *Sobre a hashtag:* Não esqueça de colocar a *hashtag* #MatThreadBR no primeiro *tweet*, pois essa é a maneira de garantir que sua postagem aparecerá nas buscas por nossa *hashtag*.

- *Sobre a linguagem:* Atente-se a linguagem a ser usada. Por se tratar de um ambiente informal evite fazer uso de palavras muito técnicas. Seu uso pode fazer com que o leitor perca o interesse em ler a postagem por achar que o tema tratado é difícil demais para que ele compreenda. Utilize uma linguagem acessível, pois a ideia é atingir o maior número de pessoas possível. Sempre que conseguir inclua metáforas no text, por exemplo, ao se referir a medidas muito grandes diga que tal medida equivale a tantos campos de futebol. Faça com que o texto seja compreensível.

- *Sobre os conteúdos multimídia e interativos:* Faça uso de imagens, gifs e vídeos. Sempre que possível use outros meios para explicar o tema, isso pode ser um atrativo, uma 'isca' para atrair leitores. Você pode criar imagens com exemplos, criar gifs, indicar vídeos e links para outras referências. Pode inclusive adicionar um gif ou figura que seja divertido a fim de acrescentar certa leveza a leitura e incentivar o leitor a continuar lendo.

Finalmente, com a prática cada um descobre sua própria maneira de escrever. Essas são apenas algumas informações que podem nortear quem tiver interesse em realizar seu primeiro contato com a divulgação científica no *Twitter*.

7.3 Discussão de resultados

Segundo Costa (2014) "A divulgação científica tem um papel importante para que a população adquira conhecimento sobre ciência e conheça o quanto ela está presente em seu entorno.". Neste contexto, criamos o perfil #MatThreadBR no *Twitter* para falar de Matemática

de um modo mais informal levando-a para um ambiente virtual onde fala-se pouco de ciência básica. A ideia é mostrar às pessoas a matemática através de uma perspectiva diferente daquela vista na escola.

Uma das maiores barreiras encontradas para divulgar Matemática é a forma desconectada com que os seus conteúdos são apresentados. Parece que nos falta um modo de mostrar que a matemática é uma ciência viva, atual e significativa. Segundo D'Ambrósio (1999?) "o problema maior do ensino de ciências e matemática é o fato das mesmas serem apresentadas de forma desinteressante, obsoleta e inútil, e isso dói para o jovem.". Algumas outras áreas das Ciências estão realizando postagens no *Twitter* com sucesso. Especificamente na área de Matemática podemos encontrar alguns vídeos na plataforma *YouTube*, mas em sua maioria eles explicam os conteúdos usando o formato vídeo-aula ou palestra. Porém, no *Twitter*, não encontramos outras páginas de divulgação matemática especificamente.

Acreditamos que a iniciativa de realizar postagens no *Twitter* promove uma cultura de levar assuntos a respeito de Matemática para as redes sociais e aproximá-las do dia-a-dia de um público variável. Desta forma, esperamos que a #MatThreadBR possa influenciar outros a falar de matemática a fim de mostrar sua relevância, beleza, importância e, acima de tudo, que iniciativas como essa sirvam para fazer com que as pessoas falem de matemática e usem seus conhecimentos para atuar de maneira responsável na sociedade.

Apesar de aparentemente o impacto inicial no *Twitter*, medido através de visualizações, ter sido pequeno, o perfil será mantido ativo e fomentado com novos projetos, tornando-se um repositório mais informal de diversos temas de Matemática. Através deste trabalho contínuo podemos aperfeiçoar vários aspectos sobre a abordagem de divulgação Matemática em redes sociais, além de realizar cooperações com outros perfis de Ciências.

CAPÍTULO

8

CONSIDERAÇÕES FINAIS

Neste trabalho nos propusemos a explorar a contextualização no ensino de alguns conteúdos de Matemática bem como a divulgação da matemática em redes sociais. Para isso fomos em busca de um tema que parecesse interessante aos olhos dos estudantes e do público em geral. A segurança dos dados na internet, em nossa opinião, era um assunto que poderia prender a atenção das pessoas e atraí-las para a matéria.

Iniciamos nosso estudo da história da criptografia e nos deparamos com uma variedade de histórias que mostravam astúcia por parte daqueles que dominavam a arte de esconder e codificar mensagens. Em um esforço de combater tal poder, outros estudiosos esforçaram-se em encontrar uma maneira de decifrar essas mensagens e dar fim a segurança de tais métodos. Percebemos que nossa história pode ser contada através do enfrentamento constante dos que cifram e dos que decifram os códigos.

Depois de estudarmos sobre a história da criptografia de Heródoto até a criptografia RSA, realizamos uma revisão teórica sobre o conteúdo. Como nosso objetivo em termos de divulgação científica era contar as principais histórias sobre a criptografia até a RSA, nos atentamos aos conteúdos necessários para o entendimento destes temas. Nos pusemos a estudar os números inteiros, suas propriedades, os números primos, o Teorema Fundamental da Aritmética e a congruência.

De posse da história e da teoria, refletimos sobre nossa experiência como professor e reavaliamos a abordagem de alguns conteúdos, pensando em como introduzi-los de modo que a criptografia funcionasse como um fator de incentivo. Como resultado, foram desenvolvidas atividades voltadas tanto para o Ensino Fundamental quanto para o Ensino Médio. Tais atividades foram pensadas com o objetivo de aumentar a participação dos alunos. Ao deixarem que expressem suas experiências anteriores e contribuam para o processo da aula acreditamos que a compreensão do conteúdo acontecerá de forma mais natural. A busca pela contextualização dos conteúdos se deu pela perspectiva de facilitar a abstração dos mesmos.

Esperamos que este material possa ajudar e inspirar outros professores a tentarem ensinar este e outros conteúdos de forma diferente.

Paralelamente, nos voltamos para uma atividade de divulgação científica em redes sociais, pois queremos dividir com outras pessoas o encantamento que sentimos pela matemática e, mais do que isso, mostrar sua importância. Por causa disso, estudamos a direção que alguns divulgadores científicos têm tomado e iniciamos nossa jornada criando pequenos textos informativos e postando-os no *Twitter*.

Nosso envolvimento em divulgação científica ainda é muito recente, mas esperamos que a longo prazo, possamos ajudar as pessoas a enxergar o valor da matemática e contribuir para a mudança dessa visão de ciência difícil e inalcansável. Em conjunto com outras ciências, acreditamos que este trabalho de divulgação em redes, a longo prazo, tem a capacidade de ampliar as discussões a respeito de Ciência, tornando as pessoas mais informadas e conscientes e que isso se reflita em decisões futuras que afetarão nossa Sociedade.

REFERÊNCIAS

ANTON, H.; RORRES, C. **Álgebra linear com aplicações**. 8. ed. Porto Alegre: Bookman, 2001. Citado nas páginas 28, 169 e 172.

BAUER, C. P. **Secret history: the story of cryptology**. [S.l.]: CRC Press, 2013. Citado nas páginas 24, 80, 82, 116 e 121.

BRASIL. **Parâmetros Curriculares Nacionais: matemática**. Brasília, 1997. Citado na página 80.

____. Parâmetros curriculares nacionais. 3º e 4º ciclos do ensino fundamental: matemática. MEC/SEF, Brasília, 1998. Citado nas páginas 76, 78 e 84.

CEPHEUS. 2016. Disponível em: <https://commons.wikimedia.org/wiki/File:Caesar3.svg>. Acesso em: 28 nov. 2019. Citado nas páginas 100, 114 e 121.

CHALON, A. E. c1840. Science Museum Group Collection. Disponível em: <https://collection.sciencemuseumgroup.org.uk/objects/co67823>. Acesso em: 31 out. 2019. Citado na página 94.

COSTA, V. A importância da divulgação científica. **Sociedade brasileira para o progresso da ciência**, 2014. Disponível em: <http://portal.sbpcnet.org.br/noticias/tunel-da-cienciaquebraa-importancia-da-divulgacao-cientifica/>. Acesso em: 13 mar. 2020. Citado na página 126.

DAHER, A. F. B. Aluno e professor: protagonistas do processo de aprendizagem. 2006. Disponível em: <http://www.campogrande.ms.gov.br/semed/wp-content/uploads/sites/5/2017/03/817alunoeprofessor.pdf>. Acesso em: 2 jan. 2020. Citado na página 76.

D'AMBRÓSIO, U. Informática, ciências e matemática. 1999? Disponível em: <http://smeduquedecaxias.rj.gov.br/nead/Biblioteca/Forma%C3%A7%C3%A3o%20Continuada/Tecnologia/matem%C3%A1tica%20ci%C3%AAncia%20e%20tecnologia.pdf>. Acesso em: 13 mar. 2020. Citado na página 127.

DANTE, L. R. **Matemática - Série novo ensino médio**. São Paulo: Editora Ática, 2005. Citado na página 76.

DATASERIES. 2019. Disponível em: <https://medium.com/dataseries/millennium-breakthrough-one-way-functions-cannot-exist-a7188186dd2f>. Acesso em: 16 jan. 2020. Citado na página 113.

FLICKR. **Enigma Machine**. 2018. School of Mathematics - University of Manchester. Disponível em: <https://www.flickr.com/photos/manunimaths/44960892745>. Acesso em: 22 nov. 2019. Citado nas páginas 45 e 104.

GANASSOLI, A. P.; SCHANKOSKI, F. R. **Criptografia e Matemática**. Dissertação (Mestrado) — Mestrado Profissional em Matemática em Rede Nacional, Paraná, 2015. Citado na página 75.

HALICKI, J. 2016. Disponível em: <https://commons.wikimedia.org/wiki/File:2016_Minox_C_8.jpg>. Acesso em: 14 nov. 2019. Citado na página 97.

HARTWELL, S. Disponível em: <https://commons.wikimedia.org/wiki/File:TuringBombeBletchleyPark.jpg>. Acesso em: 12 dez. 2019. Citado na página 105.

HEFEZ, A. **Aritmética: coleção PROFMAT**. Rio de Janeiro: SBM, 2014. Citado nas páginas 59 e 68.

HILLIARD, N. 1578. National Portrait Gallery, London. Disponível em: <https://www.npg.org.uk/collections/search/portrait/mw04273/Mary-Queen-of-Scots?> Acesso em: 5 dez. 2019. Citado na página 101.

HOOK, D.; NORMAN, J. **Origins of cyberspace: a library on the history of computing, networking, and telecommunications**. Novato, CA, USA: Jeremy Norman Co, 2002. Citado na página 94.

LEVINE, A. 2012. Disponível em: <https://www.flickr.com/photos/cogdog/7239016106/in/photostream/>. Acesso em: 5 dez. 2019. Citado na página 102.

LOPES, C. E. O ensino da estatística e da probabilidade na educação básica e a formação dos professores. **Cadernos Cedes**, SciELO Brasil, v. 28, n. 74, p. 57–73, 2008. Citado na página 79.

LUKATS, H. 2015. Disponível em: <https://commons.wikimedia.org/wiki/File:Whatsapp_texting.jpg>. Acesso em: 21 nov. 2019. Citado na página 98.

MASSARANI, L.; MOREIRA, I. C. Aspectos históricos dadivulgação científica no brasil. In: **Ciência e público: caminhos da divulgação científica no Brasil**. Rio de Janeiro: Casa da Ciência/UFRJ, 2002. Citado nas páginas 90 e 91.

MORGADO, A. C.; CARVALHO, J. B. P.; CARVALHO, P. C. P.; FERNANDEZ, P. **Análise Combinatória e Probabilidade: com as soluções dos exercícios**. Rio de Janeiro: SBM, 2006. Citado na página 77.

OLIVEIRA, W. F. **Uma proposta para ampliar a perspectiva de professores e alunos em relação ao estudo de matrizes**. Dissertação (Mestrado) — Mestrado Profissional em Matemática em Rede Nacional, São José do Rio Preto, 2017. Citado na página 86.

PEÑA, J. A. **Álgebra en todas partes**. México: Fondo de Cultura Económica, 1999. Citado na página 24.

PONTE, G. 2018. Disponível em: <https://www.geisaponte.com/astrothreadbr>. Acesso em: 20 mar. 2019. Citado na página 92.

SÃO PAULO. **Currículo do Estado de São Paulo: matemática e suas tecnologias**. 1. ed. São Paulo, 2011. Citado nas páginas 23 e 76.

SINGH, S. **O livro dos códigos**. 7. ed. Rio de Janeiro: Record, 2007. Citado nas páginas 24, 27, 28, 29, 31, 32, 37, 38, 40, 44, 48, 54, 56, 57, 99, 100 e 124.

SKITTERPHOTO. 2017. Disponível em: <https://www.pexels.com/photo/julius-caesar-marble-statue-615344/>. Acesso em: 28 nov. 2019. Citado na página 99.

SPERLING, K. 2004. Disponível em: <https://commons.wikimedia.org/wiki/File:EnigmaMachineLabeled.jpg>. Acesso em: 12 dez. 2019. Citado na página 104.

TKOTZ, V. **Frequência de ocorrência de letras no Português**. 2005. Disponível em: <http://www.numaboa.com.br/criptografia/criptoanalise/310-frequencia-no-portugues>. Acesso em: 30 set. 2020. Citado na página 82.

VAN DE WALLE, J. A. **Matemática no Ensino Fundamental: formação de professores e aplicação em sala de aula**. Porto Alegre: Artmed, 2009. Citado na página 77.

VDOCUMENTS. 2014. Disponível em: <https://vdocuments.mx/hq-o-escaravelho-de-ouro-edgar-allan-poe.html>. Acesso em: 13 fev. 2020. Citado na página 122.

VINCK, H. 2011. Disponível em: <https://commons.wikimedia.org/wiki/File:Diffie-Hellman_Key_Exchange.jpg>. Acesso em: 23 jan. 2020. Citado nas páginas 114 e 115.

WIKIMEDIACOMMONS. Disponível em: <https://commons.wikimedia.org/wiki/File:Portrait_of_Eratosthenes.png>. Acesso em: 26 dez. 2019. Citado na página 107.

____. Disponível em: <https://commons.wikimedia.org/wiki/File:Rhind_Mathematical_Papyrus.jpg>. Acesso em: 9 jan. 2020. Citado na página 110.

____. 1849. Disponível em: <https://commons.wikimedia.org/wiki/File:Edgar_Allan_Poe,_circa_1849,_restored,_squared_off.jpg>. Acesso em: 13 fev. 2020. Citado na página 122.

____. 1928. Disponível em: <https://commons.wikimedia.org/wiki/Alan_Turing?uselang=pt-br#/media/File:Alan_Turing_Aged_16.jpg>. Acesso em: 31 out. 2019. Citado nas páginas 95 e 103.

____. 2005. Disponível em: <https://commons.wikimedia.org/wiki/File:Euklid-von-Alexandria_1.jpg>. Acesso em: 9 jan. 2020. Citado na página 110.

____. 2007. Disponível em: <https://commons.wikimedia.org/wiki/File:Skytale.png>. Acesso em: 21 nov. 2019. Citado na página 98.

ANEXO

A

CIFRAS MONOALFABÉTICAS

Blocos de cifras monoalfabéticas para atividade.

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

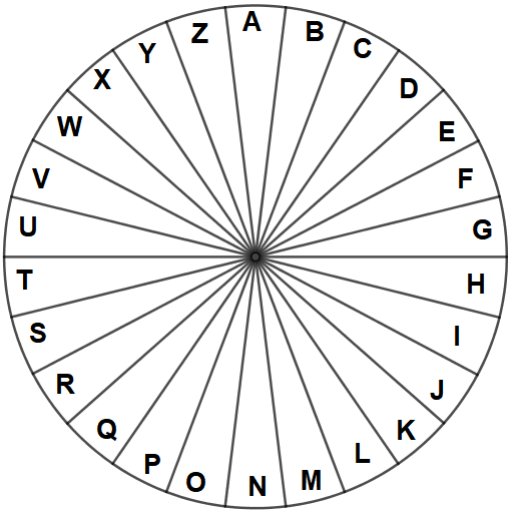
ANEXO

B

DISCO DE CIFRAS

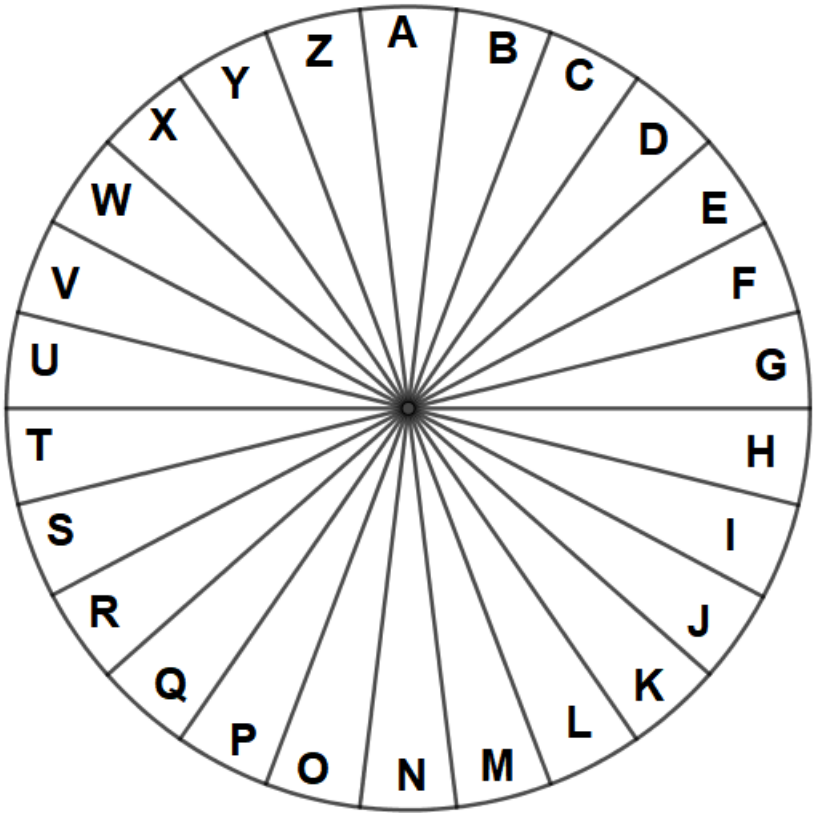
Para construir o disco de cifras basta recortar os dois discos a seguir e atá-los juntos através de seu centro, isso pode ser feito com um percevejo ou de qualquer outra forma que o professor encontrar resultado, a única condição é que os discos possam ser movimentados a fim de gerar os diversos alfabetos cifrados.

Figura 56 – Disco de cifras - parte interna



Fonte: Elaborada pelo autor.

Figura 57 – Disco de cifras - parte externa



Fonte: Elaborada pelo autor.

ANEXO

C

CONTO: O ESCARAVELHO DE OURO

O ESCARAVELHO DE OURO de Edgar Allan Poe

Oh! Oh! Este rapaz está dançando com louco!

Foi picado pela tarântula!

Tudo às avessas

Há muitos anos passados, travei amizade com um cavalheiro chamado William Legrand. Pertencia ele a uma antiga família huguenote e fora, outrora, rico, mas uma série de infortúnios tinham-no reduzido à miséria. Para evitar as mortificações que se seguiram a seus desastres, deixou Nova Orleans, terra natal de seus avós, e passou a residir na ilha de Sullivan, perto de Charleston, na Carolina do Sul.

Esta ilha é bastante singular. E formada quase que só de areia e tem cerca de três milhas de comprimento. Sua largura em ponto algum excede de um quarto de milha. Está separada do continente por um braço de mar quase imperceptível que se insinua através de uma vastidão de mangues e lodo, refúgio favorito das aves aquáticas. A vegetação, como se pode supor, é escassa, ou, pelo menos, raquítica. Nenhuma árvore de grande porte ali se vê. Perto da extremidade ocidental, onde se ergue o Forte Moultrie e onde se encontram alguns miseráveis barracões, habitados, durante o verão, pelos que fogem da poeira e da febre de Charleston, pode ser encontrada, a cerdosa palmeira-anã. Mas toda a ilha, com exceção dessa ponta ocidental e de uma faixa de áspera e branca praia na costa marítima, está coberta de densa capoeira de murta cheirosa, tão apreciada pelos horticultores ingleses.

Os arbustos atingem ali, às vezes, à altura de quinze a vinte pés e formam um matagal quase impenetrável, impregnando o ar com sua fragrância.No mais recôndito recesso desse matagal, não longe da ponta ocidental e mais remota da ilha, Legrand construiu uma pequena cabana, em que residia, quando, pela primeira vez, por mero acaso, travei conhecimento com ele.

Esse conhecimento logo amadureceu em amizade, pois naquele solitário muito havia

para excitar interesse e estima. Achei-o bem-educado, dotado de incomuns faculdades espirituais, infectadas, apenas, de misantropia e sujeitas a caprichosas disposições de entusiasmo e de melancolia alternadas. Tinha consigo muitos livros, mas raramente se servia deles. Suas principais diversões eram a caça e a pesca, além de vaguear por entre as murtas à busca de conchas ou espécimes entomológicos. Sua coleção destes últimos podia ser invejada por um Swammerdam. Nessas excursões era acompanhado, habitualmente, por um negro velho, chamado Júpiter, que tinha sido libertado antes dos reveses da família mas não pudera ser levado, por ameaças ou promessas, a abandonar o que considerava seu direito de acompanhar os passos de seu jovem "sinhô Will". Não é improvável que os parentes de Legrand, considerando-o de intelecto um tanto desarranjado, tenham tentado instilar essa teimosia em Júpiter, tendo em vista a vigilância e a guarda do erradio.

Os invernos, na latitude da ilha de Sullivan, raramente são muito severos e no fim do ano é coisa rara, na verdade, ser necessário acender. Pelo meado de outubro de 18. . . , houve, porém, um dia de sensível friagem. Justamente antes do pôr do sol, rompi, através dos arbustos sempre verdes, até a cabana de meu amigo, a quem eu não tinha visitado havia várias semanas, residente, como então era, em Charleston, a uma distância de nove milhas da ilha, num tempo em que as facilidades de travessia e volta estavam muito abaixo dos dias atuais.

Depois de alcançar a cabana, bati à porta, segundo meu costume, e, não obtendo resposta, procurei a chave no lugar onde eu sabia que ela ficava escondida, girei-a na fechadura e entrei. Belo fogo ardia na lareira. Era uma novidade, e de modo algum desagradável. Tirei o sobretudo e, puxando uma poltrona para junto das achas crepitantes, esperei pacientemente a chegada dos donos da casa. Pouco depois de escurecer, chegaram eles e me deram cordiais boas vindas. Júpiter, arreganhando os dentes de uma orelha a outra, apressou-se em preparar algumas aves aquáticas para o jantar. Legrand estava num de seus acessos - como poderia eu denominá-los diversamente? - de entusiasmo. Encontrara uma concha bivalva desconhecida, formando novo gênero, e, mais do que isso, caçara e apanhara, com o auxílio de Júpiter, um scarabaeus, que acreditava , ser totalmente novo, mas a respeito do qual desejava conhecer minha opinião, no dia seguinte.

- E por que não esta noite? - perguntei, esfregando as mãos por cima do fogo e desejando que toda a raça dos scarabaei fosse para o inferno.

- Ah! Se eu tivesse sabido que você estava aqui! - disse Legrand. - Mas faz tanto tempo que não o vejo; e como podia eu prever que você viria visitar-me logo nesta noite, grande entre todas? Ao vir para casa, encontrei-me com o Tenente G***, do forte, e, muito doidamente, emprestei-lhe o escaravelho; de modo que, para você, é impossível vê- o antes que amanheça. Fique aqui esta noite e mandarei Júpiter descer, ao nascer do sol. É a mais bela da criação!

- O quê? O nascer do sol?

- Ora. . . não! O escaravelho. É de uma brilhante cor de ouro, mais ou menos do tamanho

de uma noz grande, com duas manchas negras de azeviche, perto de uma das extremidades das costas e uma outra, um pouco mais comprida, na outra extremidade. As antenas são...

- Não tem nada de estanho nele não, sinhô Will, tou apostando - interrompeu aí Júpiter. - O escarvéio é um escaravéio de oro maciço, cada pedacinho dele, por dentro e tudo, menos as asa. Eu nunca vi um escarvéio nem a metade mais pesado, em toda a minha vida.

- Bem, suponhamos que é, Jup - replicou Legrand, algo mais vivamente, pareceu-me, do que o caso requeria. - É isso algum motivo para você deixar as aves queimarem? A cor - e aí ele voltou-se para mim - é realmente quase capaz de afiançar a opinião de Júpiter. Você nunca viu um brilho metálico mais cintilante do que o emitido pela casca dele. Mas sobre isso você poderá julgar amanhã. Até lá, vou dar-lhe alguma idéia do formato.

Dizendo isso, sentou-se a uma mesinha em que havia pena e tinta, porém não papel. Procurou alguma folha numa gaveta, mais não encontrou.

- Não faz mal - disse, por fim. - Isto servirá.

E tirou do bolso do colete um pedaço do que eu tomei por um gorro muito sujo e fez nele, com a pena, rápido desenho. Enquanto o fazia, conservei-me na cadeira junto ao fogo, pois estava ainda com frio. Quando o desenho ficou pronto, ele mo entregou, sem levantar-se. No momento em que eu o recebia, ouviu-se um alto grunhido, seguido de arranhões na porta. Júpiter abriu-a e um grande cão terra-nova, que pertencia a Legrand, entrou correndo, pulou sobre meus ombros e cumulou-me de festas, pois eu lhe dedicara muita atenção em visitas anteriores. Quando suas brincadeiras terminaram, olhei para o papel e, para falar verdade, fiquei um pouco intrigado com o que meu amigo desenhara.

- Bem! - disse eu, depois de contemplá-lo por alguns minutos.

- Esse é um estranho scarabaeus, devo confessá-lo; para mim, é novo; nunca vi coisa alguma como ele, antes, a não ser um crânio, ou uma caveira, com o que ele se parece mais do que qualquer coisa que já esteve sob a minha observação.

- Uma caveira! - repetiu Legrand. - Oh! Sim! bem... ele tem algo dessa aparência, no papel, sem dúvida. As duas manchas pretas do alto assemelham-se aos olhos, hein? E a mais comprida, embaixo, assemelha-se à boca... Depois, a forma doconjunto é oval.

- Talvez seja isso - disse eu -, mas, Legrand, receio que você não seja artista. Devo esperar até ver o próprio bicho, se quiser formar uma idéia de sua aparência pessoal.

- Bem, não sei... - disse ele, um pouco irritado. - Eu desenho toleravelmente; pelo menos, deveria desenhar; tive bons professores e orgulho-me de não ser um imbecil.

- Mas, meu caro, então você está brincando - falei. - Isto é um crânio bem passável... de fato posso dizer que é um crânio excelente, de acordo com as noções vulgares sobre tais espécimes de fisiologia. E seu scarabaeus deve ser o mais esquisito do mundo, se se parecer com isto. Ora, poderíamos extrair uma impressionante superstição desse esboço. Presumo que você

chamará o escaravelho scarabaeus caput hominis, ou qualquer coisa desse gênero. Há muitos títulos semelhantes na História Natural. Mas onde estão as antenas de que você falou?

- As antenas! - disse Legrand, que parecia estar-se tornando inexplicavelmente furioso com o assunto. - Estou certo de que você deve ver as antenas! Fi-las tão nítidas como são no inseto original e julgo que é suficiente.

- Bem... bem... talvez você tenha feito - disse eu. - Contudo não as vejo.E passei-lhe o papel, sem observação adicional, não desejando-lhe o temperamento. Mas muito surpreendido estava com a reviravolta que as coisas sofreram; seu mau-humor me intrigava. E, quanto ao desenho do bicho, positivamente nenhuma antena era visível e o conjunto possuía uma semelhança muito estreita com os desenhos comuns de uma caveira.

Ele recebeu o papel, muito impaciente, e estava a ponto de amarfanhá-lo, aparentemente para atirá-lo ao fogo, quando uma olhadela casual ao desenho pareceu de súbito prenderlhe a atenção. Num instante seu rosto enrubesceu com violência, e noutro ficou excessivamente pálido. Durante alguns minutos continuou a pesquisar o desenho, acuradamente, do lugar onde se sentava. Afinal levantou-se, apanhou uma vela na mesa e foi sentar-se sobre uma arca de viagem, no canto mais distante do aposento. Ali, de novo, procedeu a um exame ansioso do papel, virando-os em todas as direções. Nada disse, todavia, e essa conduta grandemente me assombrou; achei prudente, porém, não exacerbar o crescente mau humor de seu temperamento com qualquer comentário.

Depois ele tirou do bolso do colete uma carteira, colocou o papel dentro dela, cuidadosamente, e depositou-a numa escrivaninha, que fechou a chave.

Tornou-se, então, mais comedido em seus modos mas o aspecto primitivo de entusiasmo desaparecera por inteiro. Contudo, não parecia tão de mau-humor quanto abstraído. À medida que a noite avançava, ele se tornava cada vez mais perdido em sonhos, dos quais não o podia despertar qualquer de minhas observações. Fora minha intenção passar a noite na cabana, como antes freqüentemente fizera, mas, vendo naquela disposição de ânimo o dono da casa, considerei mais prudente despedir-me. Ele não insistiu para que eu ficasse, mas, quando parti, apertou-me a mão com cordialidade além da costumeira.

Foi cerca de um mês depois disso (e durante esse intervalo eu nada soubera de Legrand) que recebi, em Charleston, a visita de seu criado, Júpiter. Eu nunca vira o bom negro velho com aparência tão assustada e temi que algum sério desastre tivesse sobrevindo a meu amigo.

- Bem, Jup - falei -, que há agora? Como vai seu patrão?

- Ora, pra falá verdade, sinhô, ele num vai tão bem cumo devia sê.

- Não vai bem? Sinto muito em saber disso. De que é que ele se queixa?

- Tá-i. É isso! Ele num queixa de nada... mas ele está muito doente, muito mesmo.

- Muito doente, Júpiter? Por que você não disse isso logo? Ele está de cama?

- Num tá, não! Ele num acha lugá nenhum ião! Aí éque a porca torce o rabo! Tou cum a cabeça tonta por causa do sinhô Will!

- Júpiter, eu gostaria de entender o que você está dizendo. Você falou que seu patrão está doente. Ele não lhe contou de que é que sofre?

- Ora, sinhô, é bobage ficá quebrano a cabeça cum esse negócio! O sinhô Will num fala nada, diz que num tem coisa nenhuma... mas, então, por que é que ele fica pra lá e prá ca, oiano pra onde anda, cum a cabeça pra baixo e os ombro pra cima? E por que é que ele fica o tempo todo com uns numos, e...

- Com o quê, Júpiter?

- Fazendo uns numos e figuras na pedra, as figuras mais esquisitas que eu já vi. Eu já tou ficano cum medo, palavra. Tenho de ficá cum os óio pregado em riba dele só. Trodia, ele me escapuliu antes do só nascê e ficou sumido todo o santo dia. Eu tinha cortado uma boa vara, pra dá um bom ezempre nele quando ele vortasse, mas eu tô tão bobo que num tenho coração pra fazê ..... Ele tava com uma cara tão triste!

- Hein? Como? Ah, sim! ... Afinal de contas, eu acho que você fez melhor em não ser tão severo com o coitado. Não bata nele Júpiter. Ele pode muito bem não agüentar isso. Mas você não faz uma idéia do que é que causou essa doença, ou antes, essa mudança de procedimento? Aconteceu alguma coisa desagradável desde que eu estive lá?

- Não sinhô. Num teve nada desagradave desde esse dia. Foi antes disso, eu acho. Foi mesmo no dia que o sinhô teve lá.

- Como? Que é que você quer dizer?

- Ora, sinhô, eu quero dizê o escarvéio, tá-i!

- O quê?

- O escarvéio. Tou com toda a certeza de que sinhô Will foi mordido, lá por perto da cabeça, por aquele escarvéio de ouro.

- E que motivo você tem para essa suposição, Júpiter?

- Ele tem puã que chega, sinhô, e boca também. Eu nunca vi escaravéio tão encapetado. Ele bate e morde em tudo o que chegá perto . Sinhô Will apanhô ele primeiro, mas teve de deixá ele i embora depressa outra vez, tou-lhe falando... Foi nessa ocasião que ele deve tê dado a mordida. Eu num gosto do jeito da boca do escaravéio, de modo nenhum. Assim, eu num ia pegá nele cum meus dedo, mas agarrei ele cum pedaço de papé, que eu achei. Enrolei ele no papé e enfiei um pedaço na boca dele. Foi assim que eu fiz.

- E você pensa, então, que seu patrão foi picado pelo bicho e que a picada é que o fez ficar doente?

- Eu num penso, nada. Eu sei. O que é que faz ele ficá variano por causa de ouro, se num

é a mordida do escarvéio de ouro? Eu já ouvi falá desses escarvéio de ouro antes disso.

- Mas como é que você sabe que ele sonha com ouro?

- Cumo é que eu sei? Ora, porque ele fala disso enquanto tá dormindo. Tá-i como é que eu sei.

- Bem, Jup, talvez você tenha razão. Mas a que afortunada circunstância devo atribuir a honra de sua visita, hoje?

- Que é que é isso, sinhô?

- Você traz algum recado do Sr. Legrand?

- Não, sinhô. Eu trago é esta carta.

E aí Júpiter me entregou um bilhete, que rezava assim:

Meu caro:

Por que não o tenho visto, há tanto tempo? Espero que você não tenha caído na infantilidade de ofender-se com qualquer pequena rudeza de minha parte; mas, não; isso é improvável.

Desde que o vi, tenho tido grandes motivos de ansiedade. Tenho algo a dizer-lhe e, contudo, mal sei como falar, nem se devo falar.

Não tenho andado muito bem, nestes últimos dias, e o pobre velho Júpiter me irrita quase além do suportável com suas significativas atenções. Você acreditará que ele preparou uma pesada vara, no outro dia, para castigar-me, por ter escapulido dele e passado o dia, sozinho, entre as colinas do continente?

Acredito, deveras, que só minha aparência doentia me salvou de uma surra... Não fiz qualquer acréscimo à minha coleção, desde que nos encontramos.

Se você puder, de qualquer modo, fazê-lo sem inconveniente, venha com Júpiter. Venha.

Desejo vê-lo, esta noite. É assunto de importância. Asseguro-lhe que é da mais alta importância.

Sempre seu,

William Legrand

Havia algo no tom desse bilhete que me causou grande incomodo. Todo o seu estilo diferia completamente do de Legrand. Com que poderia estar ele sonhando? Que nova excentricidade dominava seu cérebro excitável? Que "negócio da mais alta importância" podia ele, possivelmente, ter a realizar? O que Jupiter me dissera dele não afiançava nada de bom. Eu temia que a contínua pressão da má sorte, afinal, tivesse inteiramente desarranjado a razão de meu amigo. Sem um momento de hesitação, por conseguinte, preparei-me para acompanhar o negro.

Ao chegar ao cais, notei uma foice e três pás, todas aparentemente novas, no fundo do

bote em que devíamos embarcar.

- Que quer dizer isso tudo, Jup? interroguei.

- Foice, sinhô, e pá.

- Muito bem; mas que é que elas estão fazendo aí?

- É a foice e as pá que sinhô Will falô pra eu comprá prá ele na cidade e foi o diabo o dinheirão que eu tive de dá por elas.

- Mas, por tudo quanto é misterioso, que é que seu "Sinho Will" vai fazer com foices e pás?

- Tá-i uma coisa que eu num sei e um raio me parta se eu num aquerdito que ele também num sabe. Mas isso tudo é coisa do escarvéio.

Verificando que nada de satisfatório podia obter de Júpiter, cuja mente parecia estar inteiramente absorvida pelo "escarvéio", entrei no bote e soltei a vela. Com bela e forte brisa, logo corremos para a pequena angra, ao norte do Forte Moultrie, e uma caminhada de cerca de duas milhas levou-nos à cabana. Eram quase três horas da tarde quando chegamos. Legrand estivera a esperar-nos com ansiosa expectativa. Apertou-me a mão, com um aperto nervoso, que me alarmou e fortaleceu as suspeitas já entretidas. Seu rosto é pálido até a lividez e seus olhos, fundos, brilhavam com um clarão anormal. Depois do algumas perguntas, relativas à sua saúde, interroguei-o, não sabendo que coisa melhor dizer, sobre se recebera do Tenente G*** o scarabaeus.

- Oh, sim! replicou ele, corando violentamente. - Recebi-o dele, na manhã seguinte. Nada me podia tentar a separar-me desse scarabaeus. Você sabe que Júpiter tem toda a razão acerca dele?

- De que modo? - perguntei, com triste pressentimento no coração.

- Ao supor que ele é um escaravelho de ouro autêntico.

Falou isso com aspecto de profunda seriedade e senti-me indizivelmente perturbado.

- Esse escaravelho vai fazer minha fortuna - continuou ele, com sorriso triunfante.

- Vai reinstalar-me na posse do que era de minha família. É qualquer coisa de admirar, então, que eu o aprecie que eu o aprecie tanto? Desde que a Fortuna achou conveniente conceder-mo, só tenho que usá- o de modo adequado e chegarei até o ouro de que ele é o indício. Júpiter, traga-me aquele scarabaeus!

- O quê? O escarvéio, sinhô? Eu acho mió num tê trabaio com aquele escaravéio... O sinhô mesmo apanhe ele.

Ai Legrand levantou-se, com ar grave e imponente, e trouxe-me o bicho, tirando-o de uma caixa de vidro em que ele estava encerrado. Era um belo scarabaeus, de tipo naquele tempo

desconhecido para os naturalistas e naturalmente de grande valor do ponto de vista científico. Havia duas manchas negras e redondas, perto de uma das extremidades das costas, e outra comprida mancha perto da outra extremidade. A casca era enormemente dura e brilhante, com toda a aparência de ouro brunido. O peso do inseto era bem digno de nota e, tomando tudo isso em consideração, eu mal poderia censurar Júpiter por sua opinião relativamente a ele; mas, por minha vida, não podia dizer que fazer, quanto à concordância de Legrand com essa opinião.

- Mandei buscá-lo - disse ele, num tom grandiloqüente -, mandei buscá-lo para poder ter seu conselho e auxílio, a fim de favorecer os desígnios da Sorte e do escaravelho.

- Meu caro Legrand - gritei eu, interrompendo-o -, você com certeza não está bem e faria melhor se tomasse algumas pequenas precauções. Deve ir para a cama e eu ficarei com você alguns dias até que recobre a saúde. Você está com febre e...

- Tome meu pulso - disse ele.

Tomei-lhe o pulso e, para falar a verdade, não achei o mais leve indício de febre.

- Mas você pode estar doente e, contudo, não ter febre. Permita-me que, desta vez, me faça de médico para você. Em primeiro lugar, vá para a cama. Em segundo lugar...

- Você está enganado - interrompeu ele. - Sinto-me tão bem quanto seria de esperar no estado de excitação em que me encontro. Se você realmente se interessa pela minha saúde, trate de aliviar-me dessa excitação.

- E como se há de fazer?

- Muito facilmente. Júpiter e eu vamos fazer uma expedição às colinas, no continente, e nessa expedição necessitamos do auxílio de alguma pessoa em quem possamos confiar. Você é a única que nos merece essa confiança. Se formos bem sucedidos ou fracassarmos, a excitação que você agora percebe em mim será, igualmente, aliviada.

- Tenho o maior desejo em servi-lo, de qualquer maneira - respondi -, mas... pretende você dizer que esse infernal escaravelho tem alguma relação com sua expedição às colinas?

- Tem.

- Então, Legrand, não posso tomar parte numa empresa tão absurda.

- Sinto muito... sinto muito... pois teremos de tentá-la nós mesmos.

- Pois tentem-na vocês! Este homem está seguramente maluco! Mas, vejamos! Quanto tempo se propõe você ficar ausente?

- Provavelmente a noite inteira. Partiremos agora mesmo e estaremos de volta, de qualquer modo, ao amanhecer.

- E você me promete, sob palavra de honra, que, quando tiver passado esse capricho de vocês e o negócio do escaravelho (bom Deus!) estiver resolvido, para satisfação sua, voltará

então para casa e seguirá estritamente meu conselho, como se fosse o seu médico?

- Sim, prometo. E agora, partamos, pois não temos tempo perder.

De coração opresso, acompanhei meu amigo. Pusemo-nos a caminho, cerca das quatro horas, Legrand, Júpiter, o cachorro, e Jupiter tinha consigo a foice e as pás, pois insistira em carregar todas, mais por medo, pareceu-me, de deixar qualquer daqueles utensílios ao alcance de seu patrão do que por qualquer excesso de solicitude ou complacência. Sua fisionomia estava extremamente carrancuda e "esse mardito escarvéio" foram as únicas palavras que escaparam de seus lábios durante o trajeto. Pela minha parte, estava encarregado de um par de lanternas furta-fogo, enquanto Legrand contentava-se com o scarabaeus, que levava amarrado à ponta de um pedaço de barbante fazendo-o girar, para lá e para cá, com o ar de um prestidigitador, enquanto caminhava. Ao observar esta última e plena prova da aberração mental de meu amigo, mal podia eu reter as lágrimas.

Pensei, porém, que seria melhor satisfazer-lhe a fantasia, pelo menos um momento, ou até que eu pudesse adotar medidas mais enérgicas, com probabilidade de êxito. Entrementes, tentei, mas completamente em vão, sondá-lo a respeito do objetivo da caminhada. Tendo conseguido induzir-me a acompanhá-lo, não parecia desejar travar conversa sobre qualquer assunto da menor importância. E a todas as minhas perguntas não se dignava dar outra resposta senão: "Veremos!"

Cruzamos o braço de mar na ponta da ilha por meio de um esquife e, subindo os terrenos altos da praia do continente, continuamos na direção noroeste, através de um trecho de terras expressivamente agrestes e desoladas, onde não se via vestígio algum de passo humano. Legrand seguia na dianteira, com decisão, parando apenas um instante aqui e ali para consultar o que parecia ser certos marcos, por ele mesmo colocados em ocasião anterior.

Caminhamos, assim, cerca de duas horas, e o sol estava a ponto de pôr-se, quando penetramos numa região infinitamente mais sinistra do que qualquer outra até então vista. Era uma espécie de tabuleiro, perto do cume de uma colina quase inacessível, densamente coberta da base ao cimo e entremeada de imensos penhascos que pareciam estar soltos sobre o solo e, em muitos casos, só não se precipitavam nos vales, lá embaixo, graças ao suporte dos troncos contra os quais se reclinavam. Profundas ravinas, em várias direções, davam ao cenário um ar de solenidade ainda mais severo.

A plataforma natural sobre a qual havíamos garimpado estava espessamente coberta de sarças, através das quais logo descobrimos que seria impossível abrir caminho, a não ser por meio da foice e Júpiter, por ordem de seu patrão, começou a rasgar para nós uma estrada, até o pé de um tulipeiro gigantesco, que se erguia, com uns oito ou dez carvalhos, sobre o planalto, e os ultrapassava, a todos, bastante, bem como a todas as outras árvores que até então eu vira, pela beleza da folhagem e da forma, pela vasta circunferência dos ramos e pela majestade geral de seu aspecto. ao alcançarmos essa árvore, Legrand voltou-se para Júpiter e perguntou-lhe se achava que podia subir por ela. O velho pareceu um tanto aturdido com essa pergunta e, durante

alguns instantes, não deu resposta. Afinal, aproximou-se do imenso tronco, andou devagar em torno dele e examinou-o com minuciosa atenção. Terminado o exame disse simplesmente:

- Sim, sinhô. Jup sobe em quarqué arve que ele nunca não viu na sua vida.

- Então suba, o mais depressa possível, pois em breve estará demasiado escuro para ver o que devemos fazer.

- Até aonde eu tenho de assubi, sinhô? - perguntou Júpiter.

- Suba primeiro pelo tronco principal e depois eu lhe direi que caminho deverá tomar... Ah! Espere! Leve este escaravelho com você.

- O escarvéio, sinhô Will? O escarvéio de ouro? - gritou o negro, recuando de medo. - Purque é que eu tenho de levar o escarvéio pra cima da arve? Que eu me dane se fizé isso!

- Se você tem medo, Jup, um negralhão como você, de pegar num pequeno escaravelho morto e inofensivo, pode levá-lo por este barbante. Mas se, de qualquer modo, não quiser levá-lo consigo lá para cima, serei forçado a quebrar sua cabeça com esta pá.

- Que negócio é esse, sinhô? - disse Júpiter, evidentemente envergonhado, a ponto de se tornar mais condescendente. Sempre quereno armá baruio com o nego véio... Eu tava só brincano! Eu, tê medo de escarvéio? Nem tou ligando pra ele!

Aí pegou com precaução a extremidade do barbante e, mantendo o inseto tão longe de sua pessoa quanto as circunstâncias lhe permitiam, preparou-se para subir à árvore.

Quando novo, o tulipeiro, ou Liriodendron tulipiferum, o mais majestoso dos habitantes da floresta americana, tem um tronco caracteristicamente liso e muitas vezes se eleva a grande alturas sem ramos laterais; mas, chegando à maturidade, a casca torna-se rugosa e desigual, enquanto muitos galhos pequenos aparecem sobre o tronco. Assim, a dificuldade da ascensão, no caso presente, era mais aparente que real. Abraçando o enorme cilindro o mais estreitamente possível, com os braços e os joelhos, agarrando com mãos alguns dos brotos e descansando os dedos nus sobre outros, Júpiter , depois de ter escapado de cair uma ou duas vezes, por fim içou-se até à primeira grande forquilha, parecendo considerar a coisa toda como virtualmente executada. Na realidade, o risco da empresa havia passado, embora o negro estivesse a sessenta ou setenta pés do solo.

- Pra donde devo i agora, sinhô Will? - perguntou ele.

- Vá subindo pelo galho mais grosso, o daquele lado - disse Legrand.O negro obedeceu-lhe prontamente e, ao que parece, sem muita dificuldade, subindo cada vez mais alto, até que não se conseguia vislumbrar seu vulto agachado, através da densa folhagem que o tocava. Nesse momento, ouviu-se sua voz, numa espécie de grito.

- Até onde eu tenho de assubi ainda?

- A que altura você está? - perguntou Legrand.

- Tão arto, tão arto - replicou o negro - que tou podendo vê o céu pelo arto da arve.

- Não se preocupe com o céu, mas preste atenção ao que eu digo. Olhe para o tronco embaixo e conte os galhos abaixo de você, desse lado. Quantos galhos você passou?

- Um, dois, treis, quatro, cinco. . . Passei cinco gaios grandes desse lado sinhô.

- Então, suba um galho mais alto. Em poucos minutos ouviu-se novamente a voz, anunciando que galho fora atingido.

- Agora, Jup - gritou Legrand, evidentemente bastante excitado. - Quero que você vá andando por esse galho, até onde puder. Se vir qualquer coisa estranha, diga-me.

Desta vez, qualquer pequena dúvida que eu pudesse ainda entreter a respeito da insanidade de meu pobre amigo foi, por fim, desfeita. Não tinha outra alternativa senão concluir que ele estava atacado de loucura e fiquei seriamente ansioso por fazê-lo voltar à casa. Enquanto ponderava sobre o que seria melhor, ouviu-se de novo a voz de Júpiter.

- Tou com muito medo de me arriscá nesse gaio mais longe. Ela tá quage todo podre.

- Você está dizendo que é um galho podre, Júpiter? - gritou Legrand, com voz trêmula.

- Nhô, sim. Tá podre que nem uma tranca véia. Podrinho da Sirva. Não tá prestano mais pra nada.

- Em nome do céu, que devo fazer? - perguntou Legrand, demonstrando o maior desespero.

- Que fazer? - disse eu, alegre por encontrar uma oportunidade de intercalar uma palavra. - Ora, ir para casa e deitar-se.

- Vamos embora! Não seja teimoso! Está ficando tarde, e além disso não deve esquecer-se de sua promessa.

- Júpiter! - gritou ele, sem me dar nenhuma atenção. - Está me ouvindo?

- Nhô, sim, sinhô Will, tou escuitando o sinhô muito bem.

- Experimente, então, o galho com seu canivete e veja se está muito podre.

- Ele tá podre, sinhô, e muito mesmo - replicou o negro, em poucos momentos. Mas num tá tão podre como devia tá. Eu sozinho, posso me arriscá mais um bocado pelo gaio.

- Você sozinho? Que é que você quer dizer?

- Ora, tou falano do escarvéio. Ele é muito pesado. Se eu soltasse ele primeiro, então o gaio não ia se quebrá, só com o peso de um nego.

- Velhaco dos infernos! - gritou Legrand, aparentemente muito aliviado. - Que é que você está pensando para falar uma asneira dessas? Se você soltar esse escaravelho, palavra que lhe quebro o pescoço. Escute aqui Júpiter. Você está-me ouvindo?

- Tou sim, sinhô. Num é preciso gritá pro pobre nego desse jeito.

- Bem, então escute! Se você se arriscar pelo galho, até onde puder chegar sem perigo, e não soltar o escaravelho, eu lhe darei um dólar de prata de presente logo que você descer.

- Tou ino, sinhô Will.. . Tá feito - replicou o negro, bem depressa. Tou agora quage na pontinha!

- Na ponta! gritou satisfeito Legrand. - Você diz que está na ponta desse galho?

- Tou chegando no fim, sinhô. . . ooooooooooooh! Vala-me Deus! Que é isso aqui em cima da arve?

- Bem! - gritou Legrand, altamente satisfeito. - Que é? Uai! Pra mim isso é uma caveira! Arguém deixô a cabeça dele aqui em riba da arve e os corvo comero tudo quanto era pedaço de carne.

- Uma caveira, foi o que você disse? Muito bem!. . . Como é que ela está presa no galho? Que é que a segura?

- Sei não, sinhô. Vô espiá. Tá-i, palavra que é uma coisa muito esquisita. . . Tem um prego enorme na caveira, pregando ela na arve.

- Bem. Agora, Júpiter, faça exatamente como eu vou dizer.

- Sim, sinhô.

- Preste atenção, então. Procure o olho esquerdo da caveira.

- Humm! Humm! Tá bem! Mas ela num tem ôio esquerdo nenhum!

- Maldita estupidez! Você não sabe distinguir sua mão direita da esquerda?

- Sei. Isso eu sei. . . Sei muito bem. . . é com a mão esquerda; que eu racho a lenha.

- Muito bem. Você é canhoto. E seu olho esquerdo está do mesmo lado de sua mão esquerda. Acho que agora você já sabe achar o olho esquerdo da caveira ou o lugar onde ele estava. Achou?

Houve um prolongado intervalo. Por fim o negro falou:

- O ôio esquerdo da caveira tá também do mesmo lado da mão esquerda dela? E purque a caveira não tem nem um pedacinho de mão nenhuma. . . Num faz mal! Achei o ôio esquerdo agora . Tá aqui o ôio esquerdo. Que é que eu vô fazê cum ele?

- Deixe o escaravelho cair por dentro dele, até onde o barbante der mas tenha cuidado e não largue o barbante.

- Tá tudo pronto, sinhô Will. Foi muito fácil pô o escarvéio no buraco. Óia ele lá embaixo!

Durante essa conversa, nenhuma parte do corpo de Júpiter podia ser vista; mas o escaravelho, que ele fizera descer, era agora visível na ponta do cordel e cintilava, como um globo de

ouro brunido, aos últimos raios do sol poente, alguns dos quais ainda iluminavam debilmente o cume sobre que nos achávamos. O scarabaeus pendia inteiramente livre de quaisquer galhos e, se deixado cair, tombaria aos nossos pés.

Legrand imediatamente tomou da foice e limpou com um espaço circular, de três ou quatro jardas de diâmetro, bem por baixo do inseto. E, tendo feito isso, ordenou a Júpiter que e soltasse o barbante e descesse da árvore.

Fincando uma cunha, com grande cuidado, no lugar preciso em que o escaravelho caiu, meu amigo tirou então do bolso uma fita métrica. Amarrando uma ponta da mesma ao ponto da árvore que estava mais próxima da cunha, desenrolou-a até alcançar a cunha e tornou a desenrolá-la, na direção já estabelecida pelos dois pontos da cunha e da árvore, pela distância de cinqüenta pés. Júpiter ia limpando as sarças com a foice. No lugar assim atingido, foi cravada segunda cavilha e em volta desta, como centro, traçou ele um círculo grosseiro, de cerca de quatro pés de diâmetro. Apanhando então uma pá e dando uma a Júpiter e a outra a mim, Legrand pediu-nos que cavássemos tão depressa quanto possível.

Para falar verdade, eu nunca tive predileção por tal divertimento, em tempo algum, e naquele momento particular de boa-vontade teria recusado, pois a noite ia chegando e me achava muito fatigado com o exercício já feito. Mas não vi jeito de escapar e temia eu turbar a serenidade de meu pobre amigo com uma recusa. Se eu, de fato, pudesse confiar na ajuda de Júpiter, não teria hesitado em tentar carregar o lunático para casa, à força; mas conhecia demasiado bem a disposição de ânimo do velho negro para crer que ele me ajudaria, sob quaisquer circunstâncias, numa disputa pessoal com seu patrão.

Não tinha dúvida de que este último era vítima de alguma das inúmeras superstições meridionais acerca de ouro enterrado e de que tal fantasia recebera confirmação pela descoberta do scarabaeus, ou, talvez, pela obstinação de Júpiter em asseverar que era "um escarvéio de ouro de verdade". Um espírito disposto à loucura seria facilmente conduzido por semelhantes sugestões, especialmente se as mesmas se harmonizassem com idéias favoráveis e preconcebidas. Recordei-me, então, da conversa do coitado acerca de ser o escaravelho "o indício de sua fortuna". Por causa de tudo isso eu me sentia tristemente aborrecido e incomodado, mas afinal resolvi fazer do mal um bem e cavar com boa-vontade, para que assim o visionário se convencesse mais cedo, pela demonstração de seus olhos, da inutilidade das opiniões que entretinha.

Acesas as lanternas, entregamo-nos ao trabalho com um zelo digno de causa mais tradicional; e ao cair o clarão sobre nossas pessoas e objetos, não pude deixar de pensar no grupo pitoresco que compúnhamos e quão estranhas e suspeitas nossas ações deveriam parecer a qualquer intruso que, por acaso, pudesse surgir onde nos achávamos.

Cavamos bem firmemente, durante duas horas. Pouca coisa se disse. E nosso embaraço principal estava nos latidos do cachorro, que tomava especial interesse em nossa tarefa. Afinal, ele se tornou tão impertinente que tivemos receio de que desse o alarme algum desgarrado que

andasse nas vizinhanças. Ou, antes, esse era o temor de Legrand, pois eu me sentiria alegre com qualquer interrupção que me permitisse levar o alucinado para casa. O barulho, por fim foi muito eficazmente silenciado por Júpiter, que, saindo do buraco com um ar carrancudo de resolução, amarrou a cabeça do bicho com um de seus suspensórios e depois voltou, com um risinho sério à sua tarefa.

Quando o tempo mencionado expirara, alcançáramos uma profundidade de cinco pés e, contudo, nenhum sinal de qualquer tesouro se manifestara. Seguiu-se uma pausa geral e comecei a esperar que a farsa estivesse no fim. Legrand, contudo, embora evidentemente muito desapontado, enxugou a testa, pensativo, e recomeçou. Caváramos todo o círculo de quatro pés de diâmetro e agora, pouco a pouco, alargávamos o limite, chegando a cavar mais de dois pés de profundidade.

Nada apareceu, todavia. O procurador de ouro, de quem eu sinceramente me apiedava, pulou afinal do buraco, com mais amargo desaponto impresso em todos os traços do rosto, pôs-se, vagarosa e relutantemente, a vestir o paletó que atirara fora ao começar o serviço. Entrementes, eu não fiz qualquer observação.

Júpiter, a um sinal do patrão, começou a juntar as ferramentas.Feito isso e desamordaçado o cachorro, voltamos para casa, em profundo silêncio.Déramos, talvez, doze passos nessa direção, quando, com um alto palavrão, Legrand saltou sobre Júpiter e agarrou-o pelo pescoço. O negro, atônito, abriu os olhos e a boca até onde foi possível soltou as pás e caiu de joelhos.

- Vagabundo! - disse Legrand, sibilando as sílabas, por entre dentes cerrados. - Negro dos diabos! Fale, estou-lhe dizendo! Responda-me neste instante, sem querer enganarme! Qual é... qual é seu olho esquerdo?

- Oh, meu Deus! Sinhô Will! Então num é este aqui meu ôio, esquerdo? - grunhiu o terrificado Júpiter, colocando a mão sob o órgão direito da visão e conservando-a ali, com desesperada pertinácia, como se temesse uma tentativa imediata de seu patrão para arrancá-lo.

- Bem eu pensei! Eu sabia disso! Viva! - vociferou Legrand soltando o negro e executando uma série de piruetas e cambalhotas, para grande espanto do criado, que, erguendo-se de sobre os joelhos, olhava, mudo, de seu patrão para mim e de mim para seu patrão.

- Venham! Precisamos voltar! - disse este último. - A partida não foi perdida ainda. E de novo caminhou para o tulipeiro.

- Júpiter, - disse ele, - quando o acompanhamos. - Venha cá! A caveira estava pregada ao galho com a face para fora ou com a face para o ramo?

- A cara tava pra fora, sinhô, e assim os corvo pudero chegá bem nos óio, sem trabáio nenhum.

- Bem. Então foi por este olho ou por aquele que você deixou cair o escaravelho? - e aí Legrand apontou para cada um dos olhos de Júpiter.

- Foi por este ôio, sinhô... O ôio esquerdo... certinho como o sinhô me disse - e aí era o olho direito o que o negro indicava.

- Pois vamos! Devemos tentá-lo de novo.

Aí meu amigo, em cuja loucura agora eu via, ou imaginava ver, alguns indícios de método, removeu a cavilha que marcava o lugar onde o escaravelho caiu para um lugar cerca de três polegadas para oeste de sua primitiva posição. Tomando, depois, a fita métrica do ponto mais próximo do tronco até a cavilha, como antes, e continuando a estendê-la em linha reta até a distância de cinqüenta pés, foi indicado um lugar afastado várias jardas do ponto em que tínhamos estado cavando.

Em torno da nova posição, um círculo, um tanto maior do que no caso anterior, foi agora traçado e nós de novo pusemo-nos a trabalhar com a pá. Eu estava terrivelmente cansado; mas, mal compreendendo o que havia causado a mudança em meus pensamentos, não sentia mais nenhuma grande aversão pelo trabalho imposto. Tinha-me tornado mais inexplicavelmente interessado, e não só, até mesmo excitado. Talvez houvesse algo, em meio de todas as atitudes extravagantes de Legrand, certo ar de previsão, ou de decisão, me impressionava.

Cavei com afinco e, de vez em quando, me surpreendia realmente aguardando, com algo que muito se assemelhava à expectativa, o imaginado tesouro, cuja visão havia dementado meu infeliz companheiro. Ao tempo em que tais devaneios de pensamento maiormente se apoderaram de mim e quando já estávamos a trabalhar talvez uma hora e meia, fomos de novo interrompidos pelos violentos latidos do cão. Sua inquietação, no primeiro caso, tinha sido, evidentemente, apenas o resultado de brincadeira, capricho; mas agora assumia um tom mais amargo e sério. À nova tentativa de Júpiter para amordaçá-lo, ele ofereceu furiosa resistência e, pulando para dentro do buraco, começou a cavar a terra freneticamente, com as patas. Em poucos segundos, tinha descoberto um monte de ossos humanos, formando dois esqueletos completos, entremeados de vários botões de metal e do que parecia ser poeira de lã apodrecida. Uma das pazadas puseram a descobrir a lamina de uma faca espanhola e, ao cavarmos mais fundo, três ou quatro moedas de ouro e de prata vieram a lume.

À vista delas, a alegria de Júpiter mal pôde ser contida, mas a fisionomia de seu patrão apresentava um ar de extremo desaponto. Insistiu conosco, porém, a que continuássemos nossos esforços e mal as palavras acabavam de ser pronunciadas, eu cambaleei para a frente, tendo enfiado a ponta de minha bota num anel de ferro que jazia semi-enterrado na terra solta.

Trabalhávamos, agora, com verdadeira ânsia e nunca passei minutos de mais intensa excitação. Durante este intervalo, havíamos completamente desenterrado uma arca oblonga, de madeira que, pela sua perfeita conservação e maravilhosa resistência, evidenciava plenamente ter sido sujeita a algum processo de mineralização, talvez o do bicloreto de mercúrio. Esta caixa tinha três pés e meio de comprimento, três pés de largura e dois e meio de altura. Estava firmemente fechada por aros de ferro fundido, com ferros formando uma espécie de grade em

volta da arca. De cada lado da caixa, perto da tampa, havia três anéis de ferro, seis ao todo, por meio dos quais seis pessoas poderiam agarrá-la com firmeza. Reunidos os nossos maiores esforços, mal pudemos afastar o cofre um pouquinho no seu leito. Percebemos imediatamente a impossibilidade de levantar tão grande peso. Felizmente, as únicas trancas da tampa consistiam em dois ferrolhos corrediços, que puxamos para trás, tremendo e vacilando de ansiedade.

No mesmo instante, tivemos ali, cintilando diante de nossos olhos, um tesouro de incalculável valor. Como os raios de luz das lanternas caíssem dentro do poço, deste subiam, irradiando, uma incandescência e um resplendor provindos dum confuso montão de ouro e de jóias, que nos deslumbravam completamente a vista.

Não pretenderei descrever os sentimentos que de mim se apossaram ao contemplar aquilo. Predominava, sem dúvida, o espanto. Legrand parecia exausto e dizia muito poucas palavras. A fisionomia de Júpiter apresentou, por alguns minutos, a palidez mortal que é possível, na ordem natural das coisas, um rosto de negro exibir. Parecia estupefato, siderado. Logo em seguida ajoelhado dentro do buraco e, mergulhando os braços, nus ate os cotovelos, no ouro, ali deixou-os ficar, como se gozasse a volúpia dum banho. Por fim, com um profundo suspiro, exclamou, se falasse sozinho:

- E tudo isso vem do escarvéio de ouro! Do bunito escaravéio de ouro! O coitado do escarveinho de ouro que eu tanto descompus, chamei tanto nome feio! Ocê num tem vergonha disso não seu nego? Vamos, me arresponda!

Tornou-se necessário, por fim, que eu despertasse tanto o patrão como o criado, chamando-lhes a atenção para a urgência de remover o tesouro. Estava ficando tarde, e era conveniente que desenvolvêssemos certa atividade para ter tudo aquilo em casa antes do amanhecer. Difícil foi combinarmos o que deveríamos fazer, e muito tempo perdemos a decidir-nos, tão confusas eram as idéias de todos nós. Finalmente, aliviamos o peso da caixa, removendo dois terços de seu conteúdo, e só então fomos capazes, com algum esforço de tirá-lo do buraco.

Os objetos retirados foram depositados entre as sarças, ficando o cachorro a guardá-los, com estritas ordens de Júpiter para, sob nenhum pretexto, nem se afastar do lugar nem abrir a boca até voltarmos. Então, apressadamente, rumamos para casa com a arca, tendo alcançado a cabana a salvo, mas depois de excessivo esforço, a uma hora da manhã. Esgotados como estávamos, ultrapassava as forças humanas fazer mais alguma coisa imediatamente. Descansamos até às duas horas e ceamos, partindo para as colinas logo depois, munidos de três resistentes sacos que havíamos encontrado, por felicidade, na cabana. Um pouco antes das quatro, chegamos ao buraco, dividimos o restante da presa, o mais igualmente possível, entre nós, e, deixando os buracos abertos, e de novo partimos para a cabana, na qual, pela segunda vez, depositamos nossas cargas de ouro, justamente quando os primeiros e fracos raios da madrugada apareciam a leste, luzindo por cima das copas das árvores.

Sentíamo-nos, agora, completamente esgotados, mas a intensa excitação daquele instante

nos impedia de repousar. Depois dum sono inquieto dumas três ou quatro horas de duração, despertamos, como se o houvéssemos combinado, para proceder ao exame do nosso tesouro.

A arca fora cheia até as bordas e passamos o dia inteiro e grande parte da noite inventariando seu conteúdo. Nenhuma ordem ou arranjo fora adotada. Tudo fora amontoado misturadamente. Depois de tudo classificado com cuidado, achamo-nos de posse duma riqueza muito mais vasta do que a princípio supuséramos. Em moedas, havia mais, muito mais, de quatrocentos e cinqüenta mil dólares, estimando o valor do dinheiro, tão acuradamente como podíamos, de acordo com as tabelas da época. Não havia uma partícula de prata. Tudo era ouro de antiga data e de grande variedade: moedas francesas, espanholas e alemãs, com alguns guinéus ingleses e uns tantos miúdos, de que jamais havíamos visto modelos antes.

Havia muitas moedas bem grandes e pesadas, tão gastas que nada se podia vislumbrar de suas inscrições. Não havia dinheiro americano. Mais dificuldade encontrávamos em avaliar o valor das jóias. Haviam diamantes, alguns deles excessivamente grandes e belos, cento e dez ao todo , e nenhum pequeno; dezoito rubis de notável brilho; trezentas e dez esmeraldas, todas lindíssimas, e vinte e uma safiras, além de uma opala. Essas pedras tinham sido, todas, arrancadas de seus engates e atiradas de qualquer modo à arca. Os próprios engates que retiramos de entre outras peças de ouro pareciam ter sido batidos com martelos, como para impedir a identificação. Além de tudo isso, havia uma enorme quantidade de pesados ornamentos de ouro, quase duzentos brincos e anéis maciços; ricas correntes, em número de trinta, se bem me lembro; oitenta e três crucifixos muito grandes e pesados; cinco turíbulos de ouro de grande valor, uma maravilhosa poncheira de ouro, ornamentada com folhas de parreira ricamente cinzeladas e figuras báquicas; dois punhos de espada, caprichosamente gravados em relevo, e muitos outros objetos menores, de que não me posso lembrar. O peso desses excedia de trezentas e cinqüenta libras, bem pesadas; e nessa avaliação eu não incluí cento e noventa e sete soberbos relógios de ouro, três dos quais valiam, cada um, quinhentos dólares, no mínimo. Muitos deles eram muito velhos e, para marcar o tempo, inúteis, pois o mecanismo sofrera, muito ou pouco, com a corrosão, mas eram todos ricamente cravejados de pedras, estando em estojos de alto preço.

Calculamos, naquela noite, que o inteiro conteúdo da arca valia um milhão e meio de dólares; e quando, depois, dispusemos dos berloques e jóias (retendo poucas para nosso uso próprio verificamos haver grandemente subestimado o tesouro. Ao concluir, por fim, nosso exame, diminuída de alguma intensa excitação daquelas horas, Legrand, que viu que eu morria de impaciência, esperando uma solução desse extraordinário enigma, passou a detalhar, completamente, todas as circunstâncias relacionadas com ele.

- Você se lembra - disse ele - da noite em que eu lhe entreguei o tosco desenho que fizera o scarabaeus. Você se recorda também, de que eu fiquei completamente zangado com você, de sua insistência de que meu desenho se assemelhava a uma caveira? Quando você pela primeira vez fez essa afirmativa, pensei que estivesse brincando; mas depois recordei as manchas características nas costas do inseto e concordei comigo mesmo em que sua observação tinha, de

fato, alguma base. Contudo, a zombaria de minhas você me restituiu o pedaço de pergaminho, estive a ponto de rasgá-lo e atirá-lo, com raiva, ao fogo.

- O pedaço de papel, quer dizer - disse eu.

- Não, ele era muito parecido com o papel e, a princípio supus que fosse isso, mas quando fui desenhar nele verifiquei que era um pedaço de pergaminho muito fino. Você disse que estava inteiramente sujo? Bem, quando eu estava a amarrotá-lo meu olhar caiu sobre o esboço para que você estivera olhando e você pode imaginar meu espanto quando, de fato, percebi a figura de uma caveira no mesmo lugar, pareceu-me, em que eu desenho do escaravelho. Por um momento fiquei demasiado atônito para pensar com clareza. Sabia que meu desenho era, em detalhes, muito diverso daquele, embora houvesse uma certa semelhança no contorno geral. Tomei então de uma vela e, sentando-me no outro canto do quarto, comecei a examinar o pergaminho mais perto. Depois de virá-lo, vi meu próprio desenho no verso, tal o havia feito. Minha primeira idéia, então, foi a de simples surpresa pela similaridade de contorno realmente notável e pela sua singular coincidência envolvida no fato, para mim desconhecido, de que houvesse um crânio no outro lado do pergaminho, bem por trás de meu desenho do scarabaeur, e de que esse crânio, não só contorno, mas no tamanho, tão estreitamente se assemelhasse a meu desenho.

Digo que a similaridade dessa coincidência me deixou estupefato por algum tempo. Tal é o efeito comum de coincidências tais. A mente luta para estabelecer uma relação, uma seqüência de causa e efeito e, sendo incapaz de fazê-lo, experimenta uma espécie de paralisia temporária. Mas quando voltei a mim desse estupor, irrompeu em mim uma convicção, pouco a pouco, que me espantou mais do que a coincidência. Comecei distintamente, positivamente, a recordar que não havia desenho algum sobre o pergaminho quando fiz o esboço do escaravelho.

Fiquei perfeitamente certo disso, porque me lembrava de ter virado primeiro um lado e depois o outro, à procura do lugar mais limpo. Se o crânio tivesse estado ali, sem dúvida eu não podia ter deixado de notá-lo. Ali estava , de fato, um mistério que achei impossível explicar; mas mesmo naquele primeiro momento, pareceu-me cintilar, fracamente, no mais íntimo e secreto recanto de minha inteligência a larva de uma concepção daquela verdade de que a ventura da noite passada nos trouxe magnífica demonstração. Ergui-me logo e, guardando o pergaminho com cuidado, transferi toda reflexão ulterior para quando estivesse só.

Quando você saiu, e quando Júpiter estava já bem adormecido, entreguei-me a uma investigação mais metódica do assunto. Em primeiro lugar, considerei a maneira pela qual o pergaminho veio cair em meu poder. O lugar onde descobrimos o escaravelho era na costa do continente, a cerca de uma milha para leste da ilha, e apenas a curta distância acima da marca da maré alta. Quando o agarrei ele me deu uma aguda picada, o que me fez deixá-lo cair. Júpiter com sua precaução costumeira, antes de agarrar o inseto que voara para o lado dele, procurou em volta uma folha, ou algo semelhante, com que apanhá-lo.

Foi nesse momento que seus olhos e também os meus, caíram sobre o pedaço de

pergaminho, que então supus ser papel. Ele estava meio enterrado na areia com uma ponta aparecendo. Perto do lugar onde o encontramos , observei os restos do casco do que parecia ter sido uma baleeira de navio. As ruínas pareciam estar ali desde muito tempo, pois nas madeiras mal se podia vislumbrar a aparência de um bote.

Bem, Júpiter apanhou o pergaminho, envolveu nele o escaravelho e deu- mo. Logo depois voltamos para casa e, no caminho, encontramos o Tenente G***.

Mostrei-lhe o inseto e ele me pediu que o deixasse levá-lo ao forte. Tendo o meu consentimento, colocou-o em seguida no bolso do colete, sem o pergaminho em que estivera enrolado e que eu continuara a ter na mão durante o tempo em que ele inspecionava o animal. Talvez receasse que eu mudasse de idéia e achasse melhor assegurar-se da presa imediatamente; você sabe quão entusiasta ele é em todos os assuntos relacionados com a História Natural. Ao mesmo tempo, sem notar o que fazia, eu devo ter cocado o pergaminho em meu próprio bolso.

Você se lembra de que, quando fui à mesa para o fim de fazer um esboço do escaravelho, não encontrei papel onde era ele habitualmente guardado. Procurei na gaveta e também nada achei. Revistei os bolsos, esperando encontrar uma velha carta, quando minha mão caiu sobre o pergaminho. Pormenorizo assim o modo preciso pelo qual este caiu em meu poder porque as circunstâncias impressionaram com força especial.

Não duvido de que você me achará um sonhador. Mas eu já estabelecera uma espécie de relação. Ajuntara dois elos de uma grande cadeia. Havia um bote jazendo sobre a costa marítima e não longe do bote, havia um pergaminho - não um papel - um crânio pintado nele. Você naturalmente perguntará: onde está a relação? Replico que o crânio, ou caveira, é o muito conhecido emblema dos piratas. A bandeira da caveira é içada em todas as suas empresas.

Já disse que aquele pedaço era de pergaminho e não de papel. O pergaminho é durável, quase imperecível. Raramente se confiam ao pergaminho coisas de pequena importância, visto como, para os simples fins ordinários do desenho ou da escrita, ele não se presta tão bem como o papel.

Essa reflexão sugeria algum significado, algum propósito na caveira. Não deixei de observar, também a forma do pergaminho. Embora um de seus cantos tivesse sido destruído por algum acidente, podia-se ver que a forma primitiva era quadrangular. Era justamente um pedaço, de fato, tal como poderia ter sido escolhido para uma nota, para o registro de alguma que devia ser prolongadamente lembrada e cuidadosamente preservada.

- Mas - interrompi -, você disse que o crânio não estava no pergaminho quando fez o desenho do escaravelho. Como, então traça alguma relação entre o bote e o crânio, desde que este último de acordo com o que você mesmo admitiu, deve ter sido desenhado (só Deus sabe como e por quem) em algum período subseqüente ao de seu esboço do escaravelho?

- Ah, aí é que todo o mistério se resolve, embora, nesse ponto eu tivesse relativamente pouca dificuldade em resolver o segredo. Meus passos eram certos e eu só podia atingir um

resultado. Raciocinei, por exemplo, assim: Quando desenhei o escaravelho, não aparecia crânio algum no pergaminho. Ao terminar o desenho, passei-o a você e observeio acuradamente, até que você o devolveu. Você portanto, não desenhou o crânio e não se achava presente mais ninguém para fazê-lo. Logo, não fora feito por meios humano não obstante, fora feito.

Nesse ponto de minhas reflexões, esforcei-me por lembrar e lembrei, com inteira exatidão, todos os incidentes que correram por volta do período em apreço. O tempo estava frio (oh! Raro e feliz acaso!) e o fogo ardia na lareira. Eu me achava aquecido pelo exercício e sentei- me perto da mesa. Você, porém, puxara uma cadeira para perto da chaminé. Logo que coloquei o pergaminho em suas mãos, e que você estava a ponto de examiná-lo, Lobo, o meu terra-nova, entrou e pulou sobre seus ombros. Com a esquerda você lhe fez festas e com a direita, que segurava o pergaminho, caiu descuidadamente entre os seus joelhos, bem perto do fogo. Em um momento pensei que as chamas o atingissem e estava quase a avisá-lo quando, antes que tivesse podido falar, você o retirou e entregou-se a examiná-lo.

Quando considerei todos esses pormenores, não duvidei um só momento de que o calor fora o agente que trouxera à luz, no pergaminho, o crânio que eu vira desenhado nele.

Você bem sabe que existem preparados químicos, e sempre existiram desde tempos imemoriais, por meio dos quais é possível escrever sobre papel ou velino, de modo que os caracteres só se tornem visíveis quando submetidos à ação do fogo. O óxido impuro de cobalto, dissolvido em água régia e diluído em quatro vezes o seu peso de água, é às vezes empregado; resulta uma tinta verde. O régulo de cobalto, dissolvido em espírito de nitro, dá uma tinta vermelha. Tais cores desaparecem em intervalos maiores ou menores, depois de efetuada a escrita, com o frio, reaparecem de novo, após a aplicação de calor.

Examinei então a caveira com cuidado. A borda exterior, a borda do desenho mais perto da ponta do velino, era bem mais distinta do que o resto. Claro estava que a ação do calórico fora imperfeita, ou desigual. Acendi fogo imediatamente e submeti todas as partes do pergaminho a um calor ardente. A princípio, o único efeito foi acentuar as linhas fracas do crânio; mas, perseverando na experiência ficou visível, num canto da faixa, diagonalmente, em oposição ao lugar em que se delineara a caveira, a figura do que, a princípio, supus ser uma cabra. Um exame mais acurado, contudo, demonstrou-me que se tratava de um cabrito.

- Ah! Ah! - disse eu. - Sem dúvida não tenho o direito de rir de você. Um milhão e meio em dinheiro é coisa muito séria para brincadeiras. Mas você não vai querer estabelecer um terceiro elo em sua cadeia. Você não vai achar uma relação especial entre seus piratas e uma cabra. Os piratas, como você sabe, não têm nada com as cabras; elas pertencem aos interesses dos fazendeiros.

- Mas eu acabo de dizer que a figura não era a de uma cabra...

- Bem, que seja de um cabrito...é mais ou menos a mesma coisa.

- Mais ou menos, mas não inteiramente - disse Legrand. - Você deve ter ouvido falar

num tal Capitão Kidd. Pela minha parte, considerei logo a figura do animal como espécie de assinatura figurada ou hieroglífica. Digo assinatura porque sua posição no velino sugeriu essa idéia. A caveira no canto diagonalmente oposto tinha do mesmo modo, o aspecto de um sinete, ou selo. Mas fiquei tristemente perturbado com a ausência de mais qualquer coisa, de um corpo para meu imaginado documento, do texto de meu contexto.

- Presumo que você esperava encontrar uma carta entre o sinete e a assinatura. Algo dessa espécie.

- O fato é que me sentia irresistível impressionado com um pressentimento de alguma vasta e boa fortuna pendente. Mal posso dizer porque talvez, afinal de contas, fosse antes um desejo que uma crença real. Mas sabe você que as tolas palavras de Júpiter acerca de ser o escaravelho feito de ouro maciço tiveram notável efeito sobre minha imaginação? E, depois, a de acasos e coincidências... eram todos tão extraordinários! Observe! como, por simples acaso, esses acontecimentos ocorreram no único dia do ano que foi, ou podia ser, suficientemente frio para que acendêssemos fogo, e sem esse fogo, sem a intervenção do cão no momento preciso em que ele apareceu, eu nunca saberia da existência dessa caveira e, assim, nunca seria o possuidor do tesouro.

- Mas, continue... estou impaciente.

- Bem, você naturalmente já ouviu as muitas estórias que correm, esses mil boatos vagos que circulam acerca de dinheiro enterrado em algum ponto da costa atlântica por Kidd e seus associados. Tais boatos devem ter tido alguma base na realidade. E o fato de que eles tenham existido tanto e tão continuamente só podia ter resultado, pareceu-me, da circunstância de que o tesouro enterrado ainda permanecia sepulto. Tivesse Kidd escondido sua pilhagem por algum tempo, retirando-a depois, tais boatos raramente poderiam ter-nos alcançado na sua forma presente e invariável.

- Observe as estórias que se contam são, todas, sobre procuradores de dinheiro e não acerca de achadores de dinheiro. Se o pirata tivesse recuperado seu dinheiro, a questão estaria encerrada. Parece-me que aí algum acidente - digamos a perda de uma nota indicando o local - o privou dos meios de recuperar o tesouro e que esse acidente se tornou conhecido de seus comparsas, que de outro modo nunca poderiam ter ouvido falar, em absoluto, que o tesouro tivesse sido escondido, e que, empregando-se em tentativas inúteis, porque sem guia para reavê-lo, deram origem, primeiramente, e depois divulgação universal, aos relatos que agora são tão comuns. Você já ouviu falar que algum tesouro importante tenha sido desenterrado longo da costa?

- Nunca.

- Mas é bem sabido que a fortuna acumulada por Kidd era imensa. Tomei como certo, portanto, que a terra ainda a conservava escondida. E você mal se surpreenderá se lhe disser que senti uma esperança, quase chegando à certeza, de que o pergaminho estranhamente encontrado

encerrasse o registro perdido do lugar do depósito.

- Mas como você continuou?

- Levei de novo o velino ao fogo, depois de aumentar o calor mas nada apareceu; julguei então possível que a cobertura de sujo podia ter alguma relação com o fracasso; assim, limpei cuidadosamente o pergaminho, derramando água quente sobre ele, e, tendo feito isso, coloquei-o numa caçarola de cobre com o crânio para baixo, e pus a caçarola sobre um fogão com carvão em brasa. Em poucos minutos a caçarola ficou inteiramente aquecida e removi a folha que, com indizível alegria, encontrei salpicada, em diversos com o que me pareceu serem figuras arrumadas em linhas. Coloquei-a de novo na caçarola e deixei que lá ficasse outro minuto. Depois de tirá-la, tudo estava tal como você agora vê.

- E aí Legrand, aquecendo de novo o pergaminho, entregou-o a meu exame. Entre a caveira e a cabra estavam toscamente traçados, em tinta vermelha, os seguintes sinais:

53%%+305))6*;4826)4%.)4%);806*;48+8&60))85;1%(;:%*8+83(88)5*+;46(;

88*96*?;8)*%(;485);5*+2:*%(;4956*2(5*-4)8&8*;4069285);)6+8)4%%;1(%9

;48081;8:8%1;48+85;4)485+528806*81(%9;48;(88;4(%?34;48)4%;161;:188;%?;

- Mas - disse eu, entregando-lhe a folha -, estou no escuro como antes. Esperassem-me todas as jóias de Golconda em troca da solução desse enigma e tenho plena certeza de que seria incapaz de ganhá-las.

- E contudo - falou Legrand a solução de modo algum é tão difícil como você poderia ser levado a imaginar após o primeiro exame apressado dos caracteres. Esses caracteres, como qualquer pessoa pode prontamente verificar, formam uma cifra, isto é, encerram um significado; mas segundo o que se conhece de Kidd, eu não podia supô-lo capaz de compor qualquer espécie de cifra muito complicada. Achei, imediatamente, que esta era duma espécie simples, tal, entretanto, que para a inteligência rude do marinheiro devesse parecer absolutamente insolúvel, sem a chave. E você realmente a decifrou? Com toda a facilidade. Já decifrei outras, dez mil vezes mais complicadas. Certas circunstâncias e certas tendências do espírito levaram-me a interessar-me por semelhantes enigmas e pode-se bem duvidar de que a engenhosidade humana consiga compor um enigma dessa espécie, que a engenhosidade humana não possa decifrar, graças a uma aplicação adequada. De fato, uma vez que tenha eu arranjado caracteres unidos e legíveis, mal ligo importância à simples dificuldade de descobrir-lhe a significação.

- No caso presente - e na verdade em todos os casos de escrita secreta - a primeira questão diz respeito à língua da cifra, pois os princípios de solução, particularmente quando se trata das cifras mais simples, dependem do gênio de cada idioma e podem por isso variar. Em geral não há outra alternativa para quem tenta a decifração, senão experimentar (dirigido pelas probabilidades) cada língua conhecida até que a verdadeira seja encontrada. Mas nesta cifra que temos aqui diante de nós, toda a dificuldade foi removida, graças à assinatura. O trocadilho com

a palavra “Kidd” só é perceptível na língua inglesa. Sem esta consideração, teria eu começado minhas tentativas com o espanhol e o francês, como línguas em que um segredo desta espécie deveria ter sido naturalmente escrito por um pirata dos mares espanhóis. Mas no caso presente, presumi que a cifra estivesse em inglês.

- Você há de notar que não existem divisões entre as palavra. Se as houvesse, a tarefa teria sido relativamente fácil. Em tal caso teria eu começado por fazer uma comparação e análise das palavras mais curtas e, se tivesse encontrado, como é sempre provável uma palavra duma só letra *A* (traduzido do inglês: um) ou *I* (traduzido do inglês: eu), por exemplo, haveria considerado a solução como garantida. Mas, não havendo divisões meu primeiro passo foi averiguar quais as letras dominantes, como as menos freqüentes.

Contando todas, construí a seguinte tábua:

O algarismo 8 ocorre 33 vezes

O sinal ; ocorre 26 vezes

O algarismo 4 ocorre 19 vezes

O sinal % ocorre 16 vezes

O sinal) ocorre 16 vezes

O sinal * ocorre 13 vezes

O algarismo 5 ocorre 12 vezes

O algarismo 6 ocorre 11 vezes

O sinal (ocorre 10 vezes

O sinal + ocorre 8 vezes

O algarismo 1 ocorre 8 vezes

O algarismo 0 ocorre 6 vezes

O algarismo 9 ocorre 5 vezes

O algarismo 2 ocorre 5 vezes

O sinal : ocorre 4 vezes

O algarismo 3 ocorre 4 vezes

O sinal ? ocorre 3 vezes

O sinal & ocorre 2 vezes

O sinal - ocorre 1 vezes

O sinal . ocorre 1 vezes

- Ora, em inglês a letra que maisse encontra é o *E*. As demais ocorrem na seguinte

ordem: *A, O, I, D, H, N, R, S, T, U, Y, C, F, G, L, M, W, B, K, P, Q, X, Z.* A letra *E* é tão singularmente predominante que raras são as frases, de certo tamanho, em que não seja ele a letra principal. Temos, pois, aqui, logo no começo, uma base para algo mais do que uma simples conjetura. É evidente o uso geral que se pode fazer dessa tábua, mas para esta cifra particular só mui reduzidamente nos utilizaremos de seu concurso. Como o algarismo predominante é o 8, começaremos por atribuir-lhe o valor de *E*, do alfabeto natural. Para verificar essa suposição, observemos se o 8 aí aparece muitas vezes aos pares, pois o *E* se duplica, com grande freqüência, em inglês: como, por exemplo, nas palavras *meet*, *fleet*, *speed*, *seen*, *been*, *agree*, etc. No caso presente, vemo-lo duplicada não menos de cinco vezes, embora o criptograma seja curto.

Admitamos, pois, que o 8 seja o *E*. Ora, de todas as palavras da língua, *THE* (traduzido do inglês: a/o) é a mais usual. Vejamos, portanto, se não há repetições e três caracteres na mesma ordem de colocação, sendo o 8 o último dos três. Se descobrirmos repetições de tais letras arranjadas desta forma, elas representarão, mui provavelmente, a palavra *THE*. Examinando-se, encontramos não menos de sete dessas combinações; sendo os caracteres **;48**. Podemos, portanto, supor que **;** representa *T*, **4** representa *H* e **8** representa *E*, estando este último bem confirmado. De modo que um grande passo já foi dado. Tendo determinado uma única palavra, estamos capacitados a determinar um ponto vastamente importante, isto é, muitos começos e fins de outras palavras. Vejamos, por exemplo, a penúltima combinação **;48** ocorre quase no fim da cifra. Sabemos que o sinal **;** que vem logo depois é o começo de uma palavra e, dos seis caracteres que seguem este *THE*, conhecemos cinco. Substituamos, pois, estes caracteres pelas letras que já sabemos que eles representam, deixando um espaço para o que não conhecemos: *T_EETH*.

Aqui já estamos habilitados a descartar-nos do *TH*, como não formando parte da palavra que começa pelo primeiro *T*, pois que temos experimentando sucessivamente todas as letras do alfabeto para preencher a lacuna, que nenhuma palavra pode ser formada em que apareça esse *TH*. Estamos, assim, limitados a *T_EE*, e percorrendo todo o alfabeto, se necessário, como antes, chegamos à palavra *TREE* (traduzido do inglês: árvore) como a única possivelmente certa. Ganhamos assim outra letra, o *R*, representada por **(**, e mais duas palavras justapostas, *THE TREE* (traduzido do inglês: a árvore). Um pouco além destas palavras, a custa distância, vemos de novo a combinação **;48**, e dela nos utilizamos como terminação da que imediatamente a precede. E assim temos este arranjo: *THE TREE* **;(%?34** *THE*, ou, substituindo pelas letras reais os sinais conhecidos, lê-se assim: *THE TREE THR%?3H THE.*

Ora, se em vez dos caracteres desconhecidos, deixarmos espaços em branco ou pontos que os substituam, leremos isto: *THE TREE THR...H THE*, a palavra *THROUGH* (traduzido do inglês: através) se torna imediatamente evidente. Mas esta coberta dá-nos três novas letras: *O*, *U* e *G*, representadas por **%**, **?** e **3**. Procurando agora, cuidadosamente, na cifra, combinações de caracteres conhecidos, descobrimos, não muito longe do princípio, disposição: **83(88**, ou *EGREE*. Isto é, claramente, a conclusão da palavra *DEGREE* (traduzido do inglês: grau) e dá-nos outra letra, o *D*, representada por **+**. Quatro letras além da palavra *DEGREE* notamos a combinação

;46(;88.

Traduzindo os caracteres conhecidos e representando os desconhecidos por pontos, como antes, vemos o seguinte: *TH...RTEE*, combinação que sugere imediatamente a palavra *THIRTEEN* (traduzido do inglês: treze) de novo nos fornece dois novos caracteres: *I* e *N*, representados respectivamente, por **6** e *****. Voltando agora ao princípio do criptograma, observamos a combinação **53‡‡+**.

Traduzindo-a como antes, obtemos *GOOD* (traduzido do inglês: bom).

Isso nos certifica de que a primeira letra é *A* e as primeiras palavras são: *A GOOD* (traduzido do inglês: um bom/uma boa). É tempo, então, de organizar nossa chave com o já descoberto, em forma de uma tábua, para evitar confusões. Tê-la-emos assim:

5 representa *A*

+ representa *D*

8 representa *E*

3 representa *G*

4 representa *H*

6 representa *I*

***** representa *N*

‡ representa *O*

(representa *R*

; representa *T*

? representa *U*

- Temos, portanto, nada menos de onze das mais importantes letras representadas e será desnecessário continuar com os detalhes desta solução. Já lhe disse o bastante para convencê-lo de que as cifras desta natureza são facilmente solúveis e para dar-lhe alguma idéia da análise racional que serve para desenvolvê-las. Mas fique certo de que o espécime presente pertence às mais simples espécies de criptogramas. Agora só resta dar-lhe a tradução completa dos caracteres do pergaminho, depois de decifrados. Aqui está ela:

"A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee-line from the tree through the shot fifty feet out".

(Traduzido do inglês: Um bom vidro no hotel do bispo na cadeira do diabo quarenta e um graus e treze minutos nordeste quadrante norte tronco principal sétimo galho lado leste atirai do olho esquerdo da caveira uma linha de abelha da árvore através do tiro cinqüenta pés distante.)

- Mas - disse eu - o enigma parece ainda em tão má situação como antes. Como é possível extrair um significado dessa trapalhada toda de “cadeira do diabo”, “caveira” e “hotel do bispo”?

- Mas - disse eu - o enigma parece ainda em tão ma situação como antes. Como é possível extrair um significado dessa trapalhada toda de “cadeira do diabo”, “caveira” e “hotel do bispo”?

- Confesso - replicou Legrand - que a questão ainda apresenta um aspecto sério, quando encarada de modo superficial. Minha primeira tentativa foi dividir a sentença nas divisões naturais, pretendidas pelo autor da cifra.

- Pontuá-la, quer dizer?

- Mais ou menos isso.

- Mas como era possível fazê-lo?

- Refleti que o autor fizera questão de amontoar as palavras sem separá-las, para aumentar a dificuldade da tradução. Ora, um homem não demasiado esperto, ao objetivar tal resultado, quase certamente iria além do devido. Quando, no decorrer de sua escrita, a uma parada do assunto, que naturalmente requereria uma pausa ou mesmo um ponto, ele seria mais do que capaz de amontoar as letras nesse lugar, mais do que nas junções anteriores. Se você observar o manuscrito aqui presente, facilmente observará cinco casos de ajuntamento incomum. Partindo dessa sugestão, fiz a divisão seguinte:

A good glass in the bishop’s hostel in the devil’s seat **-** *forty-one degrees and thirteen minutes* **-** *northeast and by north* **-** *main branch seventh limb east side* **-** *shoot from the left eye of the death’s-head* **-** *a bee-line from the tree through the shot fifty feet out.*

(Traduzido do inglês: Um bom vidro no hotel do bispo na cadeira do diabo **-** quarenta e um graus e treze minutos - nordeste quadrante norte - tronco principal sétimo galho lado leste **-** atirai do olho esquerdo da caveira - uma linha de abelha da árvore através do tiro cinqüenta pés distante.)

- Mesmo esta divisão - falei - ainda me deixa no escuro.

- Também me deixou no escuro - replicou Legrand - por poucos dias, durante os quais fiz diligentes pesquisas nas vizinhanças de Sullivan, procurando algum edifício que tivesse o nome de “hotel do bispo”, pois, naturalmente, não me inquietei com a palavra arcaica hostel. Não obtendo qualquer informação a respeito, estava a ponto de estender meu campo de pesquisa e proceder de modo mais sistematizado, quando, certa manhã, tive a bem súbita, de que esse “hotel do bispo” podia referir-se a antiga família Bessop, que, desde tempos remotíssimos, possuía mansão antiga a cerca de quatro milhas a nordeste da ilha.

Em conseqüência, fui até a fazenda e renovei minhas pesquisas entre os mais velhos negros do lugar. Afinal, uma das mulheres mais idosas disse que ouvira falar de um lugar tal como *Bessop’s Castle* (traduzido do inglês: Castelo de Bessop) e achou que me podia levar ao lugar, mas que não se tratava de um castelo nem de uma taverna, mas de um rochedo elevado.

Ofereci-lhe boa paga pelo trabalho e, depois de alguma hesitação, consentiu em acompanhar-me ao local. Encontrando-o sem grande dificuldade, mandei-a de volta e passei a examinar o lugar. O "castelo" consistia num conjunto irregular de penhascos e rochedos, sendo um destes últimos muito digno de nota, por sua altura, bem como por sua aparência isolada e artificial. Subi a seu cume e fiquei sem saber o que devia fazer em seguida.

- Enquanto me ocupava em tal reflexão, caíram meus olhos sobre uma saliência estreita, na face ocidental do rochedo, uma jarda talvez por baixo do cimo em que me achava. Essa saliência projetava-se cerca de dezoito polegadas e não tinha mais de um pé de largura; um nicho no penhasco dava-lhe tosca semelhança como uma das cadeiras de encosto côncavo usadas por nossos antepassados.

- Não duvidei de que ali se achava a "cadeira do diabo" que aludia o documento e pareceu-me então apreender todo o segredo do enigma.

- O "bom vidro", sabia eu, apenas podia referir-se a um binóculo, pois a palavra *GLASS* (traduzido do inglês: vidro) é raramente empregada em outro sentido pelos marinheiros. Logo vi, então, que se devia usar um binóculo, de um ponto de visão definido, não admitindo variação. Não hesitei em acreditar que as frases "quarenta e um graus e treze minutos" e "nordeste quadrante norte" deveriam ser direções para colocação do binóculo. Grandemente excitado por essas descobertas apressei-me em voltar à casa, apanhei um binóculo e regressei ao rochedo.

- Coloquei-me na saliência e verifiquei que era impossível ficar sentado, a não ser uma posição especial. Esse fato confirmou minha idéia preconcebida. Passei a usar o binóculo. Naturalmente, "quarenta e um graus e treze minutos" só podiam aludir à elevação acima do horizonte visual, pois a direção horizontal estava claramente indicada pelas palavras "nordeste quadrante norte". Estabeleci imediatamente esta última direção, por meio de uma bússola de bolso; depois, apontando o binóculo a um ângulo de cerca de quarenta e um graus de elevação, como podia calcular por experiência, movi-o cautelosamente para cima e para baixo, até minha atenção foi detida por uma fenda circular, ou abertura, na folhagem de uma grande árvore, que, à distância, dominava suas companheiras. No centro dessa abertura percebi um ponto branco mas a princípio não pude distinguir de que se tratava. Ajustei o foco do binóculo, olhei de novo e verifiquei então que era crânio humano.

Depois desta descoberta, eu estava confiante em considerar o enigma resolvido, pois a frase "tronco principal, sétimo galho, lado leste" só se podia referir à posição do crânio na árvore, enquanto que "atirai do olho esquerdo da caveira" também apenas admitia uma interpretação em relação à busca do tesouro enterrado. Percebi que a intenção era de lançar uma bala através do olho esquerdo do crânio e que uma "linha de abelha", ou, em outras palavras uma linha reta, tirada do ponto mais próximo da árvore através "do tiro", ou o lugar onde a bala caísse, e daí estendida a uma distância de cinqüenta pés, indicaria um ponto definido. E por baixo desse ponto considerei como pelo menos possível que estivesse oculto um depósito de valor.

- Tudo isso - disse - é excessivamente claro e, embora engenhoso, simples e explícito. Que fez você depois de deixar o "hotel do bispo"?

- Ora , tendo cuidadosamente tomado nota da aparência da árvore, voltei para casa. Logo, porém, que deixei a "cadeira do bispo" a abertura circular desapareceu. Não pude vê-la mais depois, embora me virasse para trás. O que pareceu a principal perícia, em todo esse negócio, foi o fato (pois repetidas experiências me convenceram de que era um fato) de que a abertura circular em questão não é visível de qualquer ponto de visão que se possa alcançar, a não ser o que permite a estreita saliência na face do rochedo. Nessa expedição ao "hotel do bispo", fora eu auxiliado por Júpiter, sem dúvida, observara, nas semanas anteriores, minha atitudes de abstração, tomando especial cuidado em não me deixar só. Mas no dia seguinte, levantando-me muito cedo, escapuli dele e fui às colinas, à procura da árvore. Depois de muito pesquisar, encontrei-a.

- Quando voltei para casa, à noite, meu criado estava resolvido a dar-me uma surra. Do resto das aventuras creio que você sabe como eu.

- Suponho - disse - que você errou o lugar, na primeira tentativa de cavar, por causa da estupidez de Júpiter, deixando o escaravelho cair pelo olho direito, em vez de pelo olho esquerdo do crânio.

- Perfeitamente. Esse engano produziu uma diferença de cerca polegadas e meia no "tiro", isto é, na posição da cavilha mais próxima da árvore; e se o tesouro estivesse por baixo do "tiro" o erro teria sido de pouca importância; mas o "tiro", bem como o ponto mais próximo da árvore eram simplesmente dois pontos para o estabelecimento de uma linha de direção. Naturalmente o erro, embora trivial no começo, aumentava à medida que continuava com a linha e, ao completarmos os cinqüenta pés, ficamos inteiramente fora da direção. Não fossem minhas impressões solidificadas de que o tesouro estava ali realmente enterrado, em alguma parte, poderíamos ter perdido em vão todo o nosso trabalho.

- Mas sua grandiloqüência, sua conduta ao balançar o escaravelho. . . estavam enormemente extravagantes! Eu ficara certo de você enlouquecera. E por que você insistiu em deixar cair o escaravelho, em vez de uma bala, pelo crânio?

- Ora, para ser franco, eu me sentia algo aborrecido com suas evidentes suspeitas, relativamente à minha sanidade mental e resolvi castigá-los calmamente ao meu próprio jeito, com um pouquinho de calculada mistificação. Por esse motivo balancei o escaravelho, e por essa razão fiz com que fosse atirado da árvore observação sua sobre o grande peso dele sugeriu-me essa idéia.

- Sim, percebo! E agora só há um ponto que me embaraça. Que significam os esqueletos encontrados no buraco?

- Essa é uma pergunta a que não sou mais capaz de responder do que você. Parece, contudo, haver apenas um meio plausivel de explicar o caso. . . e, entretanto, é terrível acreditar em atrocidades tal como a implicada em minha hipótese. E claro que Kidd, (se na verdade Kidd

escondeu esse tesouro, coisa de que não duvido)claro que ele deve ter sido auxiliado nesse trabalho. Concluído, porém, o serviço, pode ter ele considerado prudente fazer desaparecer todos os que participavam de seu segredo. Talvez um par de golpes com uma picareta, fosse suficiente, enquanto seus ajudantes se ocupavam em cavar; talvez fossem necessários doze... Quem sabe?

ANEXO

D

CIFRA DE HILL

Essa cifra foi atribuída ao matemático Lester S. Hill que publicou dois artigos nos quais apresentava manipulações matriciais aplicadas na criptografia. Os artigos *'Criptography in an Algebraic Alphabet'* (1929) e *'Concerning Certain Linear Transformation Apparatus of Cryptography'* (1931) foram publicados em diferentes volumes da *American Mathematical Monthly*.

A Cifra de Hill tem como objetivo superar o ponto fraco das cifras de substituição, uma vez que estas preservam a frequência com que suas letras aparecem e, portanto, são decifráveis através de uma análise estatística, Hill propõe que o texto seja dividido em grupos de letras e que tais grupos sejam cifrados.

É necessário que cada letra seja substituída por um valor numérico. A tabela 6 mostra um exemplo possível de substituição.

Tabela 6 – Exemplo de substituição numérica

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Fonte: Anton e Rorres (2001, p. 467).

Passo 1: Escolha uma matriz 2 x 2

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

com entradas inteiras para efetuar a codificação. Tal matriz precisa ser inversível e seu determinante não pode ter fatores primos comuns com 26.

Passo 2: Agrupe letras sucessivas de texto comum em pares, adicionando uma letra adicional fictícia para complementar o último par se o texto comum tem um número ímpar de letras; substitua cada letra de texto comum por seu valor numérico.

Passo 3: Converta cada par sucessivo $p_1 p_2$ de letras de texto comum em um vetor-coluna

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

e forme o produto $A\mathbf{p}$ que será o correspondente vetor cifrado.

Passo 4: Converta cada vetor cifrado em seu equivalente alfabético.

Exemplo

Usaremos a matriz

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

para obter o texto cifrado que corresponda ao texto: "PROFESSOR, VOCÊ MOVE O MUNDO". Devemos ignorar acentos e pontuações.

Vamos reescrever a frase separando-a em pares de letras e encontrar seus valores numéricos correspondentes usando a tabela 6. No caso da frase-exemplo, precisaremos adicionar uma letra adicional fictícia, escolhemos a letra A.

Tabela 7 – Exemplo: agrupamento de letras e correspondentes numéricos

Agrupamento de letras	PR	OF	ES	SO	RV	OC	EM	OV	EO	MU	ND	OA
Correspondente numérico	16 18	15 6	5 19	19 15	18 22	15 3	5 13	15 22	5 15	13 21	14 4	15 1

Fonte: Elaborada pelo autor.

Para codificar o primeiro par de letras PR faremos o produto da matriz A pelo vetor coluna dos valores numéricos correspondentes.

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 16 \\ 18 \end{bmatrix} = \begin{bmatrix} 52 \\ 54 \end{bmatrix}$$

O produto das matrizes resultou em 52 e 54 e estes números não possuem um equivalente numérico segundo a tabela 6. Para resolver este problema, faremos uso da aritmética modular, ou seja, sempre que o resultado da multiplicação for um número maior do que 25, vamos substituir o valor pelo resto de sua divisão por 26. Uma vez que o resto da divisão será sempre um dos

inteiros $0,1,2,\ldots,25$, esta operação sempre fornecerá um número que possui um equivalente alfabético.

Desta forma, o resultado anterior ficará da seguinte forma:

$$\begin{bmatrix} 52 \\ 54 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} (mod\, 26)$$

Observando a tabela 6 temos o seguinte texto cifrado: ZB.

Repetimos a operação para cada vetor-coluna e obteremos os seguintes resultados:

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 6 \end{bmatrix} = \begin{bmatrix} 27 \\ 18 \end{bmatrix} ou \begin{bmatrix} 1 \\ 18 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 57 \end{bmatrix} ou \begin{bmatrix} 17 \\ 5 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 15 \end{bmatrix} = \begin{bmatrix} 49 \\ 45 \end{bmatrix} ou \begin{bmatrix} 23 \\ 19 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 18 \\ 22 \end{bmatrix} = \begin{bmatrix} 62 \\ 66 \end{bmatrix} ou \begin{bmatrix} 10 \\ 14 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 3 \end{bmatrix} = \begin{bmatrix} 21 \\ 9 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 5 \\ 13 \end{bmatrix} = \begin{bmatrix} 31 \\ 39 \end{bmatrix} ou \begin{bmatrix} 5 \\ 13 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 22 \end{bmatrix} = \begin{bmatrix} 59 \\ 66 \end{bmatrix} ou \begin{bmatrix} 7 \\ 14 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 5 \\ 15 \end{bmatrix} = \begin{bmatrix} 35 \\ 45 \end{bmatrix} ou \begin{bmatrix} 9 \\ 19 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 21 \end{bmatrix} = \begin{bmatrix} 55 \\ 63 \end{bmatrix} ou \begin{bmatrix} 3 \\ 11 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 4 \end{bmatrix} = \begin{bmatrix} 22 \\ 12 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 1 \end{bmatrix} = \begin{bmatrix} 17 \\ 3 \end{bmatrix} (mod\, 26)$$

Esses vetores correspondem aos pares de texto cifrado: AR, QE, WS, JN, UI, EM, GN, IS, CK, VL e QC, respectivamente.

Assim, o texto normal “PROFESSOR, VOCÊ MOVE O MUNDO” seria cifrado da seguinte maneira: ZBARQEWSJNUIEMGNISCKVLQC.

Decifrando a Cifra de Hill

Na aritmética usual, cada número não-nulo a tem um *inverso multiplicativo*, denotado por a^{-1}, tal que $aa^{-1} = a^{-1}a = 1$.

Na aritmética modular temos um conceito correspondente: Dado um número a em $\mathbb{Z}_m$, dizemos que um número a^{-1} em $\mathbb{Z}_m$ é um *inverso multiplicativo* de a módulo m se $aa^{-1} = a^{-1}a = 1 \bmod m$.

Pode ser provado que se a e m não tem fatores primos comuns, então a tem um único inverso multiplicativo módulo m; reciprocamente, se a e m têm um fator primo comum, então a não tem recíproco módulo m.

Para referência, oferecemos a seguinte tabela de inversos multiplicativos módulo 26:

Tabela 8 – Inversos multiplicativos módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Anton e Rorres (2001, p. 469).

A fim de decifrar a Cifra de Hill procederemos da mesma maneira, exceto que usaremos a inversa da matriz original módulo 26.

Para isso, usaremos o seguinte resultado: Uma matriz quadrada $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ com entradas em $\mathbb{Z}_{26}$ é invertível módulo 26 se, e somente se, o inverso multiplicativo de $det(A)$ módulo 26 não é divisível por 2 ou 13. A inversa de A módulo 26 será dada por

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

onde $(ad - bc)^{-1}$ é o inverso multiplicativo de $ad - bc$ módulo 26.

Exemplo

Vamos decifrar a mensagem que encriptamos no exemplo anterior: ZBARQEWSJNUI-EMGNISCKVLQC.

Para isso precisamos encontrar a inversa da matriz $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ módulo 26.

Primeiro vamos calcular o determinante de A:

$$det(A) = ad - bc = 1 \cdot 3 - 2 \cdot 0 = 3 - 0 = 3.$$

Como o $det(A)$ não é divisível por 2 ou 13, vamos usar o resultado apresentado anteriormente, segundo a tabela 8, o inverso multiplicativo módulo 26 de 3 é 9. Assim,

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = 9 \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} (mod\, 26)$$

Conferindo,

$$AA^{-1} = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 26 \\ 0 & 27 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\, 26)$$

De forma análoga, temos que $A^{-1}A = 1(mod\, 26)$.

Vamos reescrever a frase separando-a em pares de letras e encontrar seus valores numéricos correspondentes usando a tabela 6.

Tabela 9 – Exemplo: agrupamento de letras e correspondentes numéricos

Agrupamento de letras	ZB	AR	QE	WS	JN	UI	EM	GN	IS	CK	VL	QC
Correspondente numérico	26	1	17	23	10	21	5	6	9	3	22	16
	2	18	5	19	14	9	13	14	19	11	12	3

Fonte: Elaborada pelo autor.

Para decodificar o texto faremos o produto da matriz A pelo vetor coluna dos valores numéricos correspondentes.

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 26 \\ 2 \end{bmatrix} = \begin{bmatrix} 42 \\ 18 \end{bmatrix} ou \begin{bmatrix} 16 \\ 18 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} 145 \\ 162 \end{bmatrix} ou \begin{bmatrix} 15 \\ 6 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 5 \end{bmatrix} = \begin{bmatrix} 57 \\ 45 \end{bmatrix} ou \begin{bmatrix} 5 \\ 19 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 23 \\ 19 \end{bmatrix} = \begin{bmatrix} 175 \\ 171 \end{bmatrix} ou \begin{bmatrix} 19 \\ 15 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 10 \\ 14 \end{bmatrix} = \begin{bmatrix} 122 \\ 126 \end{bmatrix} ou \begin{bmatrix} 18 \\ 22 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 21 \\ 9 \end{bmatrix} = \begin{bmatrix} 93 \\ 81 \end{bmatrix} ou \begin{bmatrix} 15 \\ 3 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 5 \\ 13 \end{bmatrix} = \begin{bmatrix} 109 \\ 117 \end{bmatrix} ou \begin{bmatrix} 5 \\ 13 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} 119 \\ 126 \end{bmatrix} ou \begin{bmatrix} 15 \\ 22 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 19 \end{bmatrix} = \begin{bmatrix} 161 \\ 171 \end{bmatrix} ou \begin{bmatrix} 5 \\ 15 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{bmatrix} 91 \\ 99 \end{bmatrix} ou \begin{bmatrix} 13 \\ 21 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 22 \\ 12 \end{bmatrix} = \begin{bmatrix} 118 \\ 108 \end{bmatrix} ou \begin{bmatrix} 14 \\ 4 \end{bmatrix} (mod\, 26)$$

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 3 \end{bmatrix} = \begin{bmatrix} 41 \\ 27 \end{bmatrix} ou \begin{bmatrix} 15 \\ 1 \end{bmatrix} (mod\, 26)$$

Esses vetores correspondem aos pares de texto decifrado: PR, OF, ES, SO, RV, OC, EM, OV, EO, MU, ND, OA respectivamente.

Assim, o texto cifrado ZBARQEWSJNUIEMGNISCKVLQC foi decifrado gerando o seguinte texto PROFESSORVOCEMOVEOMUNDOA, tirando a letra fictícia que foi adicional ao final do texto, teremos a frase original: “PROFESSOR, VOCÊ MOVE O MUNDO”.


ICMC
USP
SÃO CARLOS