PROFMAT – Mestrado Profissional em Matemática em Rede Nacional

Universidade Federal Fluminense

Criptologia - O oculto estimulando o ensino de Matemática

Leandro Freitas de Queiroz

Orientadora: Miriam del Milagro Abdon

Niterói

Março / 2013

PROFMAT – Mestrado Profissional em Matemática em Rede Nacional

Universidade Federal Fluminense

Criptologia - O oculto estimulando o ensino de Matemática

Leandro Freitas de Queiroz

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática, PROFMAT – UNIVERSIDADE FEDERAL FLUMINENSE, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Miriam del Milagro Abdon

Niterói

Março / 2013

Ficha catalográfica elaborada pela Biblioteca de Pós-graduação em Matemática da UFF

Q384 Queiroz, Leandro Freitas de Queiroz
Criptologia – o oculto estimulando o ensino de matemática / Leandro Freitas de Queiroz. – Niterói, RJ : [s.n.], 2013.
60 f.

Orientador: Profª. Miriam del Milagro Abdón
Dissertação (Mestrado Profissional em Matemática em Rede Nacional PROFMAT) – Universidade Federal Fluminense, 2013.

1. Criptografia. 2.Ensino de matemática. I. Título.

CDD512.7

DEDICATÓRIA

Agradeço a Deus e minha família, em especial meu pai, minha mãe, minha esposa sempre presente e ao meu querido filho Victor.

RESUMO

Criptologia- O oculto estimulando o ensino de Matemática

Leandro Freitas de Queiroz

Orientadora:

Miriam del Milagro Abdon

O início da criptologia está associado à curiosidade humana e o seu anseio por descobrir o que está oculto. As civilizações antigas e as atuais, por razões mais diversas possíveis, buscam meios de ocultar suas mensagens. Neste trabalho, faremos uma viagem histórica e analisaremos os primeiros processos de encriptação de mensagens. Veremos também o surgimento, o desenvolvimento e as aplicações das cifras desde épocas mais remotas até os dias atuais. Durante o decorrer do trabalho, apresentaremos vários processos de cifragem, desde a cifra de César ao todo poderoso código RSA. Veremos também os avanços deixados pela criptologia na construção de computadores e nos algoritmos criados tanto para a codificação como para a decodificação. Após analisarmos cada cifra e seu processo histórico, buscaremos estabelecer uma relação entre elas e um determinado conceito matemático, buscando através de atividades, estimular nossos alunos para que estes possam desenvolver a disciplina de uma maneira mais prática e dinâmica, tornando o aprendizado mais interessante e inserido em um determinado momento histórico de nossa civilização.

Palavras-chave: criptografia; códigos; cifras.

Niterói

Março/ 2013

ABSTRACT

Cryptology - The hidden stimulating the teaching of Mathematics

Leandro Freitas de Queiroz

Advisor:

Miriam del Milagro Abdon

The start of cryptology is associated with human curiosity and their desire to discover what is hidden. Ancient civilizations and current, for several possible reasons, seek ways to hide your messages. In this paper, we will make a historic trip and we will analyze the first processes of encrypting messages. We will also see the emergence, development and applications of figures from earliest times to the present day. During the course of our work, we present various processes of encryption, since the Caesar cipher to the almighty RSA code. We will also see the advances in cryptology left by building computers and algorithms created both for encoding and for decoding. After reviewing each figure and its historical process, we will seek to establish a relationship between them and a particular mathematical concept, searching through activities, encouraging our students so that they can develop the discipline of a more practical and dynamic, making learning more interesting and inserted in a given historical moment of our civilization.

Keywords: cryptography; codes; ciphers.

Niterói

March/2013

Sumário

Introdução

O surgimento da criptologia está intimamente associado à necessidade de nossa sociedade em esconder o conteúdo descrito em uma determinada mensagem. Para tanto, tornou-se necessária a confecção de algoritmos que pudessem modificar o corpo da mensagem. Estes algoritmos podem ser chamados de cifras e estão presentes no processo de codificação. Com o passar do tempo, da mesma forma que alguns buscavam ocultar o conteúdo de uma mensagem, outros buscavam revelar este conteúdo. Surgia assim o processo de decodificação. Naturalmente, com o passar dos séculos, os processos de codificação e decodificação caminharam juntos e progrediram paralelamente e atingiram um grau de sofisticação elevado. Estes processos são na verdade ramificações da criptologia e a codificação e a decodificação são chamadas de criptografia e criptanálise, respectivamente. Inicialmente, a criptologia era considerada uma magia e atualmente uma ciência.

A criptografia consiste no método de se codificar uma mensagem de maneira que apenas o destinatário possa decifrá-la, enquanto a criptanálise representa justamente o caminho contrário, ou seja, visa decodificar a mensagem de maneira a torná-la pública. Mais especificamente, a criptografia é a ciência ou arte de escrever em códigos ou cifras. Os códigos representam o alfabeto utilizado para a codificação da mensagem, as cifras representam o processo de codificação e são na verdade uma espécie de algoritmo.

A criptologia se desenvolveu através do tempo de acordo com as necessidades e com os avanços tecnológicos de nossa sociedade. A constante briga entre codificar e decodificar fez com que este processo evoluísse de maneira extraordinária. Ao estudarmos as civilizações antigas, veremos que estas faziam uso de formas bastante rudimentares que envolviam conceitos matemáticos bem simples. Ao estudarmos o cenário atual veremos que todo este processo se modificou radicalmente e a matemática aplicada para a confecção de códigos se tornou bem mais sofisticada.

No decorrer desta dissertação veremos que foram realizadas pesquisas sobre os tipos de cifras mais conhecidas. Veremos também algumas de suas aplicações no processo histórico e moldaremos suas aplicações para sala de aula. Iniciamos a confecção deste trabalho com a primeira forma de cifra que se tem conhecimento até as cifras utilizadas nos dias atuais. No contexto deste trabalho poderemos verificar o progresso de nossas civilizações paralelamente aos avanços nos campos referentes à tecnologia.

Objetivos

O principal objetivo deste trabalho é realizar o estudo das técnicas de criptologia, com foco voltado para a criptografia, a fim de utilizá-las em atividades desenvolvidas para a sala de aula. Com o decorrer da apresentação das cifras, e por intermédio de seus refinamentos, podemos utilizar seus conceitos em atividades que podem englobar todos os níveis de conhecimento matemático. Desta forma, nossa expectativa é que todas as séries possam ser contempladas com este trabalho. Os mistérios e as curiosidades que envolvem os processos de codificação e decodificação, assim como a contextualização histórica e a interdisciplinaridade, visam estimular nossos alunos para que o tema se torne mais prazeroso e possa se constituir em uma forma mais fácil de aplicação. Entendemos que estas aplicações possam ampliar a visão de nossos alunos em conceitos matemáticos cada vez mais importantes.

Estrutura do trabalho

Esta dissertação está organizada em cinco capítulos. No primeiro capítulo são apresentadas as origens da criptologia, a sua utilização pelas primeiras civilizações e as principais definições dos conceitos relativos ao tema. Nos capítulos 2, 3, 4, veremos as formas de cifragem, desde as mais rudimentares (utilizadas por sociedades antigas), como as mais sofisticadas (utilizadas atualmente). Analisaremos também as metodologias apresentadas em cada período histórico para que a sociedade vigente pudesse fazer uso da criptologia. No capítulo 5 apresentaremos uma atividade aplicada em sala de aula referente ao uso da criptologia e registraremos os benefícios usufruídos por nossos alunos.

Capítulo I - História da criptologia

Este capítulo é de vital importância para o entendimento do conteúdo deste trabalho e está dividido em duas seções. Na primeira, apresentamos as divisões da criptologia e suas correspondentes ramificações. Na segunda seção, apresentamos os conceitos, as diferenças e alguns exemplos encontrados na história referentes às ramificações da criptologia chamada de criptografia.

I.1 Origens da criptologia

A chamada criptologia existe desde tempos remotos e sua relação com a aritmética matemática é evidente. Em tempos não muito antigos a criptologia era classificada como magia, alguns a consideravam também como arte. Em nosso cenário atual passou a ser considerada como ciência.

Esta ciência se divide em duas áreas: a criptografia e a criptanálise. A criptografia é o ramo da criptologia responsável pela codificação da mensagem, ao passo que a criptanálise é referente ao ramo da criptologia responsável pela decodificação da mensagem.

A criptografia por sua vez se divide em códigos, cifras. Estas cifras se subdividem ainda em várias categorias que serão analisadas no decorrer do trabalho.

I.2 Criptografia

A criptografia é considerada por muitos autores como muito antiga, alguns acreditam que ela pode ser considerada tão antiga quanto a própria escrita. Segundo Jorge Loureiro Dias, em seu artigo Desenvolvimento Histórico da Criptografia, a primeira forma de criptografia registrada ocorreu por volta de

1900 a.C, em uma vila egípcia chamada de Menet Khufu. Neste local, o escriba Khnumhotep II, servo do faraó Amenenhet II, teve a ideia de substituir alguns trechos das escritas em argila, que indicavam o caminho para os tesouros do faraó contidos em sua pirâmide. O servo realizou esta substituição para que apenas os sacerdotes pudessem decifrar as mensagens. Vale salientar que esta forma de criptografia era bastante rudimentar, já que a maioria da população egípcia não sabia ler ou escrever. Existia ainda uma parcela da população que se comunicava pelo que era chamada de egípcio demótico. Este tipo de escrita era utilizada para relatar assuntos cotidianos e consistia em uma forma de escrita mais simplificada em relação à escrita hieroglífica. Apenas a parcela mais nobre da população, que era considerada como “ iluminada”, possuía acesso aos hieróglifos e os utilizava para assuntos religiosos e oficiais.

Os escribas Hebreus por volta de 600 a.C e 500 a.C também fizeram uso da criptografia e utilizaram uma cifra chamada Atbash para escreverem algumas partes do Livro de Jeremias.

Podemos considerar como outro exemplo de codificação de mensagens, datada de 200 d.C., o que ficou conhecido como Quadrado Latino ou fórmula Sator. Esta forma de codificação foi encontrada em muitos lugares da antiguidade e revela-se ainda de forma misteriosa, tanto na sua criação como também em sua localidade original. Estudiosos antigos acreditam que este quadrado era colocado em casas que ofereciam refúgio aos cristãos.

A fórmula Sator era constituída de uma série de palavras de cinco letras agrupadas de maneira a formar um quadrado. Este modelo constitui-se em um exemplo de cifra de transposição, isto é, esconde uma mensagem que pode ser encontrada através da transposição das suas letras. O quadrado latino foi encontrado em paredes de residências romanas em Pompéia, nas ruínas de Cirencester na Inglaterra, no castelo de Rochemaure, na abadia de Collepardo em Santiago de Compostella e em uma série de locais em todo o mundo.

No quadrado, Figura 2, podemos ler: 'rotas opera tenet arepo sator'. Observando a estrutura do quadrado, nota-se que ele é absolutamente

simétrico, sendo assim pode ser lido da esquerda para a direita, da direita para a esquerda, de cima para baixo e de baixo para cima.

Figura 1

Embora este modelo esteja atrelado ao passado cristão, muitos historiadores acreditam que o Quadrado Latino é mais antigo do que a Igreja Católica, fato que aumenta mais o mistério quanto suas origens.

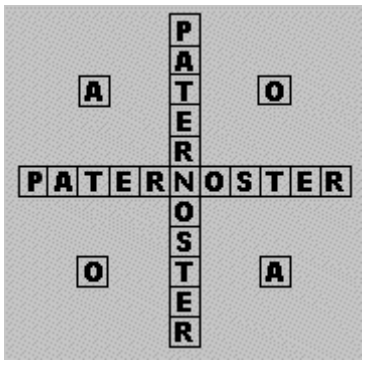


Figura 2

Muitas foram às maneiras de interpretá-lo e várias pesquisas foram realizadas para que seu mistério fosse desvendado. Este é um mistério até para os conhecedores do latim, pois as palavras arepo e rotas não tem significado direto. Porém, analisando o texto percebe-se que rotas é o contrário de sator e arepo de opera, formando assim somente 3 palavras: sator opera tenet. Traduzindo assim, encontraríamos a seguinte frase: “O semeador segura

sua obra em sua mão". Entre os anos de 1924 e 1927, três eruditos descobriram, independentemente, que as letras podiam ser rearranjadas em forma de cruz (Chr. Frank, Deutsche Gaue 25 (1924), 76; F. Grosser, "Ein neuer Versuch zur Deutung der Sator-Formel", Z.N.W. 24 (1926), 165ff.; S. Agrell, "Runornas talmystik och dess antika förebild", Skrifter utgivna av Vetenskaps-Societen i Lund 6(1927), 31f.).

Observe o que acontece quando as letras são rearranjadas e ocupam novas posições:

1. Pater noster, que significa Pai Nosso acaba se repetindo por duas vezes.

2. Os Pater noster estão dispostos em forma de cruz, que tem significado cristão.

3. Além disso, aparecem as letras A e O, que são originadas de alfa e ômega e que também possuem um significado cristão, a letra A refere-se ao começo (alfa) e a letra O refere-se ao fim (ômega).

Veja na figura 4, um exemplo de quadrado latino exposto no Manchester Museum, Universidade de Manchester.

Figura 4

Mas não é só de Pater noster que vive a fórmula Sator. Vários outros "significados" foram encontrados.

Os do lado do bem:

- Oro te, pater, oro te, pater, sanas
- O pater, ores, pro aetate nostra
- Ora, operare, ostenta te, pastor
- Retro Satana, toto opere asper

Os do lado do mal:

- Satan oro te, pro arte a te spero
- Satan, ter oro te, opera praesto
- Satan, oro te, reparato opes

Em 1902, Bartl, diretor de escola da cidade de Übersee am Chiemsee, resolveu ir à igreja de São Pedro no topo da montanha Westerbuchberg. Esta era uma pequena capela, originalmente românica, decorada com afrescos românicos e góticos. Nela havia um quadro de Anna Selbdritt, emoldurado com arabescos singulares, os quais o diretor queria copiar.

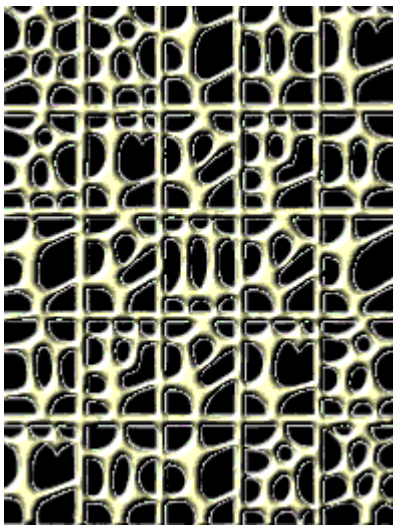


Figura 5: (Letras góticas nos arabescos da moldura do quadro de Anna Selbdritt)

Ao fazer o desenho, acabou desvendando um segredo: as áreas brancas do ornamento se revelaram como letras góticas minúsculas, com a seguinte inscrição:

sator - arepo - tenet - opera - rotas

As palavras coincidem exatamente com as utilizadas no quadrado latino. Desta forma, vários questionamentos foram lançados: qual era a real intenção do pintor? a aparição desta frase constituía-se em uma brincadeira ou o pintor fez uso apenas de um molde antigo? Ou ainda quem sabe o pintor não queria deixar registrada uma mensagem para os iniciados na abóbada da capela?

Perguntas e mais perguntas. O fato é que, até os dias atuais, a fórmula Sator conserva sua aura de enigma e segredo.

Outra curiosidade acerca da fórmula de Sator é que muitas simpatias e rezas da medicina popular são finalizadas com as palavras presentes no quadrado latino, seja para "curar" doenças de humanos ou de animais. Na antiguidade acreditava-se até que esta fórmula fosse infalível em casos de incêndio. Só era preciso pegar um pratinho de estanho, escrever rapidamente a fórmula dos dois lados e jogá-lo no fogo. Ainda no ano de 1742 existia em Sachsen, na Alemanha, uma ordem para manter tais pratinhos em estoque (em casa e nos edifícios públicos) com a finalidade de poder se defender de incêndios.

Vale ressaltar, que nestes casos, a fórmula é utilizada como um tipo de magia, suas aplicações muitas vezes acabaram se tornando fantasiosas. Na verdade, a fórmula Sator era associada à chamada magia branca da Idade Média. Ao contrário da magia negra, associada ao demônio e ao mal, a magia branca estava associada ao bem e “chamava” Cristo para ajudar. Este tipo de magia era utilizada em rituais de curas ou rituais criados para espantar o mal. Pelo menos, esta era a opinião da época. Na maioria das vezes, esta *arte* era exercida nos conventos, principalmente pelos frades que possuíam menos estudos. É deste período que se originaram receitas mágicas, que ainda são usadas hoje em dia. Mas não é aqui que termina a história da fórmula Sator.

Um amuleto da Ásia Menor, datado do século V, contém estas mesmas palavras. O verso deste amuleto de bronze é enfeitado com peixes, o que faz supor uma simbologia cristã. Neste caso, a fórmula parece ter sido utilizada como oração.

A fórmula Sator também é encontrada voltando-se ainda mais no tempo. Nas escavações feitas em Pompéia, que sabidamente foi coberta pelas cinzas de uma erupção do Vesúvio no ano de 79 d.C., Matteo della Corte encontrou esta fórmula peculiar rabiscada numa coluna. Novamente a dúvida estava presente, será que esta inscrição foi feita pelos primeiros cristãos antes da catástrofe ou será que se origina de cristãos do século III, os quais saqueavam tesouros das casas soterradas? São outras perguntas que continuam sem resposta.

Figura 6 (Inscrição em coluna de Pompéia data de 76 d.C.)

Quanto à mensagem, estas palavras não têm um significado claro, mesmo para quem domina o Latim. As palavras arepo e rotas são o maior problema. No entanto, analisando-as com mais cuidado, percebe-se que arepo é apenas o contrário de opera e que rotas é o contrário de sator. Então, na realidade, existem apenas três palavras: sator opera tenet.

Durante a história existiram vários tipos de interpretações e significados para o Quadrado Latino, mas o fato é que este formato de criptografia ainda gera grande controvérsia nos dias atuais.

As técnicas de criptografia, assim como as técnicas que buscavam ocultar mensagens, se estenderam pela idade média, moderna e atual. Os períodos de guerra acabaram contribuindo ainda mais para os avanços e a consequente dificuldade em obter a mensagem original. Atualmente estas técnicas evoluíram com a utilização de computadores e algoritmos cada vez mais sofisticados, que dificultam ao extremo as formas de decodificação de mensagens e arquivos.

Capítulo II - Cifras clássicas

Neste capítulo, apresentaremos as cifras clássicas. Estudaremos as diferenças entre as cifras de substituição e transposição. Veremos também as classificações entre as cifras de substituição monoalfabéticas e polialfabéticas. Analisaremos alguns exemplos e algumas atividades que podem ser utilizadas em sala de aula.

As definições deste capítulo foram retiradas do seguinte trabalho: (http://www.cic.unb.br/docentes/pedro/segdados_files/CriptSeg1-2.pdf)

II.1 Cifras de substituição

As cifras de substituição caracterizam-se pela substituição de cada caracter do texto pleno por outro caracter do texto cifrado. Texto pleno é a mensagem antes de receber a codificação, ou seja, o texto original. Este texto também pode ser chamado de texto puro. Para efetuar esta substituição torna-se necessária a confecção de uma tabela. Esta tabela precisa estabelecer uma relação biunívoca entre a letra a ser cifrada e sua letra, número ou código correspondente no que é chamado de alfabeto cifrante. Por intermédio destes códigos é realizada a cifragem da mensagem, em outras palavras a mensagem original é substituída por uma mensagem codificada. Para que o destinatário recupere o texto pleno é necessário apenas realizar a inversão do processo utilizado na codificação. É claro que existem diferentes técnicas que abrangem a substituição dos caracteres da mensagem original, sendo assim a pessoa que deseja realizar a decodificação da mensagem precisa em primeiro lugar identificar o processo efetuado.

As cifras de substituição podem ser classificadas em dois tipos. Estes processos são nomeados como cifras de substituição monoalfabéticas e cifras

de substituição polialfabéticas, esta diferença ocorre de acordo com o número de alfabetos cifrantes utilizados no processo de codificação.

II.1.1 Cifras de substituição monoalfabéticas

Uma cifra de substituição monoalfabética é uma cifra na qual cada caracter do texto original é substituído por um caracter do texto cifrado. Esta cifra recebe o nome de monoalfabética porque para utilizá-la fazemos uso de apenas um alfabeto cifrante. Para efetuarmos a codificação por intermédio deste tipo de cifra é necessária a existência de uma tabela de substituição. Esta tabela relaciona os caracteres do texto original com os caracteres do alfabeto cifrante.

Vale ressaltar que esta técnica não possui muita eficácia no que tange à sua segurança. Isto ocorre em função deste método ser baseado no uso de uma relação biunívoca, ou seja, se uma das letras referente à codificação for quebrada, todas as demais estariam desprotegidas, desta forma acabariam sendo descobertas.

A criptografia de César

Com o intuito de proteger e garantir a confidencialidade no envio de suas mensagens, o imperador romano Júlio César fez uso de técnicas de criptografia durante o período de guerras. Sua cifra pode ser classificada como uma cifra de substituição monoalfabética e sua técnica ficou conhecida como “Cifra de César”. O método utilizado por Júlio César consistia em substituir as letras da mensagem original por letras situadas três casas mais a frente no próprio alfabeto do texto original, ou seja, Júlio César utilizava o mesmo alfabeto para escrever a mensagem original e para realizar a cifragem desta mesma mensagem. Atualmente se denomina código de César qualquer cifra na qual cada letra da mensagem original seja substituída por outra letra deslocada sempre em um número fixo de posições.

A cifra de César, embora para a época representasse uma metodologia avançada, na época atual é considerada bastante frágil. Para revelar a mensagem camuflada basta que o inimigo após interceptar a mensagem verifique o padrão posicional utilizado. Portanto, caso o inimigo interceptasse uma mensagem e descobrisse uma das letras originais todas as demais seriam descobertas. A relação que Júlio César estabelecia entre os alfabetos pode ser verificada na Tabela 1.

Tabela 1

Texto simples	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
Cifra	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

O interessante é que apesar de sua simplicidade, o código de César acabou sendo utilizado em períodos posteriores. Podemos citar a utilização deste código pelo exército americano durante a guerra de Secessão (esta guerra iniciou-se em 1861 e terminou em 1865) e pelo exército russo, que a utilizou por volta de 1915.

Esta cifra é interessante e pode ser trabalhada em sala de aula. Sua parte histórica é bastante rica e, matematicamente, ela pode dar a ideia aos alunos das noções básicas de posicionamento, fato muito importante na execução de algoritmos básicos referentes às quatro operações. Podemos também utilizá-la de forma a fomentar curiosidade e interesse de nossos alunos a cifras mais complexas, que fazem uso de uma matemática mais avançada. Para tanto, podemos iniciar este trabalho por intermédio de algumas atividades básicas relativas a esta cifra, sempre visando estimular o público alvo a aprender o conceito de criptografia. Estas atividades propostas visam despertar seus interesses e possuem um propósito mais dinâmico durante as aulas. Algumas atividades simples que envolvem as cifras de César são apresentadas a seguir.

Atividade 1:

Cifre a mensagem abaixo usando o código de Júlio César:
"VAMOS AO CINEMA".

Texto simples	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
Cifra	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

Para cifrar esta mensagem basta ao aluno entender a relação entre o posicionamento das letras. O importante é que estas relações podem iniciar o aprendizado de relações biunívocas.

De acordo com a tabela1, os alunos devem representar a seguinte mensagem:

Resposta **: YDPRV DR FLQHPD**

Atividade 2:

Decifre a mensagem:

OHJDO FRQVHJXL

Para realizar esta atividade basta o aluno empregar o inverso do caminho utilizado na primeira atividade. Sendo assim podemos trabalhar com nossos alunos o primeiro conceito referente à ideia de uma função inversa.

Como solução da atividade os alunos devem apresentar a seguinte mensagem:

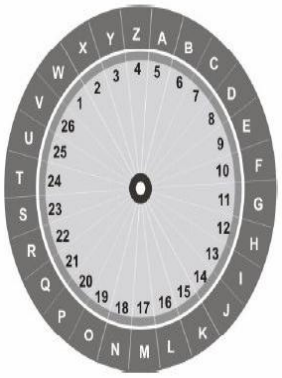
Resposta: LEGAL CONSEGUI

Atividade 3:

Esta atividade é um pouco mais complexa e foi extraída da Terceira Olimpíada Brasileira de Matemática das Escolas Públicas

3ª OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS
OBMEP 2007
Somando novos talentos para o Brasil

(2) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.



(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique *OBMEP* usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras *A*, *B* e *C* é 52. Qual é essa chave?

Estas atividades, como já foi relatado, são importantes porque servem como base para algumas de nossas definições futuras. Para alunos de nono ano e primeiro ano do ensino médio, podemos mostrar que existem relações biunívocas entre as letras, estabelecendo o alfabeto vigente como domínio e contradomínio e conjunto imagem, estendendo a estas relações o conceito de função, assim como suas classificações em injetora, sobrejetora e bijetora.

Para alunos de um nível mais elevado, que quiserem expandir seus conhecimentos matemáticos, bem como para aqueles que estudam os critérios de divisibilidade e seus restos, podemos representar a cifra de César por uma aritmética modular. Para isto poderíamos estabelecer a seguinte relação entre nosso alfabeto e nosso sistema de numeração :

A → 0 E → 4 I → 8 M → 12 Q → 16 U → 20 Y → 24

B → 1 F → 5 J → 9 N → 13 R → 17 V → 21 Z → 25

C → 2 G → 6 K → 10 O → 14 S → 18 W → 22

D → 3 H → 7 L → 11 P → 15 T → 19 X → 23

A equação da criptografia

c=(k+n) mod 26 =

$$\begin{cases} k+n, se\ 0 \leq k+n \leq 25 \\ k+n-26, se\ k+n \geq 26 \end{cases}$$

Onde,

c = Letra cifrada
k = Deslocamento
n = Letra correspondente ao texto puro

O operador **mod** é o resto da divisão por 26, e utilizamos o número 26 porque este representa a quantidade de letras presentes em nosso alfabeto.

Muito embora a aritmética modular seja apresentada em séries de nível mais alto, poderíamos mostrar a nossos alunos seu funcionamento.

Exemplo de como é a letra S cifrada:

Na equação o símbolo k representa o deslocamento utilizado na cifra a qual queremos utilizar, podemos então utilizar o valor 3, referente a cifra de César.

O símbolo n corresponde ao posicionamento da letra pura. No caso, como queremos cifrar a letra S, basta utilizarmos como valor para tal o número 18, que é a posição que a letra S ocupa na tabela.

c=(k+n) mod 26
c=(3+18) mod 26
c=21 mod 26 , o resto da divisão de 21 por 26 é o próprio 21, assim
c=21
Na lista 21 = V
Portanto, S é cifrada em V.

O mod é importante para as últimas letras do alfabeto, tipo Y, a fim de criar uma condição cíclica. Vejamos no exemplo a seguir.

Exemplo de como é a letra Y cifrada:

A letra Y é associada na tabela ao número 24, sendo assim o símbolo n será substituído por este número. Assim, temos :

c=(3+24) mod 26
c=27 mod 26
Neste caso, temos a condição de que (K+n) ≥ 26, portanto 27-26 = 1, isto é, porque a divisão de 27 por 26 deixa resto 1.
c= 1 mod 26
c=1
Na lista 1 = B
Portanto Y é cifrada como B.

A criptografia Atbash

A criptografia Atbash surge por volta do ano 600 a.C e foi criada pelos Hebreus. Este modelo, assim como a cifra de César, é classificado como uma cifra monoalfabética. Neste formato, a primeira letra do alfabeto é trocada pela última letra do próprio alfabeto, a segunda letra é trocada pela penúltima e assim sucessivamente. O nome desta cifra advém de quatro letras pertencentes ao alfabeto hebraico, são elas: Aleph (primeira letra), Taw (última letra), Beth(segunda letra) e SHin (penúltima letra).

Esta cifra foi muito utilizada na confecção de textos religiosos, entre eles o livro de Jeremias. Aplicando o sistema do Atbash ao alfabeto latino, obtemos a seguinte tabela de substituição:

Tabela 2

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

Note que na Tabela 2 existe reciprocidade, ou seja, Z substitui A e A substitui Z. O Atbash é uma cifra reversível, isto porque aplicando-se a mesma cifra ao texto cifrado obtém-se o texto original, sendo assim também se constitui numa cifra de fácil decodificação. Observe um exemplo de encriptação:

Texto Original: BOM DIA
Texto Cifrado: YLN WRZ

Estas cifras também são interessantes e podemos sugerir algumas atividades para sala de aula, estas atividades acabam se concentrando apenas na troca de posição entre algarismos.

Atividade 4 :

Decifre a seguinte mensagem utilizando a tabela de substituição Atbash :

L EVMGL HLKIZ

Resposta : O VENTO SOPRA

Código de Polybius

Existem cifras de substituição em que o texto original é dividido em blocos de caracteres, cada bloco de caracter formado é cifrado em um grupo. Vale ressaltar que o número de símbolos utilizado na cifragem é exatamente igual ao número de símbolos da mensagem original, sendo assim o tamanho da mensagem cifrada é exatamente igual ao tamanho da mensagem original.

Desta forma enquanto nas cifras anteriores as letras eram cifradas individualmente, nesta cifra obtemos uma cifragem não individual. Logo, um bloco de letras como ABR pode corresponder a um bloco que também precisa possuir 3 letras, estas podem ser MNR, PFR ou quaisquer 3 letras dependendo da forma executável da cifra utilizada.

Um dos exemplos para esta cifra é a ideia inicial do código de Polybius. Neste código, o alfabeto era distribuído em uma tabela que possuía 5 linhas e 5 colunas e cada letra recebia uma numeração específica relativa à sua posição na tabela. O primeiro número correspondia à posição da linha, enquanto o segundo número era correspondente à posição da coluna em que a letra se encontrava.

Tabela 3

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Como podemos verificar na Tabela 3, a letra A seria substituída por 11 (primeira linha e primeira coluna), a letra B seria substituída por 12 (primeira linha e segunda coluna) e assim por diante.

Atividade 5 :

Por intermédio do quadrado de Polybius, cifre a seguinte mensagem :

SOCIEDADE SECRETA

S, corresponderia a 43

O, corresponderia a 34

C, corresponderia a 13

I, corresponderia a 24

E, corresponderia a 15

D, corresponderia a 14

A, corresponderia a 11

R, corresponderia a 42

T, corresponderia a 44

Após as relativas correspondências serem efetuadas obtemos como mensagem cifrada : 43 34 13 24 15 14 11 14 15 43 15 13 42 15 44 11.

Para que algum curioso decifre o código, basta através das posições reveladas pelos algarismos encontrar as letras correspondentes.

Cifra de Bacon

Um outro processo utilizado para cifras de substituição, consistia na substituição de um caracter por um grupo de símbolos ou letras. Diferentemente das cifras anteriores, a letra ou símbolo original pode ser substituída por um grupo de letras ou por um grupo de símbolos referentes ao alfabeto cifrante. Este fato acaba fazendo com que a mensagem cifrada torne-se maior do que a mensagem original.

Uma criptografia muito interessante que abrange a forma tomográmica e também faz uso da técnica conhecida como esteganografia é a chamada cifra de Bacon, esta cifra foi criada pelo filósofo inglês Francis Bacon, por volta do ano 1600. Outra característica marcante desta cifra é a utilização dos números binários. Para que possamos entendê-la melhor, antes faremos um estudo sobre o sistema binário.

Números Binários

Em nosso sistema de numeração, utilizamos os algarismos de 0 a 9 como formadores de todos os nossos números. Desta forma, nosso sistema de numeração é conhecido como decimal (decimal porque possui 10 algarismos e através destes 10 algarismos podemos formar qualquer número em nosso sistema de numeração). O sistema binário recebe este nome porque neste sistema existem apenas dois algarismos formadores de todos os demais. Neste sistema podemos utilizar apenas os algarismos 0 e 1. Isto faz com que se torne muito mais simples o processo de realizar contas, já que para realizá-las faremos uso de apenas dois algarismos (multiplicar por 10, 100, 11 torna-se mais fácil).

Quando se utiliza o sistema decimal, trabalhamos por intermédio das potências de 10, sendo assim temos 10^0=1 (corresponde a unidade), 10^1=10 (corresponde a dezena), 10^2=100 (corresponde a centena) e assim sucessivamente. Ao somarmos os algarismos de 1 em 1, ao chegar no 9 e

somarmos mais 1 encontramos a dezena, sendo assim colocamos 1 e um 0, ficando 10, (em sala de aula muitos professores utilizam o termo vai 1), ou seja, 9+1=10.

No sistema binário, o procedimento é realizado de maneira semelhante. Para somar 1+1, fazemos o seguinte: como não existe o algarismo 2 (neste sistema, 1 é o último dígito), ao somar 1 com 1, colocamos 1 e 0, ficando 10. Assim 1+1=10. Na sequência, 10+1=11. 11+1=100. Note que neste último caso, 11+1 seria 12. Como não podemos utilizar o algarismo 2 em binários, utiliza-se 0 e coloca-se o 1 para lá (da mesma maneira aprendida a somar no Ensino Fundamental). Mas passando 1 para lá, o 2 surgiria novamente. Repete-se a operação, colocando-se 0 e passando 1 para lá. Por isso o resultado é 100.

$$\begin{array}{r} 11 \\ +1 \\ \hline \end{array}$$

$1+1=0$ e vai 1, pois não temos o 2.

$$\begin{array}{r} {\scriptstyle 1} \\ 11 \\ +1 \\ \hline 0 \end{array}$$

Novamente, $1+1=0$, e vai 1.

$$\begin{array}{r} {\scriptstyle 1} \\ 11 \\ +1 \\ \hline 00 \end{array}$$

Abaixamos esse 1 que ficou.

$$\begin{array}{r} 11 \\ +1 \\ \hline 100 \end{array}$$

O processo se repete. Temos, desta maneira, a Tabela 4:

Tabela 4

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12
Binário	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100

Para transformarmos um número em binário de volta ao sistema decimal, basta estabelecer da direita para a esquerda as potências de 2. A primeira casa seria 2^0, a segunda 2^1, a terceira 2^2 e assim sucessivamente. Cada vez que encontramos o algarismo 1 no sistema binário, substituímos seu valor em potência de 2 referente à sua posição. Ao final, somaríamos os valores relativos às potências encontradas e conseguiríamos estabelecer uma relação de equivalência na tabela apresentada acima.

Como exemplo, o número binário 11001 é o número decimal:

$1.2^4 + 1.2^3 + 0.2^2 + 0.2^1 + 1.2^0 = 16 + 8 + 1 = 25$.

Uma das formas de se escrever, utilizando a Cifra de Bacon, é associar cada letra a um número binário com 5 dígitos (ao invés de escrever 1, colocamos 00001 ou 00010 e não 2). Como cada grupo é formado por 5 dígitos e cada um destes dígitos possui 2 possibilidades (0 ou 1), podemos gerar 2^5 grupos, ou seja, 32 grupos que podem representar 32 letras distintas. Em outras palavras: A é a primeira letra, cifrada como 00001. B é a segunda letra, cifrada como 00010, e assim sucessivamente. Escrevem-se as letras de acordo com a Tabela 5.

Tabela 5

A	B	C	D	E	F	G	H	I	J	K	L	M
00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010

Sendo assim, conseguimos escrever cada letra como um conjunto de 5 dígitos. Mas é claro que se a mensagem possuísse muitos números, qualquer leigo entenderia que o texto em questão trata-se de um código e provavelmente poderia procurar uma maneira de desvendá-lo. O interessante é que existem várias formas convincentes de escrever este código. Assim, para que a integridade do código seja mantida em segredo, podemos utilizar outras

técnicas. Então, as seguintes alterações podem ser realizadas, estas alterações visam dificultar a decodificação: poderíamos considerar o 0 como letra minúscula, e o 1 como letra maiúscula. Por exemplo:

manEIrA DE EscOndeR noSSA MENsAGEM

Sabendo que está escondida com a Cifra de Bacon, pode-se agrupar a cada 5 dígitos e atribuir 0 para minúsculas e 1 para maiúsculas.

manEI rADEE scOnd eRnoS saMEN sAGEM
00011 01111 00100 01001 00111 01111

Daí, é só comparar com a tabela acima e obtemos que a palavra escondida é:

00011 01111 00100 01001 00111 01111
C O D I G O

Ao utilizarmos esta cifra, notamos que um de seus problemas consiste na mensagem criptografada ficar cinco vezes maior que o tamanho da mensagem original. A grande vantagem na utilização desta cifra está na variação de suas formas.

Desta forma, as cifras de Bacon podem utilizar, além do formato criptográfico, uma forma de ocultação da mensagem. E este fato acaba deixando a mensagem codificada bastante complicada para aquele que busca sua decodificação.

Consistiria em um bom exercício em sala de aula o uso desta cifra. Permitiria aos nossos alunos aplicarem os conceitos de adição, subtração e potenciação referentes a um novo sistema de numeração. Em virtude de suas operações, os alunos entenderiam que os algoritmos relativos a todas as operações se estendem a todas as classes de numeração que podemos montar e talvez o uso do vai 1 pudesse ser explicado de maneira mais ampla e eficiente.

Atividade 6 :

Cifre seu nome usando A para 0 e B para o 1.

II.1.2 Cifras de substituição polialfabética

Definição: as cifras de substituição polialfabéticas, são cifras do tipo: M=C=K=($\sum^n$)*, onde f é uma cifra que se decompõe em n substituições monoalfabéticas, indexadas pelas n letras da chave k, que se repetem em cada bloco de m (n é dito período da cifra).

Ao contrário das cifras monoalfabéticas, as cifras de substituição polialfabéticas fazem uso de mais de um alfabeto cifrante. O interessante é que os alfabetos não precisam ser de origens diferentes, o simples fato de alterarmos a ordem da sequência em que as letras aparecem caracteriza a presença de um novo alfabeto.

Uma tarefa, que pode chamar a atenção de nossos alunos e requer o uso de análise combinatória, consiste em encontrar todo o número possível de gerar alfabetos cifrantes. Se contarmos apenas com o alfabeto ocidental vigente em nossa sociedade veremos que este possui 26 letras. Como um alfabeto cifrante não pode ter repetição entre seus símbolos, bastaria então apenas permutar as 26 letras do alfabeto original. Então o número de alfabetos cifrantes possíveis é igual a 26! = 403.291.461.126.605.635.584.000.000, isto significa que pelo chamado método da força bruta é quase impossível alguém, sem o uso de uma máquina veloz, encontrar o alfabeto utilizado na codificação.

Esta técnica também permite que diferentes símbolos cifrados possam representar o mesmo símbolo do texto claro. Este fato dificulta a decodificação da mensagem, à medida que as representações referentes no texto original podem ser substituídas por mais do que um símbolo.

Um dos principais estudiosos responsável por ajudar no progresso e desenvolvimento da cifra de substituição polialfabética é Leon Battista Alberti, que ficou conhecido como “ pai da criptografia ocidental” . Leon Battista Alberti

foi o responsável pela criação de um disco para cifragem. Este fato acabou simplificando o processo, introduzindo a técnica de recifragem na criptografia.

O disco criado por Alberti era composto por dois anéis concêntricos: o primeiro externo, fixo, e possuía 24 casas e estas casas continham 20 letras latinas maiúsculas (incluindo o Z, com U=V e excluindo H J K W Y) mais os números 1, 2, 3, e 4. Este disco era utilizado para o texto claro. O segundo disco era interno, móvel, e possuía as 24 letras latinas minúsculas. Este disco era referente ao texto cifrado. Nestes discos, as 20 letras maiúsculas estão em ordem alfabética e as 24 minúsculas estão fora de ordem. Colocar as letras minúsculas fora de ordem é fundamental, isto porque, caso estivessem em ordem, este tipo de cifra seria apenas uma generalização do Código de César. Ao que tudo indica, os códigos inventados por Alberti não foram quebrados até os anos de 1800.

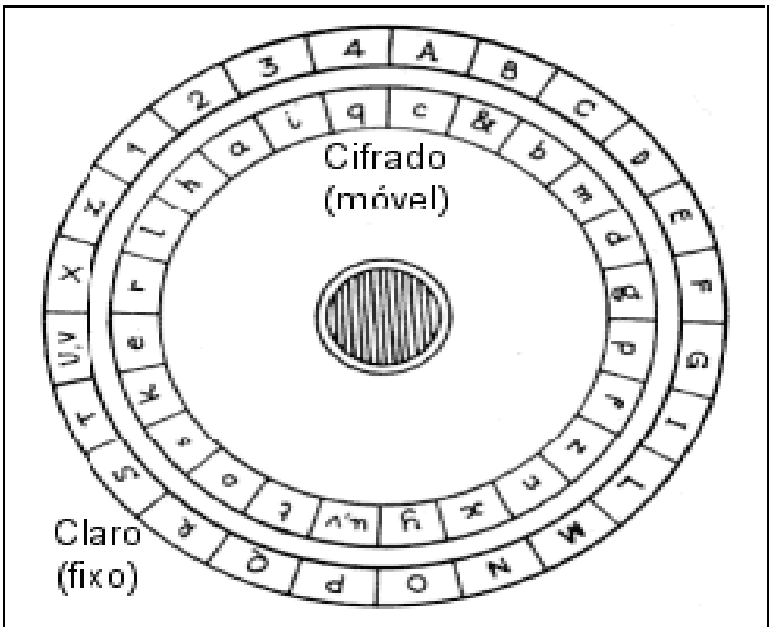


Figura referente aos discos de Alberti

Uma das mais famosas cifras relativas à substituição polialfabética é a cifra de Vigenére. Esta cifra leva o nome do diplomata francês que viveu de 1523 a 1596. Seu grande mérito consistiu em aperfeiçoar um método que já havia sido proposto por outros estudiosos só que não possuía a segurança necessária.

Cifra de Vigenére

A cifra de Vigenére constitui-se em um processo de substituição polialfabético, que utiliza uma série de diferentes cifras de César baseadas em letras de uma senha. Além disso, esta cifra também faz uso de diferentes valores de deslocamento. Para utilizar esta cifra, torna-se necessário o uso de uma palavra-chave.

A tabela abaixo mostra as carreiras de Vigenére. O cabeçalho da tabela (a linha superior) é o alfabeto e a coluna lateral esquerda mostra o deslocamento dos caracteres. Na linha 0, entra o alfabeto com deslocamento 0; na linha 1 os caracteres são deslocados em uma posição para a esquerda (o alfabeto começa com a letra B); na linha 2 os caracteres são deslocados em duas posições para esquerda e assim decorre, sucessivamente, cada caracter é deslocado para esquerda de acordo com o número da linha correspondente.

	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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

Para cifrar a primeira letra do texto claro com a primeira letra da chave, procura-se a letra do texto claro no cabeçalho e a letra da chave na coluna da esquerda. A letra encontrada na intersecção das duas referências será a substituta da letra do texto claro. Por exemplo, uma letra D do texto claro com a chave G será substituída pela letra J.

O problema do processo de substituição manual consiste em um grande número de erros, tudo em função de uma leitura penosa e, depois de algum tempo, bastante fatigante. O trabalho por intermédio de réguas sobre a tabela de alfabetos cifrantes também acaba sendo muito exaustivo, mas menos traumático. Devido a este fato, a partir de 1880, muitos criptólogos passaram a utilizar a chamada Régua de Saint-Cyr.

EXEMPLO DA CIFRA DE VIGENÉRE

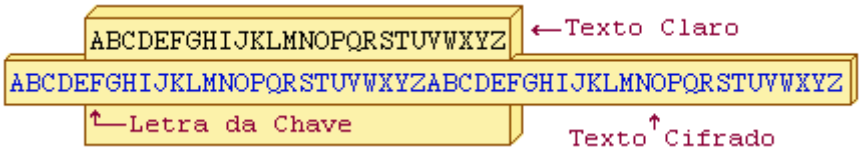
Como exemplo, vamos cifrar TEMOS UM NOVO PRESIDENTE com a palavra-chave FECHADA :

Texto Claro	T	E	M	O	S	U	M	N	O	V	O	P	R	E	S	I	D	E	N	T	E
Chave	F	E	C	H	A	D	A	F	E	C	H	A	D	A	F	E	C	H	A	D	A
Deslocamento	5	4	2	7	0	3	0	5	4	2	7	0	3	0	5	4	2	7	0	3	0
Cifrado	Y	I	O	V	S	X	M	S	S	X	V	P	U	E	X	M	F	L	N	W	E

Para cifrar um texto, convenciona-se uma palavra-chave. No exemplo é FECHADA. Neste caso, os alfabetos cifrantes F, E, C, H, A, D e A serão utilizados sucessivamente para cifrar a mensagem.

A Régua de Saint-Cyr

Batizada pelo holandês Auguste Kerckhoff, esta régua é constituída por uma estrutura fixa, geralmente de papel ou cartolina, que contém um alfabeto e uma estrutura móvel contendo dois alfabetos.



A Régua de Saint-Cyr

Esta régua pode ser utilizada para dois tipos de substituição, a primeira e mais simples é a substituição monoalfabética. Para realizar esta operação basta deslocar a parte móvel de acordo com o número de letras correspondentes ao deslocamento desejado. Este tipo de codificação torna-se muito simples de ser decodificada, para tanto, basta utilizar o processo de forma invertida utilizando-se da régua. A segunda, é a substituição polialfabética. Neste caso, a cada troca de alfabeto cifrante, desloca-se a parte móvel de modo a obter o módulo desejado.

Como pode ser notado, este tipo de régua serve tanto para as cifras do formato de César, como as cifras do formato de Vigenére.

Atividade 7:

Monte uma régua de Saint-Cyr

Atividade 8:

Utilizando a régua deslizante, decifre a mensagem:

UHV JVUZLNBP KLJPMYHY UHKH

Atividade 9:

Responda, em relação à atividade anterior, qual foi o método utilizado para que você descobrisse a chave utilizada.

Resposta das atividades 8 e 9 :

As atividades 8 e 9 estão interligadas. Para decifrar esta mensagem o aluno terá que descobrir quantas posições ele irá precisar movimentar a régua. Esta é uma atividade que busca estabelecer uma relação com o nosso ensino de português. Para encontrar a mensagem original o aluno precisará contar o número de aparições de cada letra. Realizando a contagem, o aluno verá que a letra que mais aparece é a letra H. Em nossa língua a letra que mais aparece é a vogal A. Portanto, caso a letra H corresponda à vogal A, basta que o aluno desloque as demais letras em 7 posições anteriores. O aluno necessita então testar letra por letra e assim ele encontrará a mensagem: NÃO CONSEGUI DECIFRAR NADA.

II.2 Cifras de transposição

Diferentemente das cifras de substituição, as cifras de transposição não fazem uso da troca de caracteres, nestas cifras o codificador não faz uso de alfabetos cifrantes. Estes tipos de cifras consistem num reagrupamento dos caracteres da mensagem original de maneira que sua ordem é alterada. Desta maneira, podemos dizer que as cifras de transposição se baseiam no princípio matemático da permutação. Se analisarmos, tanto o processo de codificação como o de decodificação, veremos que a cifra de transposição faz uso de uma função bijetora, utilizada para que a mensagem seja cifrada. Para decifrar a mensagem, basta fazer uso da função inversa relativa à função utilizada no processo de codificação.

Existem várias maneiras de estabelecer uma forma de criptografia por transposição, por exemplo, podemos citar o método conhecido como transposição de colunas. Em uma cifra de transposição simples de colunas, a mensagem é escrita em uma “tabela”, onde o número de colunas é dado pela chave e o número de linhas será dado pelo tamanho da mensagem. A mensagem é, então, escrita linha por linha dentro desta tabela e removida coluna por coluna em uma ordem determinada pela chave. Para que esta cifra funcione é necessário que o tamanho da mensagem seja múltiplo do tamanho da chave. Caso essa condição não seja satisfeita no início, devemos inserir letras aleatórias no final da mensagem até que esta condição seja satisfeita.

Texto Plano: O ATAQUE SERA NO DIA D NA HORA H

Chave: 315243

Criptografia:

3	**1**	**5**	**2**	**4**
O	A	T	A	Q
U	E	S	E	R
A	N	O	D	I
A	D	N	A	H
O	R	A	H	X

Com isso, tiramos as letras da tabela linha por linha na ordem indicada pela chave. Vale ressaltar que as letras são retiradas de acordo com o posicionamento crescente dos números que compõem a tabela. Sendo assim, a mensagem codificada ganha o seguinte formato :

AENDR AEDAH OUAAO QRIHX TSONA

Para realizarmos a decodificação da mensagem, podemos verificar que o comprimento de cada bloco de caracteres nos facilita a conclusão de que a chave utilizada no processo de codificação possui 5 dígitos. Com isso, deveríamos reescrever a mensagem em uma tabela de 5 linhas e 5 colunas:

A	A	O	Q	T
E	E	U	R	S
N	D	A	I	O
D	A	A	H	N
R	H	O	X	A

Em seguida, devemos analisar os pares de letras em cada linha para tentarmos identificar os dígrafos mais comuns na língua portuguesa. Para este propósito existem livros e artigos na internet que listam os dígrafos mais comuns. Por exemplo, na primeira linha temos os dígrafos “ao”, “ta” e “to”. Fazendo isso para todas as linhas encontraríamos os seguintes resultados:

Apesar de ter algumas contradições, podemos extrair alguns padrões do quadro acima:

5-2; 1-5

Tendo essas duas combinações de colunas, conseguiríamos descobrir os outros pares mais frequentes:

3-1; 2-4

Com isso, restaria-nos apenas realizar testes em cima dessas combinações de colunas até o ponto em que as palavras façam algum sentido linguístico. O que aconteceria, quando começássemos pela coluna 3: a cifra RHOXA seria rearranjada em HORAX.

Esse método de encriptação é considerado bastante simples, pois pudemos precisar o tamanho da chave e da cifra, apenas olhando para a cifra, o que facilita bastante a quebra deste tipo de cifra.

Vale ressaltar mais uma vez que a quebra dessa cifra se deu com um número de passos relativamente pequeno, devido à simplicidade da cifra. Relativamente, quanto mais complexas forem as estratégias destas cifras de transposição, o número de passos relativos à decodificação irá aumentar.

Atividade 10:

Cifre a frase: Hoje é dia de jogo

Utilize a chave: 2413

II.3 Cifras de transposição e substituição combinadas

Visando aumentar a segurança entre o envio e recebimento seguro de mensagens, muitos codificadores acabam fazendo uso de mais de uma técnica de cifragem. Pudemos verificar durante o texto que existem cifras que se utilizam de forma concomitante da criptografia e da esteganografia. Da mesma forma muitos codificadores acabam combinando as técnicas de transposição e substituição. Uma destas técnicas a qual podemos citar e que faz uso dessas combinações é a chamada cifra ADFGX.

A cifra ADFGX

A cifra ADFGX foi criada pelo exército alemão logo após a invenção do telégrafo. Esta cifra possui como principal característica a utilização de dois métodos de codificação, ela faz uso do método de substituição e do método de transposição, a consequente combinação destes dois métodos torna esta cifra mais forte, sendo assim sua decodificação não é realizada de maneira simples. Esta cifra ADFGX combinava o tabuleiro de damas de Polybius com uma palavra-chave. Em função do código Morse vigente à época os alemães se aproveitaram destas cinco letras que dão nome ao código, isto porque seus equivalentes referentes ao código Morse eram muito difíceis de confundir, reduzindo assim a chance de erros. Sendo assim, as únicas letras utilizadas por esta cifra eram as letras: A,D,F,G,X.

O tabuleiro de Polybius, como vimos em um capítulo anterior, foi criado por um estudioso grego de mesmo nome e consistia em um quadrado com 5 linhas e 5 colunas, a disposição do quadrado de Polybius é semelhante a

disposição apresentada pelo quadrado representado na figura abaixo, a única mudança consiste no fato que ao invés de usarmos letras para representar os índices referentes a linhas e colunas, no quadrado de Polybius eram utilizados números de 1 a 5.

O primeiro passo para utilização desta cifra ADFGX era criar uma matriz muito parecida com o tabuleiro de damas de Polybius, como dito acima a única diferença consiste na utilização de letras ao invés de números, sendo assim a matriz adquire a seguinte formatação:

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

Os criptógrafos fariam uso de pares de letras em cifras para representar as letras correspondentes no texto simples. A linha de letras consiste na primeira cifra do par, enquanto a coluna torna-se a segunda cifra. Neste exemplo, a letra cifrada "B" torna-se "AD", enquanto o "O" torna-se "FG". O interessante é que uma matriz do tipo ADFGX não precisa ser organizada, necessariamente, de forma sequencial, o codificador pode embaralhar esta sequência e tornar a decodificação muito mais difícil.

Da maneira como encontrasse a tabela acima, um criptógrafo poderia utilizá-la para cifrar sua mensagem. Por exemplo:

Criptografando a frase : VAMOS ESTUDAR, teríamos encontrado XAAAFDFGGF AXGFGGGXAGAAGD.

Caso o processo de codificação terminasse aí, teríamos utilizado apenas o processo relativo à substituição. O método de decodificação assim acabaria sendo realizado de maneira simples e até rápida. Mas a cifragem ainda não terminou, como já dissemos esta cifra faz uso dos métodos de substituição e de transposição, portanto, ainda existe um próximo passo.

O próximo passo, correspondente a transposição, consistiria na escolha de uma palavra-chave, a qual poderia possuir qualquer comprimento, porém nesta não devem ocorrer repetição de letras. Para este exemplo, vamos utilizar como palavra-chave a palavra **MARTELO**. O criptógrafo, então criaria uma grade com a palavra-chave soletrada no topo. O criptógrafo então escreveria a mensagem cifrada na grade, separando os pares em letras individuais e passando de uma linha para a outra.

M	**A**	**R**	**T**	**E**	**L**	**O**
X	A	A	A	F	D	F
G	G	F	A	X	G	F
G	G	G	X	A	G	A
A	G	D				

Então, o criptógrafo reorganizaria a grade de forma que as letras da palavra-chave ficassem em ordem alfabética, alterando-se assim as colunas correspondentes as letras da forma apropriada:

A	**E**	**L**	**M**	**O**	**R**	**T**
A	F	D	X	F	A	A
G	X	G	G	F	F	A
G	A	G	G	A	G	X
G			A		D	

Ele então escreveria a mensagem de acordo com cada coluna (não considerando as letras da palavra-chave no topo da linha). Essa mensagem ficaria assim: "AGGG FXA DGG XGGA FFA AFGD AAX". Desta forma podemos observar o motivo pelo qual este código é considerado muito desafiador, os criptógrafos que o utilizavam cifravam e **transpunham** cada caractere do texto simples. Para decifrar, era necessário o conhecimento da palavra-chave (MARTELO), então todo trabalho começaria apenas a partir deste instante. Após o descobrimento da palavra-chave o decodificador começaria com uma grade com colunas organizadas alfabeticamente. Uma vez preenchida a grade, as colunas deveriam ser reorganizadas de forma

apropriada e após todo este trabalho a matriz seria utilizada para decifrar a mensagem e chegar enfim ao texto original.

Uma pessoa que buscasse decodificar qualquer mensagem codificada pela cifra ADFGX poderia tentar adivinhar a palavra-chave contando o número de palavras existentes na mensagem cifrada. Este número de palavras cifradas é igual ao número de letras da palavra chave, isto em função de cada palavra cifrada representar uma coluna de texto, e cada coluna corresponde a uma letra na palavra-chave. No exemplo utilizado, existem sete letras na mensagem cifrada, isto indica que existem sete colunas e uma palavra-chave de sete letras. Em razão do número de palavras cifradas e da mensagem original poderem ter contagens diferentes, como vimos sete letras cifradas versus duas palavras de texto simples, decifrar esta mensagem torna-se algo ainda mais desafiador.

Atividade 11:

Por intermédio da cifra ADFGX, cifre a seguinte mensagem:

Hoje é dia de festa

Utilize LETRA como palavra-chave

Capítulo III - O desenvolvimento da criptografia por intermédio de máquinas

Analisaremos agora o período de desenvolvimento de máquinas especialmente criadas para realizar o processo de criptografia. Neste capítulo, estudaremos as principais criações no período da segunda guerra mundial. Realizaremos também a sugestão de atividades que podem ser aplicadas em sala de aula, bem como os conceitos que devem ser aplicados para a obtenção dos resultados das atividades.

III.1 Criptografia eletro-mecânica

O desenvolvimento de nossa sociedade e o consequente advento do uso de máquinas no processo de produção se intensificou com o passar dos anos. Com o crescimento econômico e social, vieram também as crises e, atreladas às crises, vieram também as grandes guerras. Os períodos de guerra constituem-se em um transtorno para nossa civilização, mas estes períodos, por pior que sejam, acabam por contribuir bastante no processo de aceleração e progresso, principalmente, na obtenção de máquinas cada vez mais velozes e eficazes.

Nos períodos referentes às grandes guerras, as mensagens entre os exércitos precisavam ser enviadas da maneira mais confidencial possível. Caso uma mensagem fosse interceptada, era necessário que o interceptador não pudesse entender seu conteúdo. Além disso, o envio de mensagens era feito de forma incessante, sendo assim, exigia-se um maior grau de velocidade no processo de confecção das codificações relativas às mensagens enviadas. Em razão da pressa e da melhoria da obtenção de códigos, assim como para auxiliar na decifração de mensagens, foram desenvolvidos em larga escala uma série de equipamentos eletro-mecânicos, responsáveis por acelerar os processos de codificação e decodificação.

Dentre todos estes experimentos que surgiram e que possuíam a intenção de estabelecer codificações cada vez mais elaboradas, podemos destacar entre todos eles a máquina Enigma e a máquina de Lorenz. Estas duas máquinas foram utilizadas pelos alemães durante o período referente à segunda guerra mundial e foram projetadas, especificamente, para cifrar mensagens e proteger suas informações.

Dentre os experimentos relativos ao processo de decodificação, podemos destacar a criação do computador Colossus. Este computador foi criado na Inglaterra pelo exército aliado, com a intenção de servir como antídoto para a máquina Enigma e também para a máquina de Lorenz. Este computador é de vital importância para o desenrolar da guerra, mas não só para isso, este computador acaba sendo o precursor dos computadores modernos.

O computador Colossus foi projetado pela equipe de Alan Turing, era uma máquina inglesa e foi projetada em Bletchley Park. Este equipamento processava a uma velocidade de 25000 caracteres por segundo, o que na época representava uma velocidade extremamente alta.

Com o desenrolar da segunda guerra mundial surgiam então as bases para o que ficou conhecido como era da informática. Depois deste período as tecnologias avançaram de certa forma que se iniciaram o desenvolvimento de máquinas muito mais poderosas e que possuíam fácil acesso pela população, estas máquinas permitiram a consequente criação de códigos muito mais difíceis de serem decifrados.

III.2 A máquina Enigma

O primeiro modelo desta máquina foi criado pelo holandês Dr Arthur Scherbius e possuía apenas fins comerciais. A máquina foi apresentada no Congresso Postal Internacional de Bern, no ano de 1923. Neste congresso foi apresentado o modelo A da máquina, o qual constituiu-se num verdadeiro

fracasso, muito em função do seu preço, considerado demasiadamente alto para a época.

O modelo então esquecido foi retomado pela marinha alemã no ano de 1925. Surgia então o novo modelo da máquina Enigma, agora batizado de Enigma M3, adotado pelo exército alemão em 12 de janeiro de 1937.

O funcionamento desta máquina era bastante interessante. Esta máquina possuía em seu interior três discos com cifras. Estes discos recebiam o nome de rotores e cada rotor poderia ser trocado ou retirado da máquina. Cada rotor possuía letras de A a Z, além de diferentes sistemas internos de fiação. Os rotores eram conectados entre si e cada vez que uma letra era digitada o rotor do canto direito girava uma posição. O rotor central, girava uma posição sempre que o primeiro rotor passava pelas 26 letras de nosso alfabeto. O rotor esquerdo girava uma posição, após o rotor central passar por suas 26 letras. O interessante é que o funcionamento desta máquina é similar ao hodômetro de um automóvel. A única diferença é que no hodômetro passa por dez posições ao invés das 26 realizadas pelos rotores da máquina enigma.

A máquina Enigma funcionava de maneira que ao pressionar-se uma letra do texto pleno no teclado, uma corrente elétrica passava pelos componentes de cifragem da máquina, isto fazia acender uma luz no painel de lâmpadas, a letra acendida correspondia à codificação da letra digitada. Na máquina Enigma, ao contrário das cifras de substituição utilizadas na antiguidade, uma letra poderia ser cifrada de forma diferente. Isto ocorria em função das peças móveis da máquina estarem em constante mudança em suas posições, cada vez que uma letra era pressionada. Este fato aumentava o grau de segurança da máquina.

O exército alemão dispunha de cinco rotores, sendo que a máquina podia abrigar em seu interior apenas três destes rotores.

O funcionamento da máquina Enigma é muito interessante, tanto para termos históricos quanto para a matemática aplicada, principalmente, no que tange ao ensino de análise combinatória. O funcionamento desta máquina pode prover a tão falada interdisciplinaridade entre as disciplinas de História e

Matemática, já que sua criação e desenvolvimento esta ligada a um período histórico muito importante.

Neste capítulo, vimos que a máquina Enigma dos alemães possuía 3 rotores, sendo que a cargo dos alemães estavam disponíveis 5 rotores. Desta maneira, poderíamos realizar uma atividade com alunos do ensino médio de análise combinatória. Poderíamos também tomar como público alvo alunos do ensino fundamental e iniciar o desenvolvimento do princípio multiplicativo.

Atividade 12:

Calcular o número de maneiras diferentes que os 5 rotores podem ser colocados na máquina Enigma, sabendo que esta só consegue abrigar 3 rotores de cada vez.

Resposta:

Matematicamente, não é difícil realizar este cálculo. Basta utilizarmos o princípio multiplicativo, assim faríamos 5 x 4 x 3, o que nos daria um total de 60 posições diferentes possíveis entre estes rotores.

Outras atividades com a máquina Enigma também podem ser sugeridas e podem atingir o mesmo público da atividade 12.

Atividade 13:

Determine o número de posições que a máquina Enigma pode ter em sua configuração inicial quanto ao posicionamento de suas letras.

Resposta:

Para resolver a atividade 13 basta o aluno entender que se a máquina tem 3 rotores e cada rotor possui em sua estrutura as 26 letras do alfabeto, então para calcularmos o número total de configurações que a máquina pode atingir, basta fazer 26 x 26 x 26 = 17576. Sendo assim a máquina Enigma pode ter até 17576 disposições iniciais diferentes.

Após efetuarmos a atividade 12, verificamos que o número de possibilidades que dispomos para abrigar os 5 rotores em um espaço de apenas 3 destes rotores é igual a 60. Na atividade 13 vimos que o número de configurações especiais destes 3 rotores em relação às letras que carregam é igual a 17576, ou seja, existem 17576 possibilidades de trios diferentes correspondentes às letras de cada rotor. Poderíamos então propor mais uma atividade para nossos alunos.

Atividade 14:

Calcular o número total de possibilidades de configuração inicial que a máquina Enigma pode alcançar.

Resposta:

Para obtermos a resposta referente a esta atividade, basta multiplicar os números encontrados nas duas atividades anteriores, bastaria então ao aluno fazer: 60 x 17576 = 1054560 , ou seja existiam mais de um milhão de configurações possíveis para que um soldado pudesse iniciar a codificação de uma mensagem utilizando a Enigma M3.

Importante ressaltar que embora tenhamos calculado o número total de disposições iniciais, estas são apenas as disposições mecânicas da máquina, além destas ainda existiam as disposições elétricas. Esta máquina possuía uma placa de conexões de cabos elétricos responsáveis por embaralhar as mensagens e aumentar o número de configurações iniciais.

Os cabos elétricos da máquina possuíam plugues nas extremidades e estes plugues eram conectados entre pares de letras. Como um exemplo se conectássemos A a B, ao digitarmos a letra A, a corrente elétrica seguirá o caminho relativo à letra B, e vice-versa.

Atividade 15:

Se utilizarmos apenas um cabo e resolvermos estabelecer uma relação que nos permita calcular a quantidade de conexões diferentes que podem ser formadas na utilização da máquina Enigma, qual seria o número de conexões diferentes encontradas ?

Resposta:

Quando usarmos o primeiro cabo teremos 25 possibilidades, ao usarmos o segundo teríamos 24 possibilidades e assim por diante, até chegarmos a apenas uma possibilidade. Sendo assim, a resposta da atividade será o resultado da soma : 25 + 24 + 23 + ... + 2 + 1, o que nos dá exatamente 325 maneiras.

Atividade 16:

Calcule sem o uso de calculadoras o valor da soma : 25 + 24 + 23 + ... + 2 + 1.

Resposta:

Na atividade 15 o aluno encontraria como resposta esta soma. Poderíamos estimulá-lo a resolver esta operação, sem que haja a necessidade do uso de calculadoras, bem como a soma destas parcelas por seu algoritmo. Esta atividade focaria o início do estudo de progressões aritméticas. Desta maneira, poderíamos induzir ao aluno a pensar que 1 + 25 = 26, da mesma forma 2 + 24 = 26 e da mesma forma 3 + 23 = 26. Bastaria então ao aluno efetuar a seguinte operação $\frac{(1+25)x\,25}{2}$, encontrando 325 como resposta.

O interessante agora seria realizar uma atividade em sala para que os alunos pudessem calcular o número aproximado de configurações dos circuitos elétricos da máquina. Para isto, o professor poderia mediar a aula e orientar seus alunos na execução dos cálculos. Vejamos o processo:

Primeiro precisamos encontrar como calculamos o número de maneiras de escolher k pares não ordenados dentre um total de n objetos. Inicialmente,

para escolhermos o primeiro termo teremos n possibilidades, para escolhermos o segundo, teremos (n – 1) possibilidades, para escolhermos o item 2k, teremos (n – 2k) + 1 possibilidades. Sendo assim, ao todo teremos n x (n-1) x (n-2)x...x(n–2k+1).

Neste cálculo não nos interessam pares ordenados e nem a localização de um par na escolha feita, sendo assim algumas das combinações calculadas são as mesmas e precisam ser descontadas. Para tanto precisamos pensar que os k pares podem ser escolhidos em qualquer ordem, portanto teremos k opções para o primeiro par , k-1 opções para o segundo par, k-2 opções para o terceiro par, até que haja apenas 1 opção para o último par, logo temos k x (k - 1) x (k -2) x ....x 1 maneiras. Assim, podemos escrever o número de maneiras de se organizarem os k pares como k! . O cálculo não terminou, isto porque a posição de um elemento dentro de um par não é importante. Portanto, precisamos ainda descontar 2 vezes para cada um dos k pares,ou seja, devemos descontar 2^k.

Após efetuarmos os cálculos acima, em função da ordem não ser levada em consideração, precisamos descontar k! x 2^k. Dividiremos a fórmula encontrada pelo total de descontos para que na contagem tenhamos apenas uma das combinações, logo chegaremos na fórmula : $\frac{n!}{\frac{(n-2k)!}{k!\,2^k}}$, esta fórmula é equivalente a escrevermos $\frac{n!}{(n-2k)!\,k!\,2^k}$.

Podemos então realizar com nossos alunos a seguinte atividade:

Atividade 17:

Utilizando uma placa de conexões com as letras A, B, C, D, E, F, quantas ligações podem ser realizadas se utilizarmos apenas dois cabos:

Resposta:

Basta escolhermos , n=6 e k = 2, sendo assim aplicamos a fórmula encontrada e fazemos : $\frac{6!}{2!\,2!\,2^2}$ = 45 ligações.

Através desta fórmula podemos sugerir a nossos alunos calcular o número total aproximado de configurações referentes à máquina Enigma. Para que se tenha uma ideia, o número total de configurações, tendo em vista as partes elétrica e mecânica da máquina, é de aproximadamente 1,58 x 10^{28} configurações.

Depois de verificarmos este número podemos ter a exata noção de como era complicado e árduo o trabalho de decodificação desta máquina.

Processo de decodificação da máquina Enigma:

A máquina Enigma se caracteriza por efetuar uma criptografia simétrica, sendo assim a decodificação é inversa da codificação. Além disto, a chave de decodificação é a mesma chave utilizada na codificação. Desta forma, para decifrar as mensagens tornava-se necessário o conhecimento do processo de encriptação.

Durante a segunda guerra mundial, segundo a história, os alemães alteravam a chave de codificação todos os dias reconfigurando suas máquinas todas as noites no horário de meia-noite. Os operadores destas máquinas recebiam todo mês uma folha, esta folha continha as chaves referentes às configurações que deveriam ser empregadas em cada um dos dias do mês. Vimos anteriormente que o número possível de configurações iniciais que a máquina Enigma poderia alcançar era gigantesco, como a chave era trocada todos os dias, a tarefa de codificação além de se tornar bastante complicada dispunha também de um período curto de tempo.

O interessante é que esta máquina, muito embora fosse altamente sofisticada no que se refere a códigos, possuía também suas fraquezas. Como sua chave é única, bastava aos inimigos recuperar uma das folhas que

continham estas chaves para que todas as mensagens pudessem ser decodificadas durante o período de 1 mês. Por causa deste risco constante e iminente, o exército alemão precisava de algo que mantivesse estas informações em sigilo, mesmo em caso de interceptação. Para segurança destas mensagens, os alemães mantinham então as folhas bem guardadas e realizavam um processo de impressão utilizando tintas solúveis. Desta forma, se um soldado alemão viesse a ser capturado poderia dar fim a todas as informações que as folhas continham.

A segurança alemã nesta máquina residia no total de possibilidades relativas à configuração que a máquina possuía. Como este número de possibilidades era muito grande, eles sabiam que era impossível para qualquer pessoa calcular rapidamente a chave utilizada. Vale destacar que o prazo máximo para troca de chave era de 24 horas. Desta forma, o exército alemão acreditava que enquanto o exército inimigo não se apossasse das folhas que continham as chaves, sua comunicação permaneceria segura.

Durante a segunda guerra mundial, os aliados (exército inimigo ao alemão) criaram, por intermédio de Alan Turing e sua equipe, o primeiro computador operacional. Este computador foi criado, exclusivamente, com o intuito de decifrar mensagens cifradas pela máquina Enigma.

Mesmo com a utilização do computador e com um total de 7000 pessoas trabalhando, dentre elas cientistas, operadores de máquinas e alimentadores de dados, o processo de decodificação não era simples. Os aliados precisavam interceptar as mensagens enviadas pelos alemães, depois as repassavam para uma central em Bletchley Park. Neste local trabalhava um grupo de pessoas escolhidas entre as mais inteligentes da Inglaterra. Esta central recebia pelo menos 3000 mensagens diárias e seus participantes precisavam comparar diferentes mensagens com outras para encontrar a maneira com que a máquina havia sido configurada durante aquele dia. Este grupo de pessoas dispunha de 2 horas para descobrir qual das 1,58 x 10^{20} possibilidades fora empregada. O interessante é que com o uso de computadores algumas mensagens, em função de seu padrão, puderam ser decodificadas em menos

de uma hora, mas a situação se agravou quando o exército alemão resolveu utilizar 4 rotores ao invés de 3.

Em 9 de maio de 1941 os aliados conseguiram capturar um submarino alemão que continha manuais de navegação e livros de códigos e sinais. Estes livros continham os códigos da máquina Enigma. Paralelamente, os aliados contavam agora com o computador chamado Colossus. Este computador foi criado, especialmente, para decifrar mensagens secretas e possuía uma unidade de leitura de fita de cinco canais, que funciova com uma velocidade de 5000 caracteres por segundo, e uma unidade de saída construída com um teletipo e 2500 válvulas. O Colossus era um computador paralelo assíncrono, possuía um sistema fotoelétrico e comparava todas as combinações de mensagens codificadas com suas chaves criptográficas geradas. Desta maneira ele conseguia revelar a configuração da máquina Enigma. Este computador constituiu-se no primeiro computador eletrônico programável pelo homem e através de sua utilização os ingleses conseguiram decifrar códigos gerados por máquinas Enigma com até 12 rotores.

III.3 A máquina de Lorenz

A máquina de Lorenz possuía 12 rotores utilizados para embaralhar as letras de uma mensagem. Sua forma de operação consistia em transformar as letras em números binários. Estes números eram somados (tudo isto se utilizando de aritmética binária) a outros números que eram obtidos através da rotação das engrenagens da máquina. A mensagem então era criptografada e enviada como uma mensagem telegráfica, após ter sido transformada em pulsos elétricos.

Para transformar letras em números a máquina utilizava a tabela abaixo. Logo, cada letra era transformada em um número binário composto de cinco algarismos. Com esta configuração a máquina poderia gerar conforme mostra a tabela abaixo 32 caracteres.

Tabela de transformação :

A	11000	B	10011	C	01110	D	10010	E	10000	F	10110	G	01011
H	00101	I	01100	J	11010	K	11110	L	01001	M	00111	N	00110
O	00011	P	01101	Q	11101	R	01010	S	10100	T	00001	U	11100
V	01111	W	11001	X	10111	Y	10101	Z	10001				
9	00100	8	11111	+	11011	4	01000	3	00010	/	00000		

Se observarmos a tabela, veremos que existem além das 26 letras do alfabeto, seis símbolos que diferem de seus reais significados. Estes eram utilizados como sinais de pontuação ou para controle de impressão. O algarismo 9 por exemplo era utilizado para separar palavras.

Vale ressaltar que se apenas esta troca de letras por números binários fosse realizada, estaríamos diante de um código de César, portanto sua decodificação seria fácil. Para que isto não ocorresse, quando uma letra era introduzida na máquina, os rotores giravam e produziam 12 novos números, estes números eram somados ao número associado à letra e uma nova letra era produzida. A operação de adição empregada era a adição binária, ou seja, esta máquina funcionava na adição módulo 2. Suas adições teriam os seguintes resultados:

0 + 0 = 0,
0 + 1 = 1,
1 + 0 = 1 e
1 + 1 = 0

Exemplo de codificação :

Codificando a letra P com a letra chave M:

P = 01101 (letra original)
Vamos supor que os rotores girem e produzam o número 00111, este numero corresponde à letra M.

Somamos então P com M : 01101 + 00111 = 01010 , onde em cada posição usamos a adição módulo 2. O resultado encontrado corresponde à letra R. Desta maneira, a letra P se converte na letra R.

A máquina de Lorenz também é uma máquina de chave simétrica, isto porque a adição binária possui ela mesmo como inversa. Sendo assim, a atividade proposta pode ser decodificada da seguinte maneira :

Como P + M = 01101 + 00111 = 01010 = R , então R + M = 01010 + 00111 = 01101 = P.

Capítulo IV - Novos rumos da criptografia após o período pós-guerra

No capítulo anterior analisamos as mudanças e as criações humanas que revolucionaram os métodos de criptografia. Neste capítulo analisaremos o período referente ao fim da guerra, nele perceberemos a expansão e importância atual do uso da criptografia e conheceremos novas formas desta ciência. Neste capítulo teremos como referência o livro: Coutinho, S. C. ; Números Inteiros e Criptografia RSA, Rio de Janeiro, IMPA, 226 páginas (Coleção Matemática e Aplicações), 2011.

IV.1 Período pós-guerra e o uso da criptografia

Como vimos no texto, o período de guerras contribuiu muito no desenvolvimento tecnológico. Neste período era necessário proteger a informação de espiões inimigos para que as batalhas pudessem ser vencidas. Passado o período de guerra, engana-se aquele que pensa que o uso de mensagens criptografadas tornou-se obsoleto. Na verdade o período pós-guerra apenas reorganiza a criptografia, agora ela se torna necessária para esconder informações comerciais.

Evidentemente, os muitos avanços tecnológicos registrados, tanto na área de codificação como na área de decodificação, requerem técnicas de criptografia cada vez mais desenvolvidas. A consequente disseminação de aparelhos tecnológicos, que atualmente se encontram à disposição de quase todos os habitantes do planeta, também contribuem para que as técnicas utilizadas também sofram um alto grau de refinamento.

Inicia-se, então o período referente às criptografias, que fazem o uso de chaves, podendo estas serem públicas, secretas ou até mesmo o uso destes dois tipos de chaves. O que vale agora são as condições do mercado, qual é a

forma mais rápida, segura e vantajosa de se enviar, proteger e autenticar uma mensagem.

IV.2 Criptografia simétrica versus criptografia assimétrica

A criptografia de chave simétrica também é conhecida como criptografia de chave secreta. Este tipo de criptografia faz uso de apenas uma chave. Esta chave é a responsável pela codificação e pela decodificação de uma determinada mensagem.

A criptografia de chave assimétrica, que também é conhecida como criptografia de chave pública, faz uso de duas chaves: a primeira comumente chamada de chave pública e a segunda conhecida como chave privada. A chave pública é distribuída normalmente entre os seus usuários enquanto a chave privada deve ser mantida em sigilo por seu responsável.

Entre estes dois tipos de criptografia, a assimétrica possui um grau de segurança maior. Isto porque, como já foi dito, ela possui duas chaves. Estas chaves estão relacionadas matematicamente, mas o conhecimento da chave pública não implica na descoberta da chave privada. Em função deste motivo, a decodificação da mensagem torna-se muito mais difícil do que se houvesse apenas uma chave responsável pela codificação e decodificação da mensagem.

Apesar de menos confiável, a chave simétrica encontra ainda muita utilização, muito em virtude de sua velocidade. Como este tipo de criptografia faz uso de apenas uma chave, seus algoritmos são muito mais simples, o que a torna muito mais rápida e menos custosa do que a chave assimétrica. Desta forma, para manter sua segurança é vital que suas chaves sejam trocadas frequentemente, além de ser necessário sigilo total durante sua distribuição e operação.

Criptografia Assimétrica

Vimos anteriormente que o período de guerras constituiu-se em um período muito importante no desenvolvimento da criptologia. Pudemos observar os avanços principalmente de máquinas e computadores utilizados para a codificação e a decodificação de mensagens. Com o passar do período de guerras, as transações bancárias e comerciais, assim como o constante uso da internet para estes ou demais fins, acabaram por contribuir ainda mais para os avanços da criptologia.

Um usuário qualquer que faz uso de uma transação bancária necessita que sua mensagem seja protegida. Da mesma maneira a instituição que recebe a mensagem precisa ter segurança de que um de seus funcionários recebeu e respondeu esta mesma mensagem. Aparece assim pela primeira vez no contexto o conceito de autenticidade.

Novos códigos então precisavam ser inventados. Agora os códigos não faziam mais parte de um jogo entre espiões, estes novos códigos foram criados para terem seu uso vinculados a aplicações comerciais. Sendo assim, em 1976 W. Diffie, M. E. Hellman e R.C. Merkle lançam a ideia dos códigos de chave pública.

Entre todos os códigos de chave pública, o mais usado em aplicações comerciais e, consequentemente, o mais conhecido é o RSA. Sua sigla é referente às iniciais de seus criadores, R. L. Rivest, A. Shamir e L. Adleman, faz uso de teoremas clássicos da teoria dos números e foi inventado em 1978.

Números primos

Para que possamos aplicar em sala de aula os conceitos primitivos do funcionamento da criptografia RSA, devemos primeiro observar algumas definições e propriedades referentes ao aprendizado de números primos. Alguns conceitos requerem um conhecimento de matemática mais avançado. Para tanto, como nosso público alvo não é configurado por especialistas na área e como nossa tarefa é tornar o aprendizado da disciplina mais dinâmico e

de certa forma divertido, apresentaremos as definições e propriedades de forma empírica sem o uso de demonstrações.

Definição de números primos

Dependendo da série que iremos aplicar este conhecimento poderemos utilizar uma das definições.

Primeira definição:

Para alunos que conhecem apenas o conjunto dos números naturais podemos dizer que um número é primo quando possui apenas dois divisores, são eles: a unidade e o próprio número. Lembrando que a unidade não possui classificação, poies tem um único divisor e, todos os demais números que não são primos e são diferentes da unidade são chamados de números compostos.

Segunda definição:

Para alunos que conhecem o conjunto dos números inteiros a definição precisa ser mais formal. Seja p um número inteiro tal que $p \neq 0$, $p \neq 1$ e $p \neq -1$. Dizemos que p é primo, se p possui exatamente quatro divisores, são eles -1, 1, - p e p.

Os números que não são considerados primos, à exceção do -1 e do 1, são conhecidos como números compostos.

Função φ de Euler

A função φ(n) de Euler corresponde ao número de inteiros k localizados no intervalo $1 \leq k \leq n$, onde mdc (n,k) =1.

Um fato importante nesta função é o de que se n for um número primo, então $\varphi(n) = n - 1$. Este fato é decorrente da definição de números primos. Para entendermos melhor, basta observar que o valor da função φ (n) não pode ultrapassar n. Se n for um número primo, teremos que $mdc(n,n) = n \neq 1$,

mas como n é primo todos os demais números 1,2,3,...,n-1 são primos com n, desta forma $\varphi(n) = n - 1$.

Da função de Euler podemos extrair o seguinte resultado, que nos será muito importante no entendimento da RSA :

Seja n um número inteiro, tal que n pode ser escrito na forma pq, onde p e q são números primos distintos, então $\varphi(n) = \varphi(pq) = \varphi(p) \times \varphi(q) = (p-1)(q-1)$.

IV.3 Criptografia RSA

A criptografia RSA é bastante complexa e envolve um conhecimento avançado do estudo da Teoria dos Números. A ideia do trabalho consiste em uma simples exposição de seu funcionamento e de suas características. Em função do trabalho em questão estar totalmente voltado para sala de aula, com alunos de ensino médio e fundamental, seria inútil estabelecer este tipo de matemática tão avançada em seu contexto. Sendo assim, desenvolveremos uma matemática mais simples, voltada ao funcionamento do sistema RSA que possa agregar conhecimento e interesse por parte dos alunos referendados e assistidos por nós professores.

O funcionamento do RSA inicia-se com a transformação da mensagem a qual queremos codificar (que é uma mensagem escrita) em uma mensagem numérica, sendo assim devemos converter a mensagem escrita em uma tabela de números. Após a conversão da mensagem e de possuirmos a consequente tabela numérica, escolhemos dois números primos distintos e encontramos o número $n = p \times q$.

O interessante neste início do funcionamento do código RSA é que podemos estabelecer para nossos alunos os conceitos de números primos, aplicando suas propriedades no cotidiano moderno e tornando seu aprendizado mais dinâmico e menos cansativo.

Após determinarmos n, precisamos dividir a mensagem escrita (que foi transformada em mensagem numérica) em blocos, cada bloco formado precisa

possuir um comprimento inferior ao número $\varphi(n)$, a única prerrogativa é a de que nenhum dos blocos pode começar com o algarismo 0.

Para continuarmos a codificação, utilizaremos uma chave codificadora (n, m), onde n foi escolhido e o valor de m precisa ser escolhido de forma que $mdc(m,\varphi(n)) = 1$. O par (n,m) é conhecido como chave de codificação do sistema RSA. Vale ressaltar que a escolha do número m não possui unicidade, portanto a chave codificadora pode variar de acordo com os valores escolhidos.

Após a escolha da chave precisamos codificar cada bloco b encontrado na etapa inicial de codificação. Então se denotarmos cada bloco b codificado por C(b), a maneira de calculá-lo é a seguinte :

$C(b) = b^m \bmod n$.

Cada bloco precisaria ter sua codificação estabelecida. Antes de estabelecermos o funcionamento necessário à decodificação deste método, vamos apresentar alguns exemplos referentes à codificação para tornar o trabalho referente aos alunos menos cansativo e expositivo.

Como um exemplo de codificação no RSA, vamos codificar a palavra MEDO :

Em primeiro lugar precisamos estabelecer uma tabela numérica referente às letras de nosso alfabeto, sendo assim podemos estabelecer as seguintes relações :

A – 10	F – 15	K – 20	P – 25	U – 30	Z – 35
B – 11	G – 16	L – 21	Q – 26	V – 31	
C – 12	H – 17	M – 22	R – 27	W – 32	
D – 13	I – 18	N – 23	S – 28	X – 33	
E – 14	J – 19	O – 24	T – 29	Y – 34	

Note que, para não haver confusão quando quebrarmos os blocos, as letras foram representadas sempre com dois dígitos, evitando assim quebras com 1, 2 ou 12 que podem confundir e levar ao erro na hora da codificação.

Agora, devemos transformar a mensagem escrita em mensagem numérica :

M – 22, E - 14, D – 13, O - 24, desta forma a palavra MEDO se transforma na mensagem numérica : 22141324.

Agora escolhemos dois números primos e distintos p e q. Vamos escolher p = 2 e q = 7, assim temos que n = p x q = 2 x 7 = 14.

Calculamos agora φ(n) = φ(14), φ(14) = φ(2) x φ(7) = 1 x 6 = 6. Portanto, quando quebrarmos a mensagem numérica em blocos, estes blocos não poderão ter comprimentos maiores do que 6. O que limita nossa quebra para 3 maneiras neste exemplo, utilizaremos a seguinte quebra para codificação:

22141324 = 2 – 2 – 1 – 4 – 1 – 3 – 2 – 4

Precisamos agora escolher um número m tal que mdc (m, α (n)) = 1 e 1 < m < α (n) , logo precisamos encontrar um número m tal que mdc (m, 6) = 1 e 1 < m < 6.

A única alternativa para m que temos neste nosso exemplo é m = 5, sendo assim encontramos como chave codificadora (14, 5) e agora precisamos codificar cada bloco. Encontramos então os restos das seguintes divisões :

C(2) = 2^5 mod 14 = 4

C(2) = 2^5 mod 14 = 4

C(1) = 1^5 mod 14 = 1

C(4) = 4^5 mod 14 = 2

C(1), já calculado, resto 1

C(3) = 3^5 mod 14 = 5

C(2), já calculado, resto 4

C(4), já calculado, resto 2

Após codificarmos cada bloco obtemos a sequência numérica 4-4-1-2-1-5-4-2 e, finalmente, concluímos o processo de codificação utilizando o código RSA.

O processo de decodificação é muito complicado para o público alvo que queremos atingir com a realização deste trabalho. Para decodificar precisaremos utilizar uma matemática mais avançada que além do conceito de números primos envolve também um grau de conhecimento de teoria dos números. Desta forma resolvemos não aprofundarmos mais no que tange à decodificação do código RSA.

Capítulo V – Aplicando a criptologia em sala de aula

Neste capítulo apresentaremos uma atividade envolvendo a codificação e a decodificação para uma turma do ensino fundamental. Nele descobriremos os benefícios e as dificuldades enfrentadas por nossos alunos.

V.1 A aula

Para desenvolvermos esta aula, em primeiro lugar, vamos levar em consideração os nossos objetivos e nossa estratégia.

Objetivos :

1) Estabelecer uma conexão entre nosso alfabeto e a matemática, relacionando desta forma a matemática com o português.

2) Realizar algoritmos de soma e subtração entre os alunos.

3) Despertar o interesse dos alunos pelo tema e deixar que estes se aprofundem, de forma voluntária no mundo da criptologia.

Público alvo :

Alunos que cursam o sexto ou sétimo anos do EJA (Ensino de Jovens e Adultos)

Organização da atividade:

Para iniciarmos a atividade dividimos a turma em 4 grupos de 5 alunos cada um, para cada grupo foi enviada uma mensagem que deveria ser criptografada utilizando a cifra de César. Para cada grupo foi dada uma tabela com referência entre as letras e um número do alfabeto. Após a cifragem, cada grupo escreveu sua mensagem numericamente e a colocou no quadro negro. Venceria a tarefa o grupo que primeiro conseguisse decifrar as 3 mensagens dos demais grupos primeiro.

Desenvolvimento :

Após o início da atividade vimos uma determinada empolgação por parte dos alunos, isto pela curiosidade em descobrir as mensagens alheias, assim como pela competição gerada pela atividade em si. Ainda sobre o desenvolvimento podemos citar a dificuldade de nossos alunos em estabelecer uma relação das letras com o alfabeto, isto ocorreu em função de muitos dos alunos ainda estarem em um processo inicial de escrita.

Depois de muitas dúvidas e explicações, os grupos conseguiram cifrar suas respectivas mensagens. Cada mensagem então foi colocada no quadro negro e então os grupos começaram o processo de decodificação. Neste processo, verificamos que embora a adição não tenha sido um processo difícil, a subtração constituiu-se em um verdadeiro entrave para alguns de nossos alunos. Desta forma, separamos um período da aula para explicar melhor o algoritmo da subtração.

Após um tempo de aproximadamente 90 minutos um dos grupos tornou-se vencedor ao decodificar as 3 mensagens alheias.

Conclusões :

Durante e após a atividade pudemos notar que os grupos sentiram imensa dificuldade em organizar estruturas que envolviam letras e números. Pudemos notar também a dificuldade na realização de operações básicas como a subtração.

Com o término da atividade, pudemos notar um interesse maior de nossos alunos em matemática. Muitos disseram que iriam se aprofundar no estudo da criptologia e pediram outras atividades referentes ao assunto. Alguns alunos evoluíram e entenderam o algoritmo da subtração. Talvez o mais marcante é que estes alunos acabaram por responder às dúvidas de muitos de seus colegas.

Conclusão

Neste trabalho foram identificadas várias formas de criptografias diferentes e várias atividades que podem ser expostas em sala de aula. Todas as cifras e processos de codificação foram apresentados com seu contexto histórico e com atividades relativas à sala de aula. Desta maneira, este trabalho pode ser utilizado de forma interdisciplinar, além de poder ser utilizado de forma contextualizada com as demais disciplinas que compõem o currículo básico.

Referências Bibliográficas

[1] Coutinho, S. C. ; Números Inteiros e Criptografia RSA, Rio de Janeiro, IMPA, 226 páginas (Coleção Matemática e Aplicações), 2011.

[2] Singh, Simon; O livro dos códigos : A Ciência do sigilo do antigo Egito à Criptografia Quântica; Editora Record, São Paulo, 2001.

[3] Cajori, Florian; Uma história da Matemática, Rio de Janeiro, Editora Ciência Moderna Ltda., PP 552-562, 2007.

[4] Mega, Élio; Olimpíadas brasileiras de Matemática, Rio de Janeiro, SBM 2010.

[5] Voloch, J. F. ; A distribuição dos números primos, Matemática Universitária, número 06, PP 71-82.

[6] Figueiredo, L. M. S., Números primos e criptografia de chave pública, Rio de Janeiro, CEP, 2005.

[7] Figueiredo, L. M. S., Costa, C. J., Introdução à Criptografia, Rio de Janeiro, CEP, 2005.

[8] Ribenboim, P., Números primos: mistérios e recordes, Associação Instituto Nacional de Matemática Pura, Rio de Janeiro, 2001.

[9] Santos, J. P. O., Introdução à Teoria dos Números, Rio de Janeiro, IMPA, 1998.

[10] Sites:

(a) (http://www.cic.unb.br/docentes/pedro/segdados_files/CriptSeg1-2.pdf)

(b) (http://www.schneier.com)

[11] Bletchley Park, un museo de informática y criptografia, Susana Mataix, Portal de periódicos da Capes

[12] Criptografia e matemática, Fiarresga, Victor Manuel Calhabrês Silva, Jorge Nuno Oliveira E, Portal de periódicos da Capes.