UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE DOURADOS
MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA
PROFMAT

MAURICIO SOARES DOS REIS

CRIPTOGRAFIA: UM ESTUDO HISTÓRICO E APLICADO A MATEMÁTICA DO ENSINO BÁSICO

DOURADOS-MS
2020

MAURICIO SOARES DOS REIS

CRIPTOGRAFIA: UM ESTUDO HISTÓRICO E APLICADO A MATEMÁTICA DO ENSINO MÉDIO

Dissertação apresentado ao Mestrado Profissionalizante em Matemática - Profmat, da Universidade Estadual de Mato Grosso do Sul, Unidade de Dourados, como requisito final para a obtenção do título de mestre em Matemática.

Orientador: Prof. Dr. Otávio José Neto Tinoco Neves dos Santos

DOURADOS-MS
2020

R311c Reis, Mauricio Soares dos
Criptografia : um estudo histórico e aplicado a matemática do ensino médio/ Mauricio Soares dos Reis. – Dourados, MS; UEMS, 2020.
104p.

Dissertação (Mestrado Profissional) – Matemática – Universidade Estadual de Mato Grosso do Sul, 2020.
Orientador: Prof. Dr. Otávio José Neto Tinoco Neves dos Santos.

1. Criptografia – História 2. Matemática – Estudo e ensino 3. Matemática – Ensino médio I. Santos, Otávio José Neto Tinoco Neves dos II. Título

CDD 23. ed. - 652.809

Ata de Defesa de Dissertação
Programa de Pós-Graduação em Matemática
Mestrado Profissional

Aos vinte e sete dias do mês de fevereiro do ano de dois mil e vinte, às quinze horas, na Unidade Universitária de Dourados, da Fundação Universidade Estadual de Mato Grosso do Sul, realizou-se a sessão de defesa de Dissertação, intitulada: "Criptografia: um estudo histórico e aplicado a matemática do ensino básico" de autoria do aluno: **MAURICIO SOARES DOS REIS**, CPF 017.324.481-59, sob a orientação de OTÁVIO JOSÉ NETO TINOCO NEVES DOS SANTOS do Programa de Pós-Graduação em Matemática, nível: Mestrado Profissional. Reuniu-se a Banca Examinadora composta pelos membros: OTÁVIO JOSÉ NETO TINOCO NEVES DOS SANTOS **(Presidente)**, LUIZ ORESTE CAUZ e EDSON CARLOS LICURGO SANTOS (UNIOESTE). Concluída a apresentação e arguição, os membros da Banca Examinadora emitiram parecer expresso conforme segue:

☒ Aprovação ☐ Aprovação com revisão ☐ Reprovação

EXAMINADOR	**ASSINATURA**
Dr. OTÁVIO JOSÉ NETO TINOCO NEVES DOS SANTOS	
Me. LUIZ ORESTE CAUZ	
Dr. EDSON CARLOS LICURGO SANTOS (UNIOESTE)	

OBSERVAÇÕES:

Nada mais a ser tratado, o Presidente declarou a sessão encerrada e agradeceu a todos pela presença.

Assinaturas:

Presidente da Banca Examinadora

Aluno

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

MAURICIO SOARES DOS REIS

CRIPTOGRAFIA: UM ESTUDO HISTÓRICO E APLICADO A MATEMÁTICA DO ENSINO BÁSICO

Produto Final do Curso de Mestrado Profissional apresentado ao Programa de Pós-Graduação *Stricto Sensu* em Matemática em Rede Nacional, da Universidade Estadual de Mato Grosso do Sul, como requisito final para a obtenção do Título de Mestre em Matemática.

Aprovado em: 27/02/2020.

BANCA EXAMINADORA:

Prof. Dr. Otávio José Neto Tinoco Neves dos Santos (UEMS)
Universidade Estadual de Mato Grosso do Sul

Prof. Msc. Luiz Oreste Cauz (UEMS)
Universidade Estadual de Mato Grosso do Sul

Prof. Dr. Edson Carlos Licurgo (UNIOESTE)
Universidade Estadual do Oeste do Paraná

Hoje quero dedicar a conclusão desse trabalho, ao senhor pai, o considere como uma forma de tributo. Dedico ao senhor que já não está mais entre nós e que foi embora de um jeito repentino. Dedico cada linha dessa dissertação ao senhor que se sacrificou trabalhando o tanto que fosse necessário para que eu me formasse. Ao senhor que sempre comemorou todas as minhas conquistas, desde a compra da minha primeira roupa até o dia que eu contei ao senhor que tinha passado na qualificação do mestrado. O senhor sempre foi um entusiasta do meu sucesso e mesmo depois de ter partido fisicamente eu sinto que o senhor ainda torce por mim. Muito obrigado pai, amo o senhor.

Agradecimentos

Agradeço a Deus por ter me dado inspiração, força, saúde e paciência para superar os obstáculos surgidos durante minha vida.

A minha mãe que sempre me ajudou e esteve presente na busca dos meus maiores sonhos.

Aos meus irmãos André e Mari que me confortaram nos momentos em que mais precisei.

Aos poucos e bons amigos que estiveram comigo em toda essa caminhada. Em especial Letícia, Fabia, Vitor, Naiguiel e Ronan.

Ao professor orientador Otávio Neto, pela paciência, perspicácia, compreensão, pelo olhar humano que o mesmo dedicou ao longo de todo o tempo em que me orientou.

Ao meu pai, que mesmo não estando mais aqui, sempre será minha motivação para continuar a estudar.

“Em tudo só se pode alcançar um grande êxito quando nos mantemos fiéis a nós mesmos.”

Friedrich Nietzsche

Resumo

Este trabalho tem como objetivo fazer um estudo sobre criptografia, englobando os fatos históricos mais importantes para o seu desenvolvimento como ciência. Uma vez que partindo do contexto histórico, serão propostas situações-problema e sugestões de atividades que contemplem o contexto estudado. Assim sempre que possível a Matemática será utilizada como ferramenta de resolução das situações e também será utilizada como mecanismo de compreensão das situações que serão propostas e desenvolvidas ao longo deste trabalho.

Palavras–chave: criptografia, história e matemática.

Abstract

This work aims to make a study on cryptography, encompassing the most important historical facts for its development as a science. Since starting from the historical context, problem situations and suggestions for activities that contemplate the context studied will be proposed. Thus whenever possible, Mathematics will be used as a tool for solving situations and will also be used as a mechanism for understanding the situations that will be proposed and developed throughout this work.

Keyworks: cryptography, history and mathematics.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

Introdução

Presente na troca de mensagens por whatsapp com a chamada criptografia de ponta, na troca de um bilhete entre crianças na sala de aula, ou ainda nas transações bancárias a fim de que hackers não tenham acesso a informações confidenciais que possibilitem fraudes, a criptografia é indispensável para a vida do ser humano e nos processos tecnológicos.

A palavra criptologia tem origem no idioma grego (kriptós = escondido, oculto; logo = estudo, ciência) e se constitui em uma ciência que fornece mecanismo teórico a criptografia (kriptós = escondido, oculto; grápho = grafia) é o conjunto de procedimentos com os quais se pode codificar ou decodificar uma mensagem de modo que somente o destinatário a compreenda de forma clara, a grosso modo a criptografia transforma um texto legível em algo inelegível a quem não tem a chave de decodificação. Nesse contexto chave é um pedaço de informação que regula operação de um algoritmo de criptografia. Na codificação, uma chave especifica transforma o texto puro em texto cifrado, ou vice-versa, durante o processo de decodificação a chave tem o atributo de transformar o texto cifrado no texto original.

Desde os primórdios da história da humanidade a arte de esconder mensagens, criptografia, vem sendo usada como meio de transmitir recados, ordens ou até mesmo informações de governo. Usada nos primeiros confrontos entre povos da humanidade a criptografia se apresentava como um meio de transmitir informações e sair na frente dos adversários do campo de batalha.

Porém foi nas duas grandes guerras mundiais que a criptografia juntamente com a criptoanálise (conjunto de procedimentos usado para quebrar códigos secretos) ficaram em evidência em confrontos particulares que foram sobretudo uma guerra da informação.

No período compreendido entre as duas guerras a comunicação se restringia a transmissões de rádio e ligações telefônicas, portanto não era muito fácil fazer a interceptação de informações que tinham conteúdo sigiloso. Por esse motivo a criptografia era um meio importante de se transmitir qualquer tipo de informação em segurança. Porém engana-se que a criptografia era usada somente na transmissão de informações em conflitos armados, já naquele período as informações referentes a instituições bancárias eram codificadas por meio de

conhecimentos de codificação. Um exemplo importante do que foi descrito até agora é o episódio denominado Telegrama Zimmermann, ocorrido na Primeira Guerra Mundial, onde agentes secretos tiveram acesso a um comunicado no qual o ministro alemão das Relações Exteriores sugeria a embaixadores alemães no México uma aliança com o México a fim de ganhar mais força no conflito, tal fato motivou a entrada dos Estados Unidos no confronto. De maneira similar, ou seja por meio da criptoanálise, o almirante Yamamoto, comandante mor do exército japonês que foi o artífice do ataque a Pearl Harbor, foi assassinado de forma prévia em 1943, depois dos americanos decodificarem os trajetos feitos por seu avião.

Nesse cenário existe uma teoria de que a Segunda Guerra Mundial teve seu fim preconizado por cientistas que usaram de Matemática e Criptologia (Ciência que estuda mecanismos necessários a aplicação de Criptografia e Criptoanálise) para decifrar o código da Máquina Enigma (Enigma foi uma máquina eletromecânica de criptografia, utilizada para criptografar e descriptografar códigos usados em guerra ficou famosa por ter sido utilizada pelo exército alemão na Segunda Guerra Mundial), a equipe responsável pela quebra de códigos da máquina Enigma tinha como um de seus membros o matemático e cientista da computação Alan Turing que foi considerado um personagem de grande relevância na denominada guerra da informação que ocorreu durante a o conflito mundial findado em 1945.

Turing foi o idealizador do projeto que criou uma máquina computacional que foi usada como ferramenta para quebrar os códigos utilizados na máquina Enigma. Na época tal projeto foi visto com desconfiança devido ao seu alto custo de produção, estimado em 100 mil libras, o que na época se constituía em uma fortuna.

Avançando um pouco na história e chegando aos dias de hoje, a criptografia se apresenta como ferramenta essencial em tarefa simples como o envio de um e-mail, nos serviços de compra eletrônico e transações por internet. Outro departamento de atividades comerciais que teve desenvolvimento ligado a criptografia são os serviços prestados por e-commerce e a compra e venda de produtos e serviços por telefone, pois nesse processo a transmissão de informações como senhas, documentos pessoais e endereço é feita de forma que somente a loja e o cliente tenham acesso a esses dados. Assim mesmo que alguém mal

intencionado intercepte essas informações, o interceptor não conseguirá fazer o uso das mesmas, pois elas se encontram criptografadas de forma segura.

A Matemática como mecanismo de compreensão da sociedade tem papel crucial na Criptologia desde o uso de funções que podem ser empregadas no processo de criptografia por substituição, até os conhecimentos de Aritmética que são utilizados nos processos de criptografia citados no parágrafo anterior. Tais conhecimentos se apresentam como uma contextualização de Aritmética ou Teoria dos Números e aplicações de propriedades referentes a números inteiros como M.D.C, Números primos e Aritmética modular.

Diante de todas essas informações apresentadas esse trabalho surge no intuito de apresentar situações ligadas a criptografia que podem ser empregadas como aplicação de conteúdos matemáticos, sejam eles do ensino básico ou do ensino superior.

Por meio de uma cultura de depreciação e diante das dificuldades apresentadas em sua compreensão, a Matemática é vista como uma ciência morta, carente de aplicações em muitos dos seus tópicos. Trabalhar com criptografia é um desafio e uma ferramenta que pode ser útil em situações de aprendizagem que fogem um pouco do método de definir, demonstrar e concluir tópicos sem a demonstração de suas aplicações práticas.

Na produção desse trabalho serão discorridos tópicos referentes a história de criptografia, sempre relacionando esses fatos a história da humanidade, com objetivo de proporcionar conhecimentos de todo processo construtivo da ciência de criptologia, nesse sentido é essencial ter conhecimento do contexto histórico para se compreender a criação e a evolução do manuseio dos códigos.

Culminando com a conclusão da pesquisa teremos a apresentação sequenciada de atividades que tratam de conceitos matemáticos e de criptografia de chave assimétrica.

Capítulo 1

A criptografia ao longo da história da civilização humana

A história da criptografia se encontra fortemente ligada a história do desenvolvimento da civilização humana. Não é nova a ideia de se ocultar o conteúdo de mensagens, há indícios de que os egípcios foram os primeiros a utilizar uma espécie de escrita secreta, por meio de hieróglifos, com a finalidade de surpreender inimigos em guerra e garantir o triunfo em combates.

Sobre esse fato (LOUREIRO, 2014) afirma que a necessidade de se proteger uma informação é antiga. No início, a criptografia era uma ferramenta usada exclusivamente por governos em situações de guerra ou quando desejassem manter uma comunicação segura ou proteger alguma informação vital, que poderia causar danos se caísse em mãos inimigas. E, assim foi por milhares de anos, até a invenção dos computadores e da internet. Hoje a criptografia não é mais uma ciência de uso quase que exclusivamente militar. Não só os governos que precisam proteger informações, empresas e pessoas necessitam da criptografia para proteger suas informações.

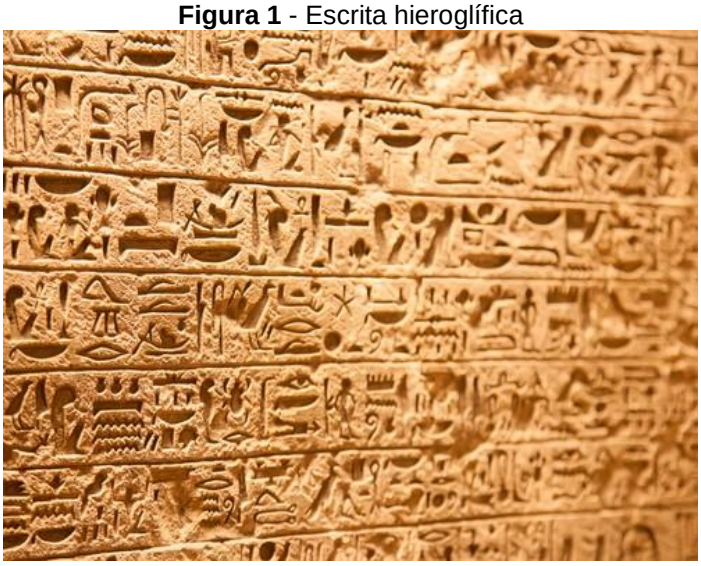
1.1 A escrita hieroglífica e o primeiro indício do uso de criptografia

Quando falamos em criptografia a primeira imagem que vem a nossa mente é a criptografia associada a computação, mas bem antes disso os egípcios a sua maneira fizeram algo similar ao ato de criptografar usando de escrita hieroglífica. A palavra hieróglifo tem origem no idioma grego e sua tradução livre é escrita sagrada, muito provavelmente pelo fato de que na época pouquíssimas pessoas tinham conhecimentos de letramento, a priori esses conhecimentos eram restritos a nobreza da época, aos escribas e aos sacerdotes, daí a denominação escrita sagrada. Além dos egípcios os povos maias e hititas também eram adeptos da escrita hieroglífica.

De acordo com David Kahn, um dos mais renomados pesquisadores da história da criptografia, o primeiro registro documental de escrita criptografada aconteceu por volta de 1900 a.C. O episódio ocorreu em uma vila egípcia situada

nas proximidades do rio Nilo, a vila de Menet Khufu que é localizada na cidade de Beni Hasan. O fato consistiu na tentativa de um escriba responsável por grafar o túmulo de Khnumhotep II, sendo que o escriba substituiu alguns hieróglifos por outros signos que ele considerava mais rebuscados e pertinentes devido a importância do chefe de estado ali sepultado.

Figura 1 - Escrita hieroglífica



(Obtido em https://www.infoescola.com/civilizacao-egipcia/hieroglifo/)

Ainda que a intenção do escriba não fosse guardar segredo ou vencer uma guerra, esse foi o primeiro fato histórico associado a criptografar, a esconder o segredo de uma frase. Nesse caso o método em questão foi a da substituição de um símbolo por outro. O próprio sistema hieróglifo se manteve por muito tempo como um sistema criptográfico, mais precisamente foi em 1822 que Jean-François Champollion decifrou os escritos da Pedra Rosetta, estudo esse que possibilitou um conhecimento maior dos povos ocidentais sobre o sistema egípcio.

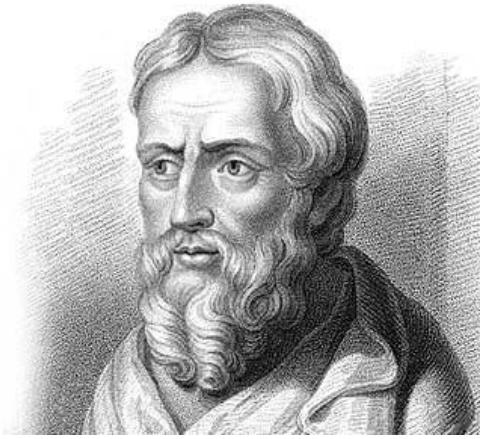
1.2 Heródoto e as narrativas sobre a esteganografia

Um dos primeiros escritos que relatam episódios ligados a criptografia é atribuído ao geógrafo e historiador grego Heródoto (485 A.C.– 425 A.C.). Para muitos Heródoto é considerado o pai da História como ciência e dispõe em seus escritos relatos sobre a arte de ocultar mensagens (esteganografia: do grego escrita escondida).

Existe diferença conceitual entre criptografia e esteganografia. A criptografia se resume a procedimentos que buscam tornar inelegível uma frase legível, ao passo que a esteganografia tem como maior preocupação a ocultação de uma mensagem. Atualmente as duas técnicas podem ser utilizadas de forma conjunta para garantir uma maior segurança na transmissão de mensagens.

Tais escritos se encontram em sua obra que relata a invasão do povo Persa a Grécia no século V A.C, essa obra é conhecida basicamente como as Histórias de Heródoto.

Figura 2 – Imagem de Heródoto



(Obtido em https://edukavita.blogspot.com/2015/06/biografia-de-herodoto-historiador-grego.html)

Durante a narrativa do fato histórico Heródoto assume que a esteganografia (arte de ocultar mensagens) salvou os gregos de serem conquistados pelo rei dos Persas Xerxes. Por aproximadamente cinco anos Xerxes comandou a criação de um dos maiores exércitos de que se tem notícia na história antiga, a intenção era submeter economicamente o povo grego aos domínios do povo Persa, em outras palavras Xerxes que elaborava um ataque surpresa, acabou surpreendido pelos contra ataques gregos na invasão de 480 A.C que foram elaborados previamente devido a intervenção de Demerato (que residia em exílio na Pérsia) que relatou através da esteganografia os planos de Xerxes para submeter o povo grego.

Vejamos como o fato foi narrado por Heródoto

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente

> com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos. (SINGH, 2007, p. 20).

Outro fato narrado por Heródoto em seus relatos é que a esteganografia foi usada para garantir que uma mensagem fosse transmitida de forma segura pelo general Histieu. Histieu arquitetou um plano de revolta contra os persas, no qual contava com a participação de Aristágoras o então governador de Mileto. Buscando garantir que a mensagem chegasse de forma segura ao seu destino, Histieu raspou a cabeça de um mensageiro e escreveu a em seu couro cabeludo. Depois que o cabelo do mensageiro cresceu o mesmo saiu em viagem até o encontro de Aristágoras, que raspou sua cabeça e conseguiu ler a estratégia de Histieu.

Outras técnicas de esteganografia foram utilizadas pelo ser humano durante a história. Uma dessas técnicas consistia em escrever em um pequeno pedaço de seda a mensagem a ser enviada, depois do processo de escrita a mensagem era coberta com cera e engolida pelo mensageiro que conseguia fazer a entrega do recado ao receptor de forma segura. Esse procedimento foi criado na China. Outro mecanismo era escrever em um pedaço de papel com uma tinta invisível, que quando submetida a uma temperatura mais alta se tornava visível ao ser humano geralmente com uma coloração marrom. As tintas invisíveis eram elaboradas por meio de ingredientes naturais. O suco de limão foi muito utilizado como tinta invisível, ele era misturado ao leite pra garantir a propriedade de tinta invisível. Ainda se destaca a técnica criada por Giovanni Porta, cientista italiano, que escrevia mensagens com tinta feita de alume e vinagre na casca de ovos. O escrito era absorvido pela clara cozida do ovo e ficava visível quando era retirada a casca. Durante o período da Inquisição, militares faziam minuciosas revistas aos civis e as informações circulavam escondidas em ovos secretos.

O microponto também foi uma técnica de esteganografia muito utilizada, principalmente na Segunda Guerra Mundial. O procedimento consistia em reduzir a imagem de um texto até que ela fosse transformada em um ponto, denominado de

microponto. Então o microponto era inserido ao fim de um texto aparentemente inofensivo, o receptor de posse da carta, ampliava o ponto e passava a ter acesso a informações secretas. A técnica do microponto foi muito utilizada pelos alemães até o ano de 1941, a partir desse ano os aliados descobriram a técnica e os alemães desenvolveram outras formas de trocar informações com sigilo.

1.3 Contribuições dos gregos a criptografia

A Cítala Espartana ou Bastão de Licurgo é um sistema de criptografia que foi muito utilizado no século V A.C na Grécia antiga, especialmente em campanhas militares. A cítala era formada por dois bastões de mesmo diâmetro e comprimento e uma tira de couro. Cada um desses bastões deveria estar em posse dos participantes desse processo de comunicação.

Figura 3 – Citala espartana

(Obtido em https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/)

A técnica era bem simples e consistia em escrever uma mensagem de forma longitudinal na tira de couro quando enrolada no bastão, em seguida essa tira se transformava em um cinto que era usado pelo mensageiro com as letras voltadas para a parte de dentro. Chegando ao destino o cinto era retirado e entregue ao receptor da mensagem que deveria enrolar a tira de couro no seu bastão para compreender o significado da mensagem.

A tabela espartana foi outro método utilizado por gregos como forma de criptografar. O método consistia em preencher uma tabela comum com as letras do alfabeto. A chave para realizar a criptografia era o número de colunas da tabela, o número de linhas iria depender do tamanho do texto a ser escrito. A mensagem era escrita numa ordem a se combinar e o texto era cifrado tomando se outra direção.

Vamos fazer uma cifragem usando esse modelo para torna-lo mais claro de compreensão.

Vamos escrever em uma tabela de 4 colunas a mensagem “EU ADORO ESTUDAR ARITMÉTICA” e sempre que formos dar um espaço vamos utilizar letra Z. No nosso exemplo a frase será escrita da esquerda pra direita.

Tabela 1 – Modelo de tabela espartana

E	U	Z	A
D	O	R	O
Z	E	S	T
U	D	A	R
Z	A	R	I
T	M	E	T
I	C	A	Z

(Tabela elaborada pelo autor do trabalho)

Para concluir a cifragem vamos tomar a escrita da frase de cima para baixo e como a chave de criptografar é o número de colunas, as letras devem ser agrupadas de quatro em quatro para se concluir o processo. Assim a frase “EU AMO ESTUDAR ARITMÉTICA”, quando criptografada pela tabela espartana adquire a forma:

EDZU ZTIU OEDA MCZR SARE AAOT RITZ

Se por acaso o número de letras da última palavra for menor do que 4, faz se o complemento com letras aleatórias. Nesse tipo de criptografia o receptor da mensagem deve estar da posse, do número de linhas e das informações de sentido de escrita.

O último método utilizado na Grécia Antiga a ser relatado nesse trabalho é a cifra de Políbio. O método foi descrito pelo historiador e geógrafo Políbio (203 A.C. - 120 A.C) no seu livro Histórias e detalha um código poligrâmico desenvolvido por Cleoxeno e Democleto.

O uso da cifra consistia em uma substituição das letras do alfabeto por um par de números cujos algarismos estão compreendidos entre 1 e 5. A tabela usada(tabela 2 da página seguinte) pode ser visualizada como uma matriz 5x5. Dessa forma a mensagem podia ser transmitida até mesmo com o uso de tochas de fogo. Por exemplo, se a letra a ser transmitida fosse a letra B pelo método das

tochas, bastava segurar uma tocha com a mão esquerda(linha 1 da tabela 2) e duas com a mão direita(coluna 2 da tabela 2). Na linguagem matricial o termo a_{ij} da matriz de codificação teria em i a quantidade de tochas a ser segurada na mão esquerda e em j o número de tochas a ser seguradas na mão direita. Essa cifra se constituía além de um código como um sistema de comunicação visual, pois através da representação por tochas era possível fazer a transmissão da mensagem sem utilizar papel, couro ou outro meio pra se registrar escrita.

Tabela 2 – Cifra de Políbio

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

(Tabela elaborada pelo autor do trabalho)

Usando a técnica de Políbio a palavra MATEMÁTICA ficaria com a seguinte escrita criptografada:

33 11 44 15 33 11 44 24 13 11

O processo de cifragem é feito pela junção dos algarismo da linha e da coluna o de decifragem é o inverso, toma-se o número da linha e da coluna e é feita a substituição pela letra correspondente na célula. O quadro de Políbio não era fixo, uma vez que ao se ter acesso as versões aqui disponibilizadas o receptor poderia repassar a outros a forma de como se decifrar. As variações do quadro eram feitas no arranjo dos caracteres interiores.

1.4 A Cifra de César

Chamamos de cifra a qualquer forma de criptografar fazendo a troca de uma letra de um alfabeto por uma ou mais letras a se combinar. As cifras se dividem em cifra de transposição e substituição. Uma cifra é dita de transposição quando os caracteres do texto quando escritos em linha são trocados de posição entre si por

meio de manipulação ou regra a combinar. O Cítale espartano é um exemplo de uso da cifra de transposição.

Por outro lado uma cifra será referida como de substituição quando os caracteres do texto forem mantidos em sua posição original, mas sendo substituído por outro de acordo com o alfabeto de cifragem a ser utilizado. No caso da cifra de substituição além das palavras também pode se combinar de substituir palavras ou frases combinadas previamente.

De acordo com a característica as cifras de substituição se classificam em monoalfabéticas ou simples, homófonas, polialfabéticas, poligrâmicas e poligráficas.

Por substituição simples ou monoalfabética se entende como o tipo de cifragem em que se usa apenas um alfabeto cifrador e cada letra tem correspondente único na tabela de cifragem. A Cifra de César é de substituição monoalfabética.

A substituição homófona possui um ou mais símbolos para alguns caracteres do alfabeto normal.

Temos ainda as cifras de substituição polialfabéticas que utilizam mais de um alfabeto de substituição para o alfabeto normal. A cifra de Viginére é um exemplo de cifra de substituição polialfabética. Por fim, cifra de substituição poligráfica são aquelas em que substituem um conjunto de caracteres do escrito por outros símbolos. A cifra de Hill é um exemplo de de código que usa cifragem poligráfica.

O primeiro código de cifragem que se tem notícia em relatos históricos, foi usado pelo ditador romano Júlio César (100 a.C. - 44 a.C.), sendo tal modelo utilizado pela primeira vez na guerra da Gália.

César é tido por muitos historiadores como um dos maiores combatentes militares que se tem notícia um dos porquês que justificam essa alcunha, se dá pelo seu pioneirismo em codificar mensagens usadas durante batalhas com o objetivo de transmitir ordem e informações secretas. Suetônio, um historiador romano relatou grande parte da biografia de César no livro “As vidas dos Césares”. No livro é possível encontrar relatos de que a Cifra de César consistia em escrever dois alfabetos em linha reta, de modo que o alfabeto debaixo fosse deslocado sempre em três letras para a frente. Para uma ilustração melhor do fato vamos pensar que a letra de primeira posição no alfabeto, que no nosso caso é o A será trocada pela

letra de quarta posição D. O B que é a letra de segunda posição em nosso alfabeto seria substituído pela letra E que é a quinta letra do nosso alfabeto, o C que é a terceira letra será substituído pelo F que é a sexta letra. De um modo geral o número referente a posição é sempre somado a três no processo de criptagem pela Cifra de César.

Tabela 3 – Cifra de César

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
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

(Tabela elaborada pelo autor do trabalho)

Dessa forma ao fazermos a codificação com a Cifra de César da palavra AMOR obtemos a palavra DPRU.

Usando a tabela 3 qual seria então a forma criptografada da palavra CANETA? Fazendo uma consulta a tabela, temos que a letra C vai ser trocada por F, o A por D, o N por Q, o E por H, o T por W e o A por D. Logo a palavra CANETA ficaria criptografada como FDQHWD. Por outro lado sabendo que uma palavra foi criptografada com um deslocamento de três unidades resultando em HXOHU. Qual seria a forma decodificada dessa palavra? Fazendo o processo inverso partindo da segunda linha da tabela 3, a letra H será substituída por E, o X por U, o O por L, e o U por R. Assim a palavra obtida será EULER.

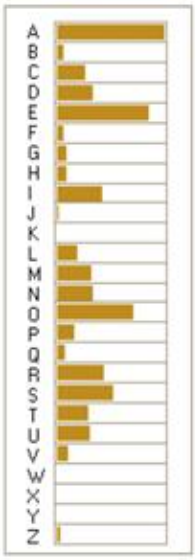
A chave para se criptografar nesses moldes é saber que o alfabeto foi deslocado em três unidades a direita. Embora hoje a Cifra de César seja facilmente decifrada, tomando como referência o contexto histórico da época a cifra foi de grande valia. Principalmente quando se pondera que a maioria dos inimigos do Império Romano eram analfabetos e quando não, os que tinham acesso a informações decodificadas pensavam se tratar de um outro alfabeto.

De forma geral as cifras de substituição monoalfabética são simples de serem quebradas, pois para esse caso existe um método denominado análise de frequência. Tal método é utilizado porque as letras tem frequência de aparição diferente quando considerado determinado idioma. Na língua portuguesa por exemplo a letra A é a mais utilizada na escrita de textos, a figura 4 representa uma

estimativa da frequência das letras utilizadas na língua portuguesa na escrita de textos.

Tabela 4– Tabela de frequência letras do alfabeto brasileiro

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



(Obtido em https://brutalsecurity.blogspot.com/2015/03/entendendo-criptografia-parte-6.html)

Para se traduzir um texto que foi cifrado por uma tabela monoalfabética, se organiza uma nova tabela, é registrada a frequência de aparição das letras, depois se faz uma comparação das frequências registradas na tabela de cunho próprio com a tabela 4. É necessário que se observe também as iniciais de cada palavra, os encontros consonantais e a estrutura de escrita do texto.

Para a ilustração do processo de análise de frequência vamos usar o exemplo que será dado, o qual irá explicar melhor como se decifrar um texto, no qual não se sabe qual o modelo de cifragem usado. Essa análise será feita por meio da observação das letras do alfabeto e também da observação de regras de escrita de textos. O texto escolhido é: “R UDWR URHX DV UROKDV GDV JDUUDIDV GH UXP GR UHL GD UXVVLD”.

Inicialmente o texto deve ser lido e é necessário que se observe algumas regularidades e alguns aspectos que ocorrem quando construímos frases e textos com o alfabeto usado no Brasil.

O primeiro passo é verificar a frequência de aparição da letra que mais se repete no texto. Fazendo a contagem, a letra do nosso texto com maior frequência de aparição é o D que aparece nove vezes, portanto de acordo com a tabela da

figura 4 o D provavelmente vai ser a letra A. Outra observação importante é que a letra que inicia o texto é o R, pelas regras de escrita, as únicas letras que podem ser usadas como iniciais de um texto são A e O. Como possivelmente o D fará papel de A, a letra R provavelmente será O.

Vamos fazer o primeiro teste de como ficará o texto ao trocar o D por A e o R por O, nesse sentido o texto por enquanto será: “o UaWo UoHX aV UoOKaV GaV JaUUaIaV GH UXP Go UHL Ga UXVVLa”.

Com o novo texto é perceptível que as palavras Go e Ga apresentam uma letra inicial comum, o G. Sendo que se as palavras são de duas letras possivelmente elas serão da, de ou do. Assim o G provavelmente será a letra D(qualquer outra letra que de forma simultânea substitua o G, fará as palavras perderem o sentido).

Fazendo agora a troca do G por D teremos o seguinte texto “o UaWo UoHX aV UoOKaV daV JaUUaIaV dH UXP do UHL da UXVVLa”,

Essa troca nos leva a observar que em dH, o H representa uma vogal. Entre as possibilidades de palavra temos da, de ou do. Pelas observações anteriores o A será equivalente ao D do texto original, a letra O será o R, assim em DH o h é equivalente ao E. Outra observação é a referente aos encontros consonantais das palavras JaUUaIaV e UXVVLa. Nas palavras da língua portuguesa a única possibilidade para o encontro de consoantes é RR ou SS o que nos leva a crer que U e V representam R e S. Para ter um pouco de certeza vamos recorrer ao texto do parágrafo anterior e observar que em “aV” e “daV” o V provavelmente representa S, logo U representa R.

Assim o texto se aproxima de sua significação original quando fazemos a troca de V(por S) e U(por R) e H(por E). Agora o texto passará a ser: “o raWo roeX as roOKas das JarraIas de rXP do reL da rXssLa”

A últimas palavras desse novo texto são “reL da rXssLa”, “reL” seria o equivalente a rei, então L é o equivalente a I. Se é rei, é rei de algum país. Dos países do globo o único com inicial R e encontro consonantal “SS” é a Rússia. Logo no nosso texto X representa U e L representa o I.

Fazendo essa última substituição teremos: “o raWo roeu as roOKas das JarraIas de ruP do rei da rússia”. Considerando o contexto a frase obtida será “O rato roeu as rolhas das garrafas de rum do Rei da Rússia.”

Note que com o auxílio da tabela de frequência e com algumas observações de escrita é possível quebrar uma cifra que use um único alfabeto. Em caráter de simplificação de entendimento o texto decifrado em nosso exemplo anterior, foi codificado através a Cifra de César. Textos criptografados por outros métodos que usam de cifra monoalfabética também podem ser decifrados com a estratégia adotada no texto do rato roedor de garrafas de rum. Ao longo da história o recurso de decifrar textos (monoalfabéticos) sem saber qual o processo utilizado para cifrar foi recorrente. E isso foi preponderante para que com o passar do tempo fossem criadas as cifras polialfabéticas.

Um dos episódios da história que exemplificam a fragilidade das cifras de substituição monoalfabética, foi a morte da rainha Maria da Escócia(1542 – 1587) que também atendia pela alcunha de Mary Stuart. Por motivos políticos Maria foi mantida em cárcere privado por 19 anos, cárcere esse ordenado por sua prima Elizabeth I que era rainha da Inglaterra e enxergava em sua prima uma ameaça a perda do trono real. Os boatos dão conta de que Maria conspirava uma subida a coroa inglesa por meio das cartas que trocava com Anthony Babington e John Ballard membros do clérigo inglês. O plano de execução de Elizabeth I ficou conhecido como Conspiração de Babington.

As cartas que descreviam os passos do plano de assassinato eram escritas de forma cifrada com cifras de substituição simples através de símbolos no lugar de letras e palavras. Interceptadas por agentes duplos que tinham proximidade com Maria I, as cartas foram decifradas pelo criptógrafo inglês Thomas Pheelipes.

Diante essas provas Maria I foi condenada e decapitada no ano de 1587. Há de se ressaltar que todo o roteiro de escrita das cartas e a sua intercepção por agentes britânicos foi um ato tramado pela rainha Elizabeth I que enxergava em Maria uma ameaça devido a sua forte ligação com a igreja católica. Se Maria I tivesse conhecimento de cifras polialfabéticas como a Cifra de Viginére talvez naquele momento seu destino tivesse sido diferente.

O método de análise de frequências foi criado pelo polímata árabe Abu Yusuf Ya 'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi (801-873), que também é conhecido como Al Kindi. Al Kindi desenvolveu seus trabalhos na área de Matemática na Casa da sabedoria de Bagdá. Nos anos áureos da biblioteca

aconteceu a produção de sua maior obra para a criptografia, o livro “Um manuscrito sobre a decifração de mensagens criptográficas”. Essa obra só foi tornada pública em 1987 quando foi descoberta no Arquivo Otomano Sulaima-niyyah de Istambul.

Figura 4 - Ilustração do busto de Al Kindi

(Obtido em https://www.9ways.org/sound-glossary/abu-yusuf-yaqub-ibn-ishaq-al-kindi)

A primeira vista o método de análise de frequência parece obsoleto nos dias atuais, mas durante a Idade antiga e a Idade Média o recurso foi de grande valia devido ao fato dos métodos criptográficos se resumirem em sua maioria em cifras monoalfabéticas.

> Daí em diante, mesmo ficando explícita a vulnerabilidade do método da substituição monoalfabética diante da análise de frequências, durante toda a Idade Média a Europa ainda utilizava esta técnica de criptografia. Na realidade, o avanço científico nesta época foi moroso, sendo que grande parte do conhecimento sobre a criptografia era considerado magia negra. A criação da criptoanálise como ciência, a partir da definição do método da análise de frequências, deu início a uma permanente luta entre os criadores e os quebradores de códigos, o que, desde aquela época, vem beneficiando ambas as partes (SANTOS, 2013, p. 20).

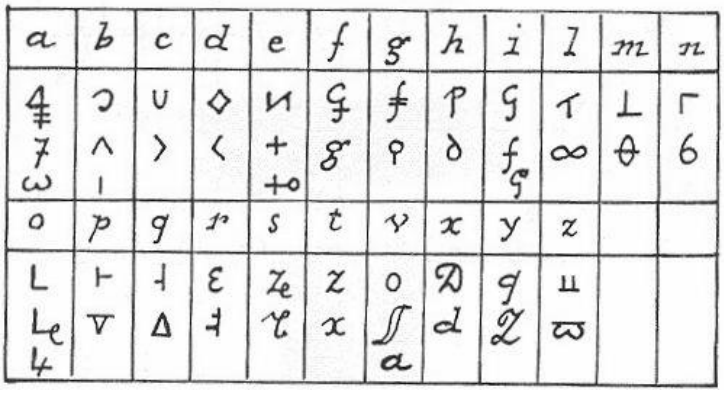
E nesse sentido a criptoanálise impulsionou o desenvolvimento da criptografia, substituindo os métodos de criptografia por métodos mais avançados como as cifras de substituição polialfabética, aquelas que faziam o uso de mais de um alfabeto pra codificar mensagens.

1.5 O disco de Alberti e o método de Giovan Batista Belaso

Antecedendo a criação das cifras polialfabéticas tivemos a criação das cifras homofônicas. A análise de frequências serviu para mostrar que criptografar com um único alfabeto não era vantajoso e com um hiato de tempo partindo da Idade antiga, as cifras polialfabéticas foram inventadas somente quando do Renascimento.

Nessa linha cronológica as cifras homofônicas foram criadas por volta do ano de 1411, no intuito de impor alguma dificuldade aos criptoanalistas. Nesse tipo de cifragem são incluídos os homófonos e os nulos. Os homófonos eram os diferentes caracteres que podiam representar uma mesma letra e os nulos eram símbolos inseridos no intuito de propiciar confusão quando fosse feita a análise de frequências. Abaixo segue um exemplo de Cifra homofônica.

Tabela 5– La Cifra General, usada pelo rei Felipe II



(Obtida em https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto08.html)

Simone de Crema foi um dos pioneiros na utilização da cifragem homofônica, em 1412 ele criou um cifra homônima, onde o número de símbolos para cada letra dependia da frequência que a letra aparecia em textos escritos em determinado idioma. Supondo que a Cifra tivesse como base o alfabeto usado no Brasil e consultando tabela 4 a letra A deveria ter 14 catorzes símbolos diferentes para sua representação(frequência de 14%), a letra E 12 e assim respectivamente.

Outro personagem que contribui com cifras mais elaboradas foi o italiano Leon Batista Alberti (1404 – 1472), considerado o pai da criptologia ocidental, que publicou o tratado De Componendis Cifris ou De Cifris acerca do tema em 1466. Nele era sugerido a cifragem usando dois ou mais alfabetos para uma mesma frase. A vantagem crucial do sistema de *Alberti* é que a mesma letra do sistema original

não aparece, necessariamente, como uma única letra no texto cifrado (LOUREIRO, 2014, p. 7).

A Leon Alberti também é atribuída a invenção do disco de Alberti.

> O disco de Alberti , é composto por dois anéis concêntricos, um externo e um interno. O anel externo é fixo, com 24 casas contendo 20 letras latinas maiúsculas (incluindo o Z, com U=V e excluindo H J K W Y) e os números 1, 2, 3, e 4 para o texto claro. O anel interno é móvel, com as 24 letras latinas minúsculas para o texto cifrado. As 20 letras maiúsculas estão em ordem alfabética e as 24 minúsculas estão desordenadas. Letras minúsculas fora de ordem é uma norma fundamental pois, caso estivessem em ordem, a cifra seria apenas uma generalização do Código de César. (TKOTZ, 2005, p, 194)

Figura 5 – Disco de Alberti

(Obtida em http://uenf.br/posgraduacao/matematica/wp-content/uploads/sites/14/2017/09/29082014Flavio-Ornellas-Loureiro.pdf)

O funcionamento do disco se dava da forma como será descrito a seguir. Cada um dos participantes do processo de comunicação portava uma cópia do disco.

Tomando o disco em questão era feito um giro e se escolhia uma letra que seria usada como referência de consultar. Para o exemplo vamos escolher a letra G, que no caso seria a letra de referência. Tomando uma frase qualquer de início as letras seriam substituídas como se apresentam no disco, ou seja, A por G, B por K, C por l e assim sucessivamente. Os numerais formavam números compreendidos

entre 11 e 4444, os quais eram associados a 336 palavras que continham as letras que estão omitidas no disco da figura, essas palavras eram registradas em um livro que era produzido em duas cópias, uma para o emissor e outra para o receptor da mensagem.

Diferente das cifras monoalfabéticas o método de Alberti oferecia uma vantagem que era a de fazer o uso de mais de um alfabeto na mesma frase. O uso era feito de forma que um grupo de quatro ou cinco letras era decifrado por um alfabeto, o próximo grupo de quatro ou cinco palavras era feito por outro alfabeto a troca de alfabeto era coordenada pelo giro do disco e da chave escolhida. A tabela 6 apresenta um modelo planificado do disco de Alberti, a tabela nos mostra como fazer o processo de criptografia de um texto por meio de agrupamento de palavras usando alfabetos diferentes.

Tabela 6 - Modelo de alfabeto cifrado pelo disco de Alberti

Texto limpo	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
1º alfabeto	**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
2º alfabeto	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**
Criptograma	d	e	f	g	h	S	t	u	v	w	x	y	z	Q	r	s	t	u	v	w	x	I	j	k	l	m

(Imagem obtida de: https://slideplayer.com.br/slide/395343/)

Repare que na tabela a primeira linha apresenta o nosso alfabeto como ele é. A segunda e a terceira linha dizem respeito ao alfabeto em sua forma criptografada. O primeiro alfabeto é um exemplo da Cifra de César, onde o A corresponde ao D, B corresponde ao E, C corresponde ao F e assim sucessivamente.

Tabela 7–primeiro alfabeto usado na tabela 6

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
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

(Tabela elaborada pelo autor do trabalho)

O primeiro alfabeto vai ser usado para as cinco primeiras letras do texto (número de letras em negrito da tabela 6) e também para as letras de posição catorze até a de posição vinte e um. O segundo alfabeto é uma cifra de César com o

deslocamento de treze unidades, onde o A corresponde ao N, B corresponde ao O, C corresponde ao P e assim sucessivamente.

Tabela 8 – segundo alfabeto usado na tabela 6

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

(Tabela elaborada pelo autor do trabalho)

O segundo alfabeto servirá para criptografar as letras de posição seis até as letras de posição treze (número de letras em negrito na terceira linha da tabela 6) e as letras de posição vinte dois a posição 26 no texto. Se o texto tiver mais que 26 letras o processo é o mesmo. Por exemplo, em um texto com cinquenta letras devem-se cifrar as letras de posição um a vinte e seis, e repetir o processo para as letras de posição vinte sete a cinquenta. Nesse caso a letra vinte sete seria equivalente à letra de posição um na tabela 6, a letra de posição vinte e oito equivaleria a letra de posição dois e a letra de posição cinquenta seria equivalente a letra de posição vinte e quatro. Vamos usar a tabela 6 para criptografar a frase a “A CASA DA FABIA É ROSA”. As cinco primeiras letras da frase serão criptografadas pela tabela 7, assim o primeiro A deverá ser trocado por D, o C por F, o segundo A por D, o S por V e o terceiro A por D. Da sexta a décima terceira letra da frase iremos usar a tabela 8, assim o D equivalerá ao Q, o A ao N, o F ao S, o B ao O, o I ao V e o E ao R. As letras de posição catorze a dezessete serão criptografadas novamente de acordo com a tabela 7. Assim, o R equivalerá ao U, O ao R, S ao V e A ao D. Portanto a frase “A CASA DA FABIA É ROSA”, quando criptografada pelo método da tabela de Alberti (tabela 6) ficará como “D FDVD QN SNOVN R URVD”.

Já podemos amadurecer a ideia de que o uso de mais alfabetos inviabiliza o método da análise de frequência, pois nesse exemplo simples as letras D e N são as mais frequentes. O que de acordo com a tabela levaria o leitor a impressão que D e N são letras diferentes do alfabeto, pois os mesmos apresentam frequências de aparição no texto diferente. Possivelmente o leitor que fosse tentar descriptografar a frase “D FDVD QN SNOVN R URVD”, iria deduzir que D e N representam A e E não necessariamente nessa ordem.

Na escala de evolução da criptografia o próximo grande feito é atribuído ao polímata alemão Johannes Trithemius (1462 – 1516), nesse aspecto foi de grande valia o seu trabalho intitulado Poligrafia, que foi publicado em 1518 dois anos após a sua morte. Na obra em questão é proposta a adoção de um sistema polialfabético por uso de uma tabela chamada *tabula recta,* a tabela tinha o mesmo número de linha e de colunas, sendo que a primeira linha era inserido o alfabeto padronizado e nas próximas linhas o alfabeto era apresentado de forma similar a cifra de César.

Tabela 9 - Modelo de tabula recta

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

(Figura obtida em http://www.multiwingspan.co.uk/cipher. php?page=vig)

Para fazer a cifragem se usava o seguinte método, a primeira letra da palavra era substituída pela sua correspondente na segunda linha da tabela, a segunda letra pelo seu equivalente na terceira linha, a terceira letra pelo seu correspondente na quarta linha e assim sucessivamente até chegar a última linha da tabela e fazer a repetição do processo se o número de letras não tiver acabado.

A título de exemplo vamos fazer a criptografia da Frase “A RATAZANA ROEU A ROUPA DA RAINHA DE ROMA” pelo método de Trithemius.

Para que a criptografia ocorra pelo método de Trithemius, vamos usar a correspondência da tabela 9. Assim na frase “A RATAZANA ROEU A ROUPA DA RAINHA DE ROMA” o A de início de parágrafo será trocado pelo correspondente ao A no primeiro alfabeto(segunda linha da tabela 9), no caso a própria letra A. O R é a segunda letra da frase, portanto será trocado pelo equivalente ao R no segundo alfabeto(terceira linha da tabela 9), no caso a letra S. O segundo A da frase será trocado pelo seu equivalente no terceiro alfabeto(quarta linha da tabela 9) que no caso é a letra C. Repetindo esse processo até a última letra A da palavra ROMA, obtemos a frase criptografada que é “A SCWEEGUI AYPG N FDKGS WU MWFLGA EG USRG”. Repare que o método de análise de frequência é ineficaz na tentativa de quebra desse tipo de cifra. Pois no texto criptografado as letras de maior frequência são o G(seis vezes) e W, E, A e S com frequência três. Usando a análise de frequência e a tabela 4, deduziríamos de maneira errada que a letra G corresponde a letra A, o que é um engano, pois a correspondência de letras pela tabula recta (tabela 9) não é feita de forma única. Ou seja a letra G pode assumir o valor A, mas também pode representar qualquer uma das vinte e cinco letras restantes do alfabeto. Portanto o uso de cifras polialfabéticas praticamente anula a utilidade da descriptografia de texto pela análise de frequências das letras.

Acompanhando a evolução da história humana a criptografia progride, sendo que o próximo grande colaborador é o italiano Giovanni Batista Bellaso(1505 – depois de 1568 antes de 1581) que em 1553 publica o livro “La cifra del Sig Giovan Batista Bellaso”, onde é descrita a ideia de chave para realizar os processos de criptografar e descriptografar mensagens. Para a consulta de alfabeto é usada a tabula recta (tabela 9) e uma chave que poderia ser uma palavra, uma frase ou uma

sequência de letras. Cada uma das letras da palavra a ser cifrada é substituída ordenadamente pela letras da palavra chave.

Para tornar mais claro o método vamos criptografar pelo método de Bellaso a frase “Deus é amor”, usando como chave a palavra “bigode”

Tabela 10 - Cifragem pelo Método de Belaso

CHAVE	B	I	G	O	D	E	B	I	G
PALAVRA A SER CRIPTOGRAFADA	D	E	U	S	E	A	M	O	R
RESULTADO DA CRIPTAGEM	E	M	A	G	H	E	N	W	X

(Tabela elaborada pelo autor do trabalho)

Olhando pela tabela fica fácil perceber que a chave é usada para se saber qual o alfabeto a ser utilizado, a letra D foi trocada pelo seu correspondente no alfabeto que se inicia por B, a letra E foi trocada pelo seu correspondente no alfabeto da letra I, a letra U foi trocada pelo seu correspondente no alfabeto que se inicia por G e assim é feito até a última letra da frase.

Para se decifrar faz se um processo análogo com a palavra chave.

Em 1586 o diplomata francês Blaise de Viginère publica o livro Traicté des Chiffres, no qual descreve o método de Bellaso e apresenta uma opção a mais de criptografar que seria usar o próprio texto como a chave de criptografia. Dessa forma era escolhida uma letra aleatória pra se iniciar o processo e as demais eram criptografadas usando o próprio escrito.

Posteriormente a literatura histórica atribui de forma errada a invenção do método de Bellaso a Viginère, portanto quando a referência for a cifra de Viginère deve se ter em mente que o método utilizado é o de Bellaso e de forma correta a cifra deveria ser nomeada com o nome do italiano.

Deve-se ressaltar que na época em questão o método de cifragem polialfabético era pouco prático, pois cifrar letra a letra era demorada e muitas vezes confuso, o uso desse método muitas vezes era restrito a estudiosos do tema. Por uma questão de praticidade eram usados livros de códigos denominados nomenclators. Tais livros apresentavam cifras de palavras e até mesmo de frases a fim de tornar a tarefa de criptografar menos trabalhosa.

Apesar de ter pouca utilidade prática para época, o método de cifragem polialfabético teve por quase 300 anos a áurea de indecifrável, sendo que somente em 1850 o método de Belasso foi quebrado pelo polonês Friedrich Kasiski e pelo inglês Charles Babbage.

> Por ser imune a análise de frequência de letras, a Cifra de Viginère ficou conhecida por quase dois séculos como a “cifra indecifrável”. Anos mais tarde, o sistema ficou arcaico e, dessa forma, o inevitável aconteceu: por volta de 1850, Charles Babbage e Friedrich Kasinski desenvolveram um sistema de decodificação para a cifra de Vigenère por meio da análise de palavras, algo parecido com as análises feitas pelos teólogos mulçumanos no fim do primeiro século. (SCHURMAN, 2013, p, 23)

Era necessário um passo adiante pra garantir que mensagens de conteúdo privado fossem transmitidas de forma mais segura, talvez um novo método, talvez uma segurança maior no processo de se escolher a chave de criptografar.

1.6 Máquinas de cifragem utilizadas no século vinte

Considerando o período das grandes guerras mundiais três máquinas criptográficas tiveram importância no desenrolar do confronto e foram elas a Colossus, Enigma e Purple (máquina japonesa de funcionamento similar a Enigma).

A máquina Enigma foi criada em 1918 na Alemanha por Arthur Scherbius e Richard Ritter. Inicialmente uma versão rudimentar da máquina Enigma foi inventada por Hugo Alexander Koch, essa versão era denominada de máquina de rotor e tinha esse nome por funcionar com rotores eletromecânicos que produziam mensagens criptografadas Koch patenteou a ideia, mas não trabalhou em seu posterior aperfeiçoamento.

As melhorias foram implementadas por Scherbius e Ritter, sendo que a criptografia na máquina Enigma era feita por um mecanismo similar ao disco de Alberti e funcionava por meio de eletricidade. Os componentes operacionais da máquina eram um teclado, uma unidade de cifragem e um visor. Para realizar a cifra de uma mensagem, o teclado era usado para inserir um a um os caracteres do texto, na unidade de cifragem, cada letra era transformada em outra, sendo que o resultado era apresentado de forma instantânea no visor da Enigma. Na primeira versão da máquina a unidade de cifragem era composta por três misturadores, cada

um com vinte e seis possíveis posições, a posição inicial dos misturadores formava a chave da cifra. Nas versões aperfeiçoadas a Enigma continha cinco rotores.

Após a criação e patenteamento do Enigma a fábrica dos amigos alemães começou a operar e vender a máquina em escala comercial, vale ressaltar que de início a comercialização não atingiu seus objetivos, transformando o investimento dos amigos em fracasso. Somente em 1920 é que as máquinas foram compradas pela marinha alemã e posteriormente por todo o exército alemão.

Figura 6 – Máquina Enigma

(Obtida em https://muitocurioso.org/enigma-maquina-eletromecanica-de-criptografia/)

Na década de 30 sob a vigência do nazismo a Enigma passou por melhorias, sendo usada fortemente pelo exército alemão em todas as suas missões. Sob as ordens de Hitler existia uma cautela imensa quanto ao uso da máquina, a fim de que a mesma não fosse “decodificada”. Para isso era usado um livro de códigos entre o emissor e o receptor das mensagens e a chave da máquina era atualizada diariamente a fim de se evitar interceptação de informações.

No período da Segunda Guerra a Enigma foi muito utilizada, sendo importante na distribuição de informações de tática de guerra e no decorrer de várias batalhas aéreas. Por muito tempo a Enigma manteve um caráter de máquina indecifrável, pois era possível a elaboração de 1058691676442400 chaves distintas. Fazer essa decifração com os métodos até então disponíveis era uma tarefa humanamente impossível.

Na intenção de quebrar a criptografia da máquina uma equipe de cientistas poloneses, franceses e ingleses se reuniu em Bletchley Park, onde ficava a sede da

Escola de Cifras e Códigos do governo inglês. A operação que visava a quebra dos códigos foi batizada de Ultra tendo início em 1939, sendo que no ano de 1943 depois de muito trabalho a criptografia da Enigma foi quebrada.

> Descobriram que alguns operadores de rádio alemães, especialmente um homem chamado Walter, estavam a ignorar as instruções e iniciavam as suas máquinas com a mesma chave todos os dias. Calcularam, acertadamente, que as unidades alemãs espalhadas por toda a Europa transmitiriam mensagens idênticas pelo aniversário do Führer, em abril de 1940. E deitaram as mãos a uma máquina Enigma atualizada que a marinha britânica obtivera num navio meteorológico alemão capturado ao largo da Groenlândia (NORMAN, 2008. p. 55).

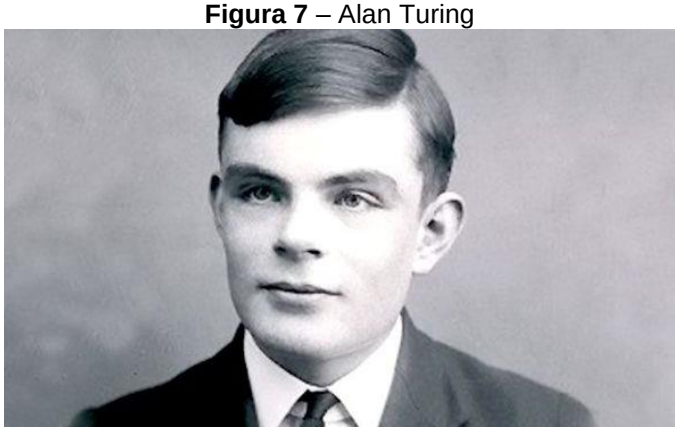
Perante ao descuido dos alemães em não trocar as chaves da máquina diariamente, a operação Ultra teve êxito em ter acesso aos códigos da Enigma, conseguindo entender todo o processo de codificação e fazer a criptografia das mensagens nazistas. A reação dos alemães aconteceu em 1944 com o desenvolvimento de um aparato ainda mais sofisticado, a máquina *B-Schreber.* Para a compreensão e quebra dos códigos da nova máquina foi imprescindível o trabalho de Alan Maison Turing, que atualmente é conhecido como o pai da ciência computação. Turing trabalhou arduamente em conjunto com William Gordon Welchman, Stewart Milner-Barry e Alfred Dilwyn (“Dilly”) Knox” pra desenvolverem a calculadora eletromecânica Bomb, que testava várias configurações de criptografia ao mesmo tempo. De forma consequente a invenção da Bomb deu propulsão aos estudos realizados em Bletcheley Park, sendo que anos mais tarde foi criado primeiro computador que se tem notícia, o Colossus.

> Em seguida, a Bomba de Turing, uma calculadora eletromecânica, conseguiu descobrir as permutações e produzir respostas. No segundo ano da guerra, Bletcheley Park estava a ler todas as transmissões da Enigma três horas depois do início de cada dia. Acompanhavam todas as atualizações a que procediam os alemães. E, em 1944, para rivalizar com o B-schreiber, inventaram o primeiro computador eletrônico do mundo, o Colossus. (NORMAN, 2008. p.56).

Apesar de toda a genialidade de Turing e de seus estudos serem a base para a computação moderna, o mesmo ainda é muito pouco conhecido do público geral. Muito provavelmente pelo fato de ser homossexual e pelo fato de que na

década de 40 o homossexualismo ser considerado crime na Inglaterra. A versão mais conhecida sobre a morte de Turing é que em seus últimos dias de vida foi condenado a castração química, pelo fato de ser homossexual, tendo cometido suicídio com cianeto aos 41 anos de idade em Winslow na Inglaterra.

Figura 7 – Alan Turing



(Figura obtida em http://horizontes.sbc.org.br/index.php/2016/11/22/alan-turing-e-a-enigma/)

É fato que os pesquisadores de Bletchley Park levaram vantagem sobre os criadores de código do exército nazista. Há de se fazer menção que os estudiosos de Bletchley tiveram um bom referencial teórico no estudo da quebra dos códigos alemães. Na década de 30, mais especificamente no ano de 1933 os poloneses Marian Rejewski, Jerzy Różycki e Henryk Zygalski quebraram o código da primeira versão militar da máquina Enigma. Os poloneses fizeram uso de espionagem, intuição matemática e contaram com um pouco de sorte. Um funcionário do Ministério da Guerra em Berlim, chamado Hans-Thilo Schmidt, vendeu documentos secretos a um espião francês, que de posse dos documentos fez o envio aos matemáticos poloneses. A informação secreta foi de grande valia para que Marian Rejewski e seus colegas decifrassem a Enigma. A cópia dos mecanismos de encriptação obtidas por meio de Schmidt permitiu que os poloneses construíssem uma réplica da Enigma, um modelo similar da réplica se encontra exposto no museu da matemática Arithmeum, em Bonn na Alemanha.

Tão importante quanto as bombas de Turing foi a máquina Colossus, que foi criada para decifrar os códigos da máquina Lorenz SZ40. A Colossus foi a primeira máquina programável a ser construída, para muitos ela foi uma primeira versão de computador e teve importância fundamental para o desenvolvimento da criptografia no período pós guerra. A máquina Lorenz SZ40 era utilizada para a comunicação

entre Hitler e os generais de seu exército. Em termos operacionais a Lorenz SZ40 tinha algumas semelhanças com a Enigma, mas a distinção entre as máquinas se dava pelo fato da Lorenz apresentar muito mais possibilidades de chave do que a Enigma. Mesmo sendo uma máquina com cifras muito difíceis de serem descriptografadas dois pesquisadores de Bletchley John Tiltman e Bill Tutte descobriram fragilidades no processo operatório da Lorenz, o que abria a possibilidade para se revelar um modo de decifrar a Lorenz SZ40.

As bombas de Turing apresentavam uma velocidade absurda para a realização de tarefas humanamente impossíveis pelo método da força bruta, porém as Bombas não podiam ser programadas para realizar tarefas de análise e tomada de decisões condicionadas a ocorrência de eventos. Diante dessa limitação e referendando pelos estudos de Turing, Maxwell Herman Alexander Newman projetou uma máquina que seria capaz de resolver diferentes problemas, mediante a uma programação, que em outras palavras seria um computador. Um fato notório é que os diretores de Bletchley arquivaram o projeto de Newman por o acharem o impossível de ser construído. Eis que surge a figura de Tommy Flowers, um engenheiro eletrônico que trabalhava para o General Post Office (GPO), serviço de telecomunicações do governo Britânico. Como Flowers estava a par sobre os debates da construção da máquina Colossus ele decidiu prosseguir com a execução do projeto de Newman e depois de dez meses ele conclui a construção da máquina, entregando-a aos chefes da operação Ultra em 8 de dezembro de 1943. A Colossus tinha 1.500 válvulas eletromecânicas que eram mais rápidas do que os relés eletromecânicos das Bombas de Turing. Além da velocidade a vantagem da Colossus é que ela era uma máquina programável e podia realizar diferentes tarefas, de acordo com os comandos de entrada de dados.

Com o fim da Segunda Guerra a máquina Colossus foi destruída, assim como todos os outros registros dos estudos realizados no período de guerra. Os cientistas que trabalharam como quebradores de códigos também foram impedidos de falar sobre tudo o que ocorreu em Bletchey. Mesmo contrariado ao receber as ordens de queimar o projeto da Colossus Tommy Flowers foi obediente e queimou todos os registros do projeto. A destruição do projeto da Colossus fez com que por

muito tempo outros cientistas levassem os créditos da criação do primeiro computador.

No ano de 1945 John Adam Presper Eckert Jr e John William Mauchly em parceria com engenheiros da Universidade da Pensilvânia desenvolveram o ENIAC(Eletronica Numerical Integrator and calculator), que tinha 17.468 válvulas eletrônicas, que em conjunto podiam realizar até cinco mil cálculos por segundo. Por muito prevaleceu o pensamento de que a ENIAC foi o primeiro computador ao invés da máquina Colossus que foi criada anos antes.

1.7 Criptografia usada nos computadores

O desenvolvimento da criptografia no período pós-guerra acompanhou o desenvolvimento e as novas tecnologias que foram criadas no aperfeiçoamento dos computadores. Os computadores foram usados para quebrar todo o tipo de cifras. E isso era possível devido a rapidez de execução de tarefas pelo computador, o que tornava mais fácil o trabalho de descrever todas as chaves possíveis de um sistema de criptografia.

Nesse sentido o uso do computador foi essencial na disputa entre codificadores e decodificadores. O computador apresenta alguns mecanismos de cifragem semelhantes as cifras mais tradicionais como as cifras de substituição e transposição. Porém o computador apresenta diferenças em relação as formas tradicionais de cifragem e máquinas como a Bomb. Uma diferença é que o computador pode ser programado para simular o comportamento de diferentes tipos de cifra, outra diferença é a velocidade de execução de uma tarefa. Outra diferença é que o computador trabalha com a cifragem de sequências de dígitos binários(sistema dito de base 2 e que usa apenas os algarismos 0 e 1 para representar números). A transformação das letras em sequências de binário se dá por meio da aplicação de protocolos. Um exemplo de protocolo é o American Standart Code for Identification Interchange(Código Padrão Americano para Troca de Informações), conhecido pela sigla ASCII. O ASCII faz uma correspondência entre cada letra do alfabeto e uma sequência de sete dígitos binários. Dessa forma com o protocolo ASCII é possível construir uma sequência de até 128 caracteres,

pois cada caractere pode ser ocupado por dois valores(0 ou 1) e pelo princípio fundamental da contagem temos que 2^7 = 128.

A tabela abaixo representa como os números são lidos pelo computador após serem digitados numa plataforma do protocolo ASCII.

Tabela 11 - Correspondência gerada pelo protocolo ASCII

LETRAS MAIÚSCULAS REPRESENTADAS NO ASCII				
A	1000001		N	1001110
B	1000010		O	1001111
C	1000011		P	1010000
D	1000100		Q	1010001
E	1000101		R	1010010
F	1000110		S	1010011
G	1000111		T	1010100
H	1001000		U	1010101
I	1001001		V	1010110
J	1001010		W	1010111
K	1001011		X	1011000
L	1001100		Y	1011001
M	1001101		Z	1011010

(Tabela elaborada pelo autor do trabalho)

Se uma pessoa digita a palavra UVA o protocolo ASCII a entende como a seguinte sequência de binários 1010101 1010110 1000001. Vamos fazer uma simulação de cifra para a palavra UVA. O processo de cifragem consistirá na troca de posição entre os dígitos vizinhos, ou seja o primeiro dígito é trocado pelo segundo, o terceiro pelo quarto e assim até chegar ao sétimo dígito que ficará na mesma posição. Nessas condições a cifra da palavra UVA seria 01010110101110010000 1.

Com o barateamento em sua produção o computador se tornou um item mais acessível a população civil. Um fato muito importante para essa popularização, foi a invenção do transistor em 1947 pela companhia AT&T Bell Laboratories que substituiu a válvula eletrônica. A produção de computadores mais acessíveis a população civil teve início em 1951 quando a empresa Ferranti iniciou a produção de computadores sob encomenda. No ano de 1953 a IBM também iniciou suas atividades com a produção de computadores, sendo que em 1957 lançou a linguagem de programação FORTRAN para que seus usuários pudessem escrever e executar programas para computadores.

Na década de 60 o computador se tornava mais popular e era usado em grandes empresas para troca de correspondências, envio de documentos e realização de algumas operações bancárias. Havia aí um problema, os algoritmos de cifragem não eram padronizados e muitas vezes o algoritmo usado por uma empresa A não era o mesmo usado pela empresa B, dessa forma as empresas A e B não conseguiriam se comunicar devido a diferença de algoritmos.

Devido a esse impasse o NBS(National Bureau of Standards American) em 15 de maio de 1973 lança uma proposta de seleção de um algoritmo de cifra padrão para realização de troca de informações confidenciais entre empresas.

O algoritmo Lucifer da IBM era um dos algoritmos criptográficos mais utilizados . Um dos protagonistas da criação do algoritmo foi um cientista alemão chamado Horst Feistel, que emigrou para os Estados Unidos no ano de 1934. Devido a ter chegado aos Estados Unidos durante a ocorrência da Segunda Guerra Mundial, Foster foi colocado de forma preventiva em estado de prisão domiciliar, permanecendo assim até em 1944. Devido ao medo de novas represálias Feistel deixou de tralhar com criptografia por algum tempo. Porém ele acabou fazendo pesquisas com criptografia quando prestava serviços ao Cambridge Research Center, órgão militar dos Estados Unidos.

O fato de Feistel continuasse atuando no desenvolvimento de algoritmos de criptagem fez com que ele tivesse problemas com a NSA (National Security Agency), que é o órgão estatal Norte Americano incumbido de manter seguras as comunicações militares, da cúpula do governo dos EUA e por espionar e decifrar correspondências de outros países.

A NSA continuou sua perseguição a Feistel, intervindo para que seu projeto de algoritmo fosse sabotado e cancelado mais uma vez. Por fim Feistel começou a trabalhar na IBM, onde no ano de 1971 desenvolveu em conjunto com a sua equipe o Lucifer. O Lucifer era considerado o algoritmo de encriptação mais seguro de sua época daí a predileção por sua adoção como padrão. Porém a NSA queria garantir que a cifra fosse segura o suficiente para uso empresarial, mas que pudesse ser quebrada de alguma forma por seus membros usando o recurso tecnológico dos computadores que dispunham. Para isso a NSA estabeleceu uma condição, onde o Lucifer só seria adotado como padrão se fosse elaborada sua versão mais “frágil”, a

chave a ser empregada no Lucifer tinha 56 bits. Essa nova versão foi batizada de DES(Data Encryption Standard) e foi adotada em 23 de novembro de 1976, sendo usada maciçamente por indústrias, escritórios de grandes corporações e bancos. Em 1980 o ANSI (American National Standards Institute) estabeleceu que o DES seria o algoritmo padrão para o sistema bancário. Provavelmente a perseguição da NSA a Feistel não se deu pela sua nacionalidade, mas muito mais pelo fato dele estar desenvolvendo um algoritmo tão seguro que impedia a capacidade de intervenção do NSA no processo de captação e espionagem de mensagens.

1.8 A solução do problema da troca de chaves

A adoção do DES resolveu o problema da padronização de chaves, assim era possível que duas empresas diferentes trocassem correspondências e dados com um nível de segurança maior. Porém com o sucesso do computador e pelo fato de cada vez mais empresas fazerem o seu uso, a distribuição de chaves tornou-se uma tarefa difícil de ser executada do ponto de vista da logística de distribuição. Com o início do uso do DES, na década de 70, os bancos quando enviavam informações a seus clientes contratavam um mensageiro que entregava pessoalmente a chave de criptagem. Esses funcionários percorriam vários lugares do mundo com maletas, distribuindo de forma individual cada chave. Esse procedimento além de não ser totalmente seguro demandava tempo e isso tornava a troca de informações demorada.

Ao longo da história o problema da distribuição de chaves tem se constituído uma questão de difícil solução. Foi assim quando usuários da Cifra de Viginére entregavam pessoalmente a palavra-chave ou durante a Segunda Guerra quando os submarinos alemães faziam de certa forma um estoque de suprimento de chaves para fazer comunicação por meio da máquina Enigma.

Novamente voltando a década de 70 a agência estatal norte americana COMSEC que era responsável por segurança em processos de comunicação, realizava a distribuição de uma grande quantidade de chaves através de navios que atracavam nos portos das cidades mais importantes dos Estados Unidos. De lá os “criptozeladores”, funcionários de uma empresa responsáveis pela entrega das

chaves, recolhiam as chaves(que eram distribuídas em disquetes e fitas) de sua responsabilidade e a entregavam em seus respectivos destinos.

O maior problema nesse contexto era o de confiar informações tão importantes a uma pessoa e de fato esse processo era arriscado, pois se o criptozelador fosse de má índole poderia vender as chaves ou ainda no meio do processo as chaves poderiam ser tomadas por meio de furto.

Esse contratempo da distribuição de chaves foi resolvido no ano de 1976, com a publicação do protocolo Diffie-Hellman-Merkle, desenvolvido em um estudo comandado por Whitfield Diffie, Martin Hellman e Ralph Merkle.

Whitfield Diffie foi um dos criptógrafos mais envolvidos com o estudo do problema de distribuição de chaves. Diffie nasceu em Washington no ano de 1944, tendo passado grande parte da sua infância em Nova Iorque. Desde a infância Diffie demonstrou paixão por números e Matemática, tanto que em 1965 concluiu sua graduação no Instituto de tecnologia de Massachussets. Após a conclusão do curso de graduação Diffie teve vários empregos relacionados a segurança computacional. No início dos anos 70 Diffie era um dos poucos especialistas em criptografia computacional que não trabalhava para o governo e nem para grandes empresas do ramo. Ele dedicava parte do seu tempo a estudar e tentar resolver o problema da distribuição de chaves, Diffie tinha a crença de que a resolução do problema poderia propulsionar a elaboração de redes de comunicação, na qual os computadores estariam interligados para se comunicar e distribuir informações.

A rede imaginada por Diffie foi desenvolvida pela Agência de projetos avançados de pesquisa (ARPA). A rede foi criada em 1969 e tinha o nome de Arpanet e seu objetivo era interligar computadores militares que se encontravam a longas distâncias. De início a Arpanet tinha a disposição quatro sites interconectados. A rede foi se expandindo e no ano de 1982 ela passou a se chamar internet. Entre o fim dos anos 80 e começo dos anos 90 a Internet se expandiu deixando de ser usada somente no meio militar e fora do rol acadêmico. Atualmente mais de 4 bilhões de pessoas utilizam a internet para trocar e-mails, usar redes sociais e fazer compras.

Em seus estudos Diffie já antevia esse cenário em que as pessoas usariam uma rede de computadores pra se comunicar e fazer compras a distância. Ele

demonstrou preocupação em como as pessoas iam desenvolver essas atividades com o máximo de privacidade, outra indagação de Diffie era a de como realizar a troca de chaves, tendo em vista que seria inviável enviar as chaves de criptagem uma a uma, em cada residência, empresa ou órgão governamental.

No ano de 1974 Diffie dá uma palestra na IBM onde descreve sua pesquisa referente a procura de solução para o problema da distribuição das chaves. A maior parte dos ouvintes presentes recebe as ideias de Diffie de forma cética, duvidando de que algum dia se desenvolveria um método com grande eficácia para se trocar chaves. Um dos poucos entusiastas da palestra de Diffie foi Alan Konheim, que era um dos principais especialistas de criptografia da IBM. Após a palestra em um diálogo com a Diffie Alan diz que um professor de Stanford na Califórnia desenvolvia pesquisas que visavam solucionar o problema da troca de chaves, o professor atendia pelo nome de Martin Hellman.

Na mesma noite da palestra, Diffie pega seu carro e anda 5 mil quilômetros até chegar a casa de Hellman. Hellman nasceu em 1945 em Nova Iorque, sendo praticante da religião judaica. O desejo de Hellman em estudar criptografia foi impulsionado por sua determinação, desde adolescente Hellman demonstrou interesse em temas de criptografia e sempre realizava a leitura de livros ligados ao tema.

No início de seus estudos Hellman teve como referência teórica o livro The Codebrakers de David Kahn tendo o destrinchado, sendo o livro o seu guia até o momento do encontro com Diffie.

> The Codebrakers foi o único companheiro de Hellman em sua pesquisa, até setembro de 1974, quando ele recebeu uma inesperada chama telefônica de Whitfield Diffie, que acabará de atravessar o país para encontra-lo. Hellman nunca ouvira falar de Diffie, mas concordou, hesitantemente, em recebe-lo, durante meia hora, no final daquele dia. Ao fim do encontro, Hellman percebeu que Diffie era a pessoa mais bem-informada que ele já encontrará. O sentimento foi mútuo. Hellman lembra: “Eu tinha prometido a minha mulher que iria para casa tomar conta das crianças, e assim que cheguei em casa com ele e jantamos juntos. Ele partiu por volta da meia noite. Nossas personalidades eram muito diferentes, ele é muito mais ligado a contracultura do que eu, mas depois deste choque de personalidades transformou-se numa relação muito simbiótica(SINGH, 1999, p, 280).

Após esse encontro Hellman fez articulações para que Diffie fosse contratado como estudante graduado, atuando na Universidade de Stanford. Trabalhando em conjunto Diffie e Hellman não pouparam esforços na busca de uma solução para o problema de se transportar chaves a longa distância. Algum tempo depois o grupo formado por Diffie e Hellman acolhe Ralph Merkle. Ralph Merkle fez sua graduação na Livermore High School, no ano de 1970 ele inicia seu curso de ciências da computação na Universidade de Berkeley, obtendo seu bacharelado em 1974. Em 1979, Merkle se torna Phd em engenharia elétrica da Universidade de Stanford, com uma tese intitulada “Sigilo, autenticação e sistemas de chave pública”.

> Como diz Hellman “Ralph como nós, estava disposto a bancar o tolo. E o modo de se alcançar o cume em termos de desenvolvimento de pesquisas originais é ser um tolo, porque só os tolos continuam tentando. Você tem a ideia número 1, fica empolgado e então ela fracassa. Então tem a ideia número 2, fica empolgado e ela também fracassa. Depois você tem a ideia número 99, fica empolgado e ela também fracassa. Só um tolo se entusiasmaria com ideia número 100, mas podem ser necessárias 100 ideias antes que realmente uma dê resultado. E ao menos que você seja suficientemente bobo para continuar se empolgando, não terá a motivação, não terá a energia para ir até o fim. Deus recompensa os tolos”(SINGH, 1999, p, 281).

O maior desafio do trio (Diffie-Hellman-Merkle) residia no fato de como fazer a chave de criptografar cheguasse ao seu destino sem a necessidade de um atravessador. Imagine que duas pessoas queiram trocar mensagens criptografadas por meio de telefone. Inicialmente a mensagem deve ser cifrada e a pessoa deve usar uma chave, que deve ser secreta, caso contrário qualquer pessoa pode decifrar a mensagem a ser transmitida. Em linhas gerais antes de todo o processo de cifrar a mensagem as pessoas devem compartilhar a chave a ser utilizada, pois a mesma chave é usada para descriptografar os escritos.

Na ilustração desse processo criptográfico, usamos uma história clássica que é empregada de forma recorrente para descrever as especificidades do problema da troca de chaves, é a história de Bob, Alice e Eva.

Imagine que Alice quer mandar uma mensagem para Bob e Eva tem a intenção de descobrir o conteúdo da mensagem. Alice irá cifrar os textos e manda-los para Bob, porém Bob deverá ter a chave usada por Alice para saber

descriptografar o texto e saber o conteúdo da mensagem. Uma forma de resolver esse problema é que Bob e Alice se encontrem para fazer a troca de chaves, esse encontro poderá ser semanal e eles podem trocar chaves o suficiente por um determinado período de tempo. A limitação dessa prática é que Alice ou Bob podem estar atarefados e não ter tempo pra trocarem chaves. Alice poderia contrair uma doença e assim não poderia comparecer aos encontros. Uma solução alternativa seria a de contratar uma pessoa responsável pelo processo de entrega das chaves, mas como dito em outra oportunidade o ponto fraco dessa estratégia é que o mensageiro poderia não ser uma pessoa de confiança e aí ele poderia fazer a leitura das mensagens ou entregar a chave a qualquer outra pessoa. Com a expansão da internet as soluções encontradas até aqui seriam insuficientes para garantir o sigilo de troca de informações entre todos os usuários da rede. Vamos imaginar agora outra possibilidade para a história de Bob e Alice com uma saída alternativa para o problema da troca de chaves. Alice vai aos correios e manda sua mensagem em uma caixa de ferro trancada com seu cadeado pessoal. Ao receber a caixa Bob a tranca agora com o seu cadeado e a reenvia para Alice. Alice ao receber a caixa novamente destranca o seu cadeado e envia a caixa para Bob mais uma vez. Ao receber a caixa Bob destranca o seu cadeado, tendo acesso a mensagem escrita por Alice. Enfim essa parecia uma solução para o problema da distribuição de chaves.

O que esse exemplo diz é que seria possível Alice criptografar a mensagem com sua chave, Bob criptografaria o recebido por Alice, ao receber novamente a mensagem de Bob, duplamente criptografada Alice a decodificaria com sua chave, devolvendo os escritos para Bob e finalmente Bob decodificaria o escrito final com sua chave. Mas será que isso é possível com as cifras de criptografia que usamos?

Vamos usar as chaves de Alice e Bob aplicando o raciocínio de dupla cifragem para criptografar a palavra MAU.

Tabela 12 - Chave de Alice

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

(Tabela 12 - autoria própria)

Tabela 13 - Chave de Bob

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
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

(Tabela 13 - autoria própria)

PALAVRA:	MAU
CIFRADA COM A CHAVE DE ALICE:	GWM
CIFRADA COM A CHAVE DE BOB:	SIY
DECIFRADA COM A CHAVE DE ALICE:	KBD
DECIFRADA COM A CHAVE DE BOB:	YPR

É fácil de perceber que o exemplo da inserção dos dois cadeados não funciona com cifras, a palavra MAU, quando criptografada por esse processo não produziu a palavra correta quando é decifrada por Bob no último estágio do processo. Se uma mensagem fosse cifrada por esse método a mensagem chegaria com o conteúdo incorreto ao destinatário.

Esse método de dupla criptografia só funcionaria se a decodificação de Bob for feita antes da de Alice. Se isso não ocorrer o método produzira resultados como o aqui experimentado. O modelo da caixa trancada com dois cadeados era inconcebível na prática, mas a comparação serviu para que Diffie e Hellman procurassem uma solução para o problema da distribuição de chaves. A pesquisa de Diffie, Hellman e Merkle consistiu na procura de funções matemáticas que pudessem ser usadas no processo de criptagem. Em Matemática entende-se como função uma operação ou conjunto delas que transforma uma entrada (número ou objeto) em outro correspondente. O dobro é uma função matemática, que transforma todo número de entrada em uma quantidade duas vezes maior ou menor. A função dobro transforma o número dez em vinte e o número x em 2x.

Mais precisamente eles concentraram seus esforços na busca por um sistema de encriptação que utilizasse funções de mão única ao invés de funções de mão dupla. Mas afinal o que é função de mão única e função de mão dupla? Em termos computacionais a função de mão única é uma função que é fácil de calcular a imagem para qualquer entrada (domínio), mas é difícil de inverter, ou seja dado o

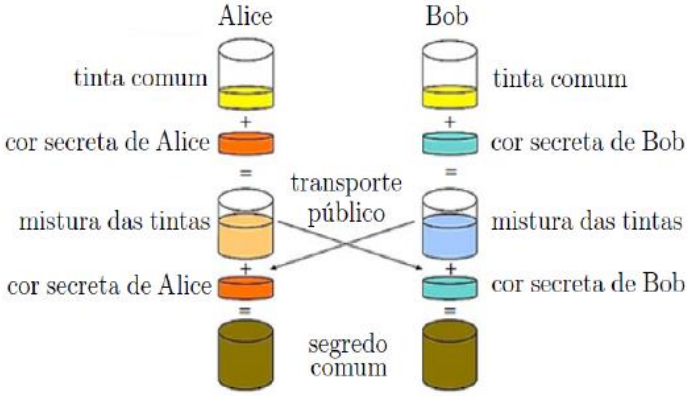
valor da imagem é difícil determinar que valor do domínio gerou tal resultado. A função de mão dupla é aquela que é fácil calcular a imagem através do valor de entrada e também é aquela em que dado um valor da imagem é fácil de determinar qual valor do domínio gerou tal imagem.

A função triplo é uma função de mão dupla, pois é fácil saber qual a imagem de número dez é trinta e também é fácil saber que se um número(x) gerou o valor vinte e quatro como imagem, esse número(x) só pode ser o número oito.

As funções de mão única procuradas por Diffie, Hellman e Merkle foram encontradas no estudo aprofundado de aritmética modular. A aritmética modular parte de um conceito bem simples que é a definição de módulo. (Para se aprofundar mais sobre a definição de módulo, seus desdobramentos e seu emprego em criptografia é recomendada a leitura do livro “Aritmética” da coleção PROFMAT, cujo autor é Abramo Hefez. O livro aborda aspectos da aritmética, de módulo, congruência e de aplicações de aritmética em Criptografia).

Uma analogia que pode ser usada para compreender a troca de chaves por meio de função de mão única é o exemplo do misturador de tintas. O esquema irá representar a troca de chaves usando cores de tinta, ao invés de números. De início Alice e Bob escolhem a mesma cor para dar entrada no misturador, no nosso exemplo a cor será amarela. A cor inicial é de conhecimento público, sendo assim Eva que pretende ter acesso às mensagens trocadas por Bob e Alice pode ter conhecimento dessa cor. Em seguida Alice e Bob escolhem individualmente suas cores secretas (Eva não tem acesso a essas cores), que serão misturadas a tinta amarela. No nosso exemplo a cor secreta de Alice é laranja e a cor secreta de Bob é azul. A parte mais importante do processo é quando Alice e Bob trocam suas misturas iniciais (Amarelo e laranja mistura de Alice e amarelo e azul mistura de Bob), esta mistura, resultado das combinações da cor comum (amarela) e das cores secretas, muito dificilmente será revertida por Eva, pois é impossível separar as cores misturadas por Alice e Bob em seus respectivos misturadores. A figura a seguir representa uma ilustração de como se dá a troca de chaves (tinta) por meio de uma função de mão única.

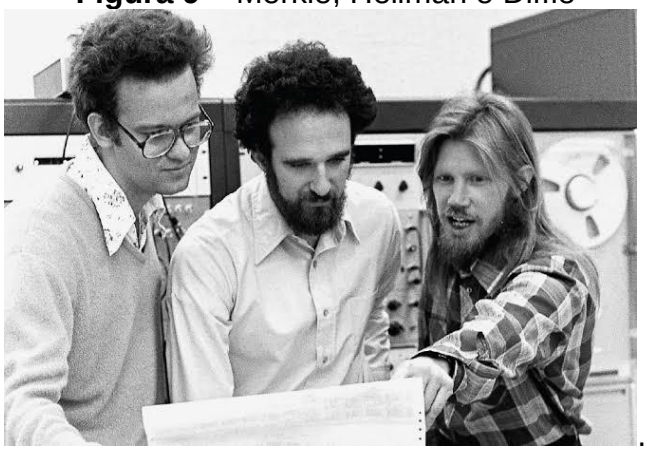
Figura 8 – Misturador de tintas



(Figura obtida em https://pt.wikipedia.org/wiki/Diffie-Hellman)

A descoberta do esquema de troca de chaves por meio de função de mão única alçou o trio Diffie, Hellman e Merkle ao rol dos grandes cientistas da computação do século XX. Os escritos do trio fizeram com que a criptografia fosse reestruturada em razão da solução do problema de distribuição de chaves. Em junho de 1976 o trio apresentou de forma pública sua pesquisa na Conferência Nacional de Computação.

Figura 9 – Merkle, Hellman e Diffie



(Figura obtida em: https:news.stanford.edu/2016/03/01/turing-hellman-diffie-030116/)

1.9 A criptografia de chave pública

A utilização de funções de mão única resolveu o problema da troca de chaves, mas existia um inconveniente. Para que isso fosse possível os dois envolvidos no processo deveriam estar conectados, pois a determinação da chave dependia das duas partes envolvidas. O problema residia no fato de que a troca de

chaves proposta por Hellman por vezes poderia não ser espontânea. Imagine que Alice deseja mandar uma mensagem para Bob de extrema urgência e que nesse dia em específico Bob não tenha acesso a internet, nesse caso Alice ficaria impossibilitada de mandar o e-mail, pois a troca de chaves depende do seu número e do de Bob. O desafio agora era estabelecer um artifício que tornasse a troca de chaves instantânea, não demorou muito e esse problema foi resolvido com a criação de um algoritmo de criptografia de chave pública. Antes de explorarmos o contexto histórico do desenvolvimento da criptografia de chave pública vamos recorrer a duas definições importantes, os conceitos de chave simétrica e assimétrica.

Chamamos de criptografia de chave simétrica o modelo de criptografia que transforma um texto simples em um texto encriptado, com o uso de um algoritmo e de uma chave privada. Na criptografia simétrica é utilizada apenas uma chave que deve ser de conhecimento do emissor da mensagem para fazer o processo de encriptação e pelo receptor da mensagem para fazer o processo de decriptação. A chave usada no processo pode ser uma palavra, uma frase, um número ou ainda uma sequência de caracteres. O tamanho das chave é medido em bits e quanto maior a chave mais segurança terá a troca de mensagens.

A criptografia assimétrica é conhecida como criptografia de chave pública e transforma um texto significativo em um texto cifrado, A criptografia de chave assimétrica é realizada com um algoritmo de criptografia, com uma chave pública que é usada para criptografar o texto e uma chave privada que é usada pelo receptor da mensagem para descriptografar o texto. Recebe o nome de criptografia de chave pública, porque a chave para criptografar é acessível a qualquer pessoa, sendo disponibilizada em modo público.

Enquanto Hellman concentrava esforços no problema da troca de chaves pela procura de funções de mão única, Diffie trabalhou em outra linha de raciocínio. Sua grande contribuição se deu na idealização de um sistema de criptografia assimétrica, até o momento Diffie tinha sido primeira pessoa a pensar em um modelo criptográfico de chave pública. Mesmo não tendo desenvolvido um sistema ou algoritmo que operasse com uma chave pública para cifrar e outra chave privada usada para decifragem, Diffie foi o autor da ideia de criptografia assimétrica.

Vamos recorrer novamente aos personagens Alice, Bob e Eva para ilustrar o conceito de chave pública.

Bob quer mandar uma mensagem para Alice, para isso ele se dirigirá a uma agência dos correios, pois todas as agências de correio tem um cadeado de Alice(chave pública) que se encontra destrancado. Bob pega uma caixa, coloca a mensagem dentro e a encaminha para Alice que é a única pessoa que tem a chave. Depois de trancada(criptografada), mesmo se Bob quisesse não conseguiria mais abrir a caixa, Eva também não conseguiria abrir a caixa, pois Alice é dona da única chave que abre o cadeado.

Figura 10 – Comunicação por criptografia de chave pública

(Figura obtida em: https://www.gta.ufrj.br/grad/04_1/tcpa/Page9.html)

Nessa ilustração o cadeado aberto seria a chave pública e a chave de Alice seria a chave privada. Apesar dos esforços de Diffie, Hellman e Merkle foram outros os cientistas que colocaram em prática a ideia de Diffie de criar um algoritmo de cifragem assimétrica. Os cientistas responsáveis pela implementação da cifra simétrica foram Ron Rivest, Leonard Adleman e Adi Shamir, pesquisadores do MIT. Rivest e Shamir eram cientistas da computação e Adleman matemático por formação.

O trabalho do trio consistiu na procura de uma função de mão única que oferecesse a possibilidade de privacidade para a chave que fosse usada no processo de descriptografar, mesmo levando em conta que a chave de criptografar fosse pública. Rivest e Shamir concentravam esforços em procurar funções que tornassem concreta a ideia da criptografia assimétrica e sempre que encontravam as possíveis candidatas a apresentavam a Adleman. Que sempre encontrava pontos falhos na segurança que cada chave(função) oferecia. As tentativas sempre eram refutadas por Adleman, até que em 1977, mais especificamente em Abril na época da Páscoa, Rivest teve um estalo e rascunhou um escrito que apresentava a função procurada. No dia seguinte Rivest levou os escritos a Adleman que desta vez não encontrou brechas na segurança que a função de mão única oferecia.

> Na manhã seguinte Rivest entregou o trabalho para Adleman, que repetiu todo o processo normal de tentar derrubá-lo, só que desta vez, não conseguiu encontrar falhas. Sua única crítica foi quanto a lista de autores. “Eu disse a Ron que tirasse meu nome do trabalho “, relembra Adleman. “Eu lhe disse que era sua invenção, não minha. Mas Ron se recusou e nós começamos uma discussão. Concordamos, afinal, que eu iria para casa e examinaria o trabalho durante uma noite, considerando o que queria fazer. Voltei no dia seguinte sugeri a Ron que eu fosse o terceiro autor. Lembro-me de pensar que esse trabalho era o menos interessante do qual já participara”. Adleman não poderia estar mais enganado. O sistema chamado de RSA(Rivest, Shamir, Adleman) em oposição a ARS, tornou-se a cifra mais importante da criptografia moderna.(SINGH, 1999, p, 299).

A criptografia de chave pública proposta por Rivest e Shamir e Adleman era centrada no problema da fatoração de números que eram resultado da multiplicação de dois números primos de grande valor e no uso de funções modulares, podemos dizer que sem os estudos de teoria dos números o conceito de cifra assimétrica jamais sairia do papel. A ideia consistia no fornecimento de uma chave pública, o número N, que era obtida por Alice através da multiplicação de dois números primos(número primo é aquele que só é divisível por 1 e por ele mesmo, um, dois, três e cinco são exemplos de números primos) p e q que devem ser mantidos em segredo. Para termos de segurança o número obtido da multiplicação deve ter 10^{100} algarismos. Bob ou qualquer outra pessoa que for enviar mensagens a Alice só vai ter conhecimento da chave pública, o resultado da multiplicação de p e q, sem ter conhecimento dos números utilizados como fatores é humanamente impossível

realizar a quebra da chave de criptografia em um tempo viável, já que a tarefa de descriptografar consiste na manipulação dos números p e q e de conhecimentos razoáveis de aritmética modular.

Foi muito importante que Rivest escolhesse funções de mão única para desenvolver o método RSA, pois mesmo que Eva tenha acesso ao número de Alice é praticamente impossível a curto prazo fazer a inversão da função e descobrir os valores de p e q por meio de N. A depender do tamanho da chave, a procura da fatoração que gera a chave utilizada na RSA, quando feita por computadores de última geração leva anos ou décadas.

Em razão da segurança oferecida, o RSA é o algoritmo usado por bancos e sites de compras. As chaves usadas em bancos, operadas pelo RSA são compostas por números da ordem de 10^{308}algarismos. Quando usada com essa quantidade de algarismos a chave é tão segura, que mesmo juntando cem milhões de microcomputadores a chave só poderia ser quebrada depois de mil anos.

Por ter chaves com uma quantidade enorme de algarismos o RSA é mais lento que os algoritmos de chave simétrica, muitas vezes ele é usado conjuntamente com algoritmos de criptografia simétrica.

A história de desenvolvimento da criptografia acompanhou e a acompanha toda a história de desenvolvimento da civilização humana. Desde os primórdios das primeiras sociedades, a criptografia se mostrou como uma ferramenta muito útil ao ser humano. Seja em comunicações simples ou até mesmo na troca de informações bancárias, segredos de estado e informações de guerra. Nesse sentido não é possível estudar o mínimo que seja de criptografia, sem fazer esse resgate histórico. Conhecer a história da criptografia é pré-requisito para compreender todos os desdobramentos que a criptografia apresenta como ramificação da ciência.

Capítulo 2 – Atividades de aplicação de conceitos de criptografia

No capítulo dois serão trabalhadas atividades que podem ser utilizadas em sala de aula nos níveis Fundamental e Médio. No desenvolvimento de cada atividade foi buscado relacionar a criptografia com tópicos de Matemática, sendo que cada atividade pode ser associada de alguma forma a criptografia simétrica(modelo de criptografia em que é usada a mesma chave para encriptação e decriptação do texto obtido) ou assimétrica(modelo de criptografia em que é usada uma chave pública para encriptação de um texto e uma chave privada para decriptação do texto cifrado). As situações apresentadas também buscam proporcionar ao leitor uma breve noção do funcionamento da criptografia em operações que envolvem o uso de computação.

2.1. Atividade 1: Usando a cifra de César na troca de mensagens do cotidiano.

Objetivo geral: Usar da criptografia como fator motivacional para o estudo de operações com números reais e de funções.
Objetivo específico: Usar de conhecimentos de operações com números reais para se calcular a chave de criptografar, estabelecer relações entre o resto da divisão de dois números e a noção de congruência e trabalhar com os alunos o conceito de cooperação.
Série/ano: A partir do 6° ano do Ensino Fundamental.

O objetivo da atividade é apresentar aos alunos de forma lúdica a criptografia, de forma mais específica o conceito de cifra simétrica. A cifra de César tem esse nome em homenagem ao imperador romano Júlio César. César usava a cifra com chave(chave é uma informação que regula a operação de um algoritmo de criptografia, na encriptação, uma chave detalha a transformação do texto original em texto criptografado, a chave tem a mesma utilidade quando transforma o texto criptografado no texto original) constituída por um deslocamento de três posições no alfabeto, ou seja no processo de cifragem a letra A era trocada pelo D, o B pelo E, o C pelo F e assim sucessivamente. O objetivo de César ao usar de criptografia, era o de se comunicar com os seus subordinados, transmitindo informações de caráter

militar, garantindo nesse sentido sigilo o que era uma vantagem em relação a seus rivais militares. A tabela abaixo ilustra o processo criado por César, a substituição de letras por meio do deslocamento de três unidades em sua posição original. Assim a letra A que é a primeira do alfabeto seria trocada pela quarta letra do alfabeto, a letra B que era a segunda seria trocada pela quinta letra do alfabeto, a letra C que era a terceira era trocada pela sexta e o processo continuava até a letra Z.

Tabela 14 – Cifra de César

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

(Tabela elaborada pelo autor do trabalho)

No contexto da atividade da Cifra de César a chave é o número de deslocamentos que se faz com as letras do alfabeto. No exemplo citado acima, a chave do processo seria o número três.

Como sugestão o professor pode pedir para que os alunos se reúnam em duplas para escrever frases simples e fazer a sua cifragem usando a tabela 10 como referência. Terminado esse procedimento o professor irá solicitar as duplas que troquem mensagens e desenvolvam estratégias para fazer a decodificação da mensagem recebida. Concluída a fase de decodificação o professor irá discutir com os alunos como usar de operações matemáticas para fazer a decodificação das frases.

Exercício 1 : De posse da Cifra de César(tabela 14), com deslocamento de três unidades, responda aos questionamentos que serão dados a seguir.

a) Escreva o nome da sua disciplina escolar favorita utilizando a cifra de César (resposta pessoal).

b) Criptografe com a Cifra de César a palavra “ESCARAVELHO”.

Solução: Com o deslocamento de unidades a palavra ESCARAVELHO deverá ser lida como “HVFDUDYHLKR”.

c) Com a Cifra de César criptografe a frase ”A ARITMÉTICA MODULAR TEM MUITA UTILIDADE EM CRIPTOGRAFIA”.

Solução: Basta fazer a correspondência das letras da frase com as letras da tabela 14, assim a resposta a questão será:

“D DULWPHWLFD PRGXOAU WHP PXLWD XWLOLGDGH HP FULSWRJUDID.”

d) Cifre pelo método de César a frase “VIM, VI E VENCI”.

Solução: Usando a tabela 14 para fazer a correspondência entre as letras teremos “YLP YL H YHQFL.”

Exercício 2: De posse da cifra de César, tendo conhecimento que a chave para criptografar é o deslocamento de 3 unidades para a direita, decodifique a frase **“YRFH H D PXOKHU PDLV OLQGD GR HJLWR”.**

Solução: Para solucionar esse exercício basta fazer uma consulta a tabela 14 e fazer as correspondências entre a letra da frase e sua codificação. Por exemplo, a letra Y decodificada equivale a letra V, a letra R equivale a letra O, a letra F equivale a letra C e assim sucessivamente. A frase do exercício quando descriptografada passa a ser **“VOCÊ E A MULHER MAIS LINDA DO EGITO”**

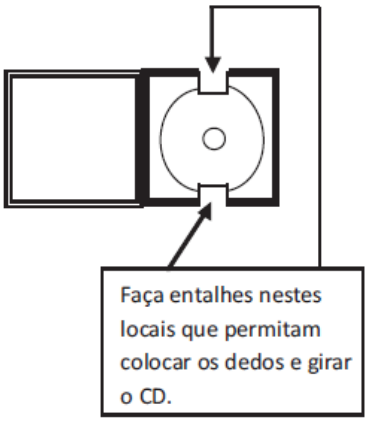
Uma sugestão alternativa de decodificação é o método de análise de frequência. O professor poderia propor aos alunos que registrassem a frequência de aparição de letras da frase e posteriormente seria feita a comparação com uma tabela como a tabela 6 desse trabalho.

Exercício 3: A terceira atividade proposta consistirá no uso de instrumentos práticos que podem criptografar dados. O professor irá propor aos alunos a construção e utilização de um disco que criptografa dados simples. Nesse sentido responda cada um dos itens propostos a seguir.

a) Construa com caixinha de cd e papel sulfite um modelo de disco de César. Para isso você vai precisar de um cd, uma caixinha de cd plástica como a da figura 10, cola ou fita adesiva e folha de sulfite.

Solução: Providencie caixinha de cd como a da figura 11.

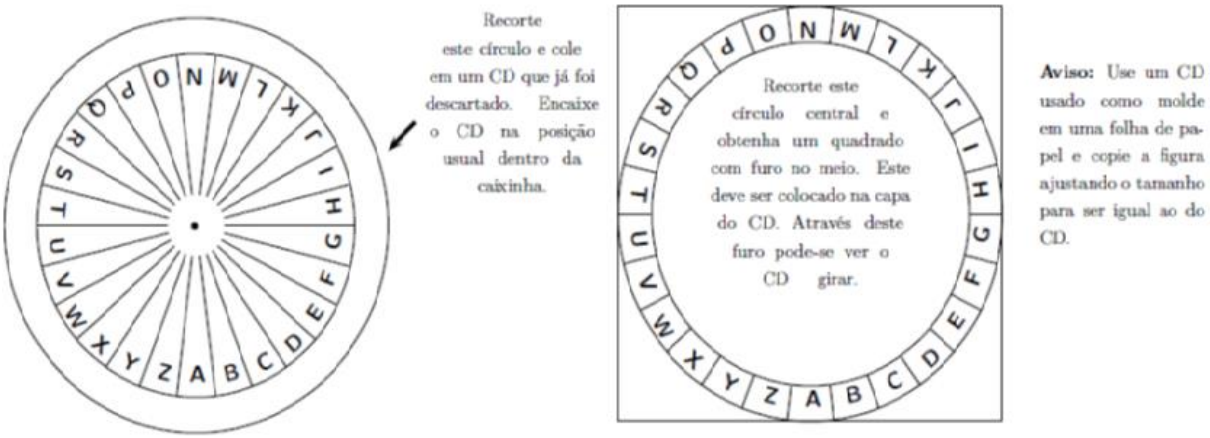
Figura 11 – Modelo de caixinha de cd



(Figura obtida em: http://www.obmep.org.br/docs/apohttp://www.obmep.org.br/docs/apostila10.pdfstila10.pdf)

Inicialmente recorte as laterais da caixinha de cd como na figura 11, imprima dois modelos de círculo como os da figura 12.

Figura 12 – Modelo de círculos para o disco de César



(Figura obtida em: http://www.obmep.org.br/docs/apohttp://www.obmep.org.br/docs/apostila10.pdfstila10.pdf)

O primeiro círculo da figura 12 deve ter sua coroa circular externa e o seu círculo central recortado, para depois serem colados no cd. O segundo círculo deve ter o círculo central que conta com a instrução recortado e colado na capa do porta cd. Depois de seco está pronto um modelo de círculo de César, o qual é ativado quando se gira o cd pelos recortes laterais do porta Cd.

b) Utilizando do disco de César e de um deslocamento do alfabeto em dez unidades, criptografe a resposta do enigma “Qual o próximo número da sequência 2 – 3 – 4 – 11 – 12 – 13 – 17 – 18 ?“

Resposta: “NOJOXYFO”

c) Utilizando do disco de César e de um deslocamento do alfabeto em dez unidades, criptografe a resposta do enigma. “Três homens, Luís, Carlos e Paulo, são casados com Lúcia, Patrícia e Maria, mas não sabemos quem é casado com quem. Eles trabalham com engenharia, Advocacia e Medicina, mas também não sabemos quem faz o quê. Com base nas dicas abaixo, quem é a esposa de Paulo?.

- O médico é casado com Maria.
- Paulo é advogado.
- Patrícia não é casada com Paulo
- Carlos não é médico.”

Resposta: “VEMSK”

Exercício 4: De posse da cifra de César e com um deslocamento de 5 unidades criptografe:

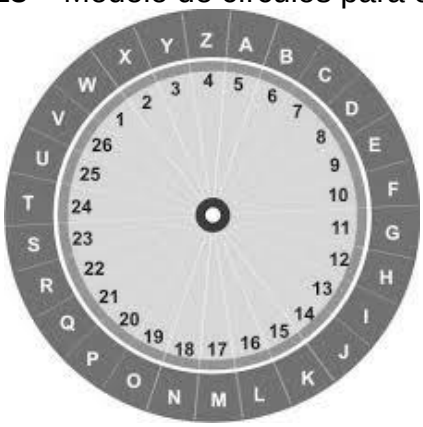
a) O nome do seu professor.

b) O nome dos seus pais.

c) O nome da sua escola.

Exercício 5: Um método alternativo ao disco de César tal como o que foi confeccionado no exercício 4 é um disco giratório no qual as letras são associadas a números. Para isso é necessário um círculo como o que será apresentado abaixo:

Figura 13 – Modelo de círculos para o disco de César



(Figura obtida em: http://www.obmep.org.br/docs/apohttp://www.obmep.org.br/docs/apostila10.pdfstila10.pdf)

A criptografia com esse disco funciona com base na associação numérica entre a letra A e o número 5(como está explícito na figura 13). Dessa forma a palavra LUA seria codificada como 16 – 25 – 5. De acordo com essas informações solucione os itens a seguir.

a) Usando a chave 5 como é proposto na figura 13 criptografe a palavra MERLIN.

Solução: Observando as associações do disco a palavra MERLIN em sua forma criptografada ficará como

17 – 9 – 22 -16 – 13 – 18.

b) Novamente usando o disco da figura 13 decodifique com a chave 5 a sequência numérica 18 – 19 -26 – 9 – 17 – 6 – 22 – 19.

Solução: Fazendo a associação dos números com as letras obtemos a palavra NOVEMBRO.

c) Criptografe a palavra RINITE com chave 15.

Solução: Fazendo o ajuste do disco e o representando como uma tabela, teremos a correspondência:

Tabela 15 - Cifra de César

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4

Q	R	S	T	U	V	W	X	Y	Z
5	6	7	8	9	10	11	12	13	14

(Tabela elaborada pelo autor do trabalho)

Trocando R por 6, I por 23, N por 2, T por 8, E por 19 a palavra RINITE ficará criptografada como 6 – 23 – 2 – 23 – 8 – 19.

d) Uma palavra de 5 letras foi codificada com chave 15, mas na hora de fazer a escrita esqueceram de colocar os traços de separação de cada número, sendo que a palavra foi escrita como 2119151815. Ordene a palavra colocando os traços de separação, em seguida faça a sua decodificação.

Solução: Como a palavra tem 5 letras e temos 10 algarismos, é fato que cada palavra é representada por dois algarismos. Então a separação dos algarismos ficará na forma 21-19-15-18-15. Fazendo a correspondência entre os números e as letras da tabela 15 chegaremos a palavra GEADA.

e) Observando a situação exposta no item d existe relevância na separação com traços dos números que são resultado do processo de criptografia? Justifique sua resposta com algumas palavras que modificam seu sentido devido a colocação dos traços.

Exercício 6: Usando a cifra de César com um deslocamento de 4 unidades decodifique a resposta dos seguintes enigmas.

a) Uma mãe tem 30 reais para dividir entre suas duas filhas, que horas são?

Resposta: "UMRDITEVEEWHYEW"

b) Roberto passou três dias em um hospital, e quando foi liberado, ele teve que ser carregado. No entanto, ele não estava nem ferido, nem doente. Na verdade, ele estava com a saúde em perfeito estado. Por que ele teve que ser carregado?

Resposta: "TSVUYIIPIIVEVIGIQREWGMS"

c) Duas pessoas chegam até um rio. O rio está cheio de piranhas que atacam qualquer ser vivo que entre na água. Lá há um barco a remos, no entanto, o barco só pode levar apenas uma pessoa. Como é que cada um pode chegar ao outro lado do rio, utilizando o barco?

Resposta: "IPIWIWXESIQQEVKIRWSTSXEWSVMS"

d) Se, durante uma corrida de carros, você deixa o segundo colocado pra trás, qual é a sua colocação após a ultrapassagem?

Resposta: "WIKYRHSPYKEV"

Embora o uso da Cifra de César seja útil a fim de desenvolver situações didáticas que tem a criptografia como pano de fundo, na prática o uso do código de César é inviável, uma vez que por ser uma cifra monoalfabética ela pode ser facilmente quebrada pelo método de análise de frequências ou por testes variando os deslocamentos do alfabeto.

2.2 Atividade 2: A arte de se comunicar por meio de números

Objetivo geral: Conhecer e fazer o uso de cifras que relacionam letras do alfabeto a números.

Objetivo específico: Explorar e reconhecer relações matemáticas bem como de números e operações e funções e congruência através do estudo de cifras que fazem correspondência entre letras do alfabeto e números.

Série/ano: A partir do 6° ano do Ensino Fundamental.

A segunda atividade vai trabalhar com cifras que fazem correspondência entre letras e números, de forma geral os exercícios a serem apresentados trarão correspondência entre letras do alfabeto e números. No transcorrer da atividade teremos exercícios que envolvem as correspondências letra x número com o conceito da Cifra de César. A intenção com essas atividades é mostrar aos alunos que as cifras podem se tornar mais difíceis de serem criptografadas quando são mais sofisticadas, quando envolvem modos de criptografar mais complexos. Do ponto de vista matemático as atividades abrem espaço para o professor aplicador relacionar os exercícios propostos a operações com números inteiros, correspondência biunívoca, ao conceito de periodicidade e a apresentação da noção de função.

Exercício 1: Fábio quer criptografar mensagens, mas prefere adotar outro método que não seja a Cifra de César. Para isso ele tem a ideia de associar letras do alfabeto a números compreendidos entre 0 e 25. A tabela 16, expressa o que ele pensou.

Tabela 16- Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

(Tabela elaborada pelo autor do trabalho)

Usando a tabela criada por Fabio criptografe as palavras.

a) BAU

Solução: Fazendo as trocas de acordo com a tabela 16, a palavra BAU ficará como “1 – 0 – 20”.

b) QUEIJO

Solução: A palavra queijo em sua forma criptografada ficará como “16 – 20 - 4 – 8 – 9 – 16”.

c) O nome do seu professor.

d) O nome de um colega da sala de aula, sendo que ao concluir o processo de criptografia entregue o nome criptografado a pessoa com o nome codificado.

Exercício 2: Usando a tabela construída por Fabio(tabela 16) decodifique as seguintes palavras.

a) 2 - 14 - 17 - 8 - 13 - 19 - 7 - 8 - 0 - 13 - 18.

Solução: Associando o número a letra correspondente e fazendo as substituições convenientes, teremos a palavra “CORINTHIANS”.

b) 13 - 0 - 21 - 8 - 14.

Solução: A sequência de números corresponde a palavra “NAVIO”.

c) 2 - 8 - 5 - 17 - 0 - 3 - 4 - 2 - 4 - 18 - 0 - 17.

Resposta: “CIFRA DE CÉSAR”.

d) 12 - 0 - 19 - 4 - 12 - 0 - 19 - 8 - 2 - 0.

Resposta: “MATEMÁTICA”.

Exercício 3: A fim de tornar sua cifra mais segura para a troca de mensagens Fabio pensa em algumas alterações em sua operação. Fábio chega a conclusão que seu método se tornará mais seguro se além da troca de letras por número também ocorra deslocamentos na linha de números, um processo similar ao que acontece na Cifra de César. Para deixar suas ideias mais claras e usando os mesmos números de 0 a 25, Fabio organizou a tabela 17, onde cada número da segunda linha da tabela 16 é acrescido de 3 unidades, resultando em:

Tabela 17 - Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Q	R	S	T	U	V	W	X	Y	Z
19	20	21	22	23	24	25	0	1	2

(Tabela elaborada pelo autor do trabalho)

Nesse sentido responda cada item:

a) Construa uma tabela que facilite o processo de decodificação da tabela a que representa um acréscimo de 3 unidades para cada letra associada a número na tabela 17.

Solução: A resposta do item consiste em construir uma tabela que sobreponha os números iniciais (0 a 25) com os números criptografados, aqueles que foram acrescidos em três unidades. Dessa forma a tabela que responde o item é:

Tabela 18 - Tabela de associação de alfabetos

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25
19	20	21	22	23	24	25	0	1	2

(Tabela elaborada pelo autor do trabalho)

Repare que a segunda linha da tabela representa os números antes de serem criptografados e a terceira linha representa os números criptografados.

b) Quando inicialmente o número que representa a letra é maior que 25 como podemos fazer para descobrir é o seu equivalente entre os números de 0 a 25? Existe relação entre o método utilizado para descobrir números equivalentes e uma breve noção do conceito de congruência da aritmética modular?

Solução: Os números maiores que 25 que inicialmente aparecem na tabela18 são 26, 27 e o 28**.** Que quando se considera a cifra inicial (tabela16) estão associados respectivamente a 23(X), 24(Y) e 25(Z). Mas que raciocínio podemos estabelecer para saber que o número 26 equivale ao 0, 27 ao 1 e 28 ao 2? É fato que a tabela apresenta 26 números, pois a regra criada por Fabio prevê a utilização de números de 0 a 25 para escrever o texto, então ao chegar em números maiores que 25 podemos recorrer a divisão desses números por 26(são 26 os números utilizados por Fabio), ou seja 26 dividido por 26 deixa resto 0, 27 dividido por 26 deixa resto 1 e 28 dividido por 26 deixa resto 2.

Em aritmética modular dois números a e b são congruentes módulo m, quando produzem o mesmo resto ao serem divididos por um natural m. A ideia aritmética de congruência se constitui quando dois números naturais a e b são divididos por um natural m. Dessa maneira usando o contexto de se usar números de 0 a 25 para trocar mensagens, podemos concluir que 27 é congruente a 1, 28 a 2 e 29 a 3, pois:

- 27 = 26.1+1 e 1 = 26.0+1, ambos 27 e 1 produzem o mesmo resto quando são divididos por 26.
- 28 = 26.1+2 e 2 = 26.0+2, ambos produzem resto 2 na divisão por 26.
- 29 = 26.1+3, ambos produzem resto 3 na divisão por 26.

Repare que a ideia desse item não é reproduzir de forma rigorosa a escrita e a definição de congruência em aritmética modular, mas apenas mostrar que de uma simples atividade de criptografia podemos discutir e apresentar breves noções sobre tópicos matemáticos mais elaborados.

c) Em um exercício de imaginação se ao criptografarmos (somar 3 unidades) usando a tabela17 forem encontrados os números 29, 35, 48 e 60 quais seriam os números entre 0 e 25 equivalentes a eles ?

Solução: Basta recorrer a ideia de se dividir os números maiores que 25 por 26. Ou seja 29 estaria associado ao 3, 35 estaria associado ao 9, 48 estaria associado ao 22 e 60 estaria associado ao 8.

d) Criptografe a palavra “ROMARIA” com um deslocamento de 3 unidades(use a tabela 17).

Solução: Para isso basta utilizar a substituição das letras da palavra pelos números que se apresentam na terceira linha da tabela 17, o R seria associado ao número 20, o O ao número 17 e assim por diante, dessa maneira a palavra ROMARIA ficaria criptografada como “20 - 17 - 15 - 3 - 20 - 11 - 3”.

e) Decodifique a palavra “3 - 20 - 11 - 22 - 15 - 7 - 22 - 11 - 5 - 3”, sabendo que ela foi criptografa com base na tabela 16 usando um deslocamento de 3 unidades.

Solução: Usando a tabela 18 como referência e fazendo as substituições corretas chegamos ao fato de que a sequência de números “3 - 20 - 11 - 22 - 15 - 7 - 22 - 11 - 5 - 3” quando decodificada representa a palavra “ARITMÉTICA”.

Exercício 4: Criptografe cada palavra usando o método da tabela 16, com as orientações de deslocamento do alfabeto que serão estabelecidas.

a) JUNDIAÍ com um deslocamento de +4 unidades nos números da tabela 16.

Solução: Na tabela 16 o J está associado ao número está associado ao número 9, após o deslocamento de 4 unidades o J passará a ser representado pelo número 13(9+4).

A letra U está associada ao número 20, fazendo o deslocamento de 4 unidades o U passa a ser o número 24.

O N se associa ao número 13, com um deslocamento de 4 unidades o N passará a ser representado pelo número 17.

O D se associa ao número 3, com o deslocamento de 4 unidades o D será associado ao número 7.

O I se associa ao número 8, com o deslocamento de 4 unidades o I passará a ser o número 12.

O A se associa ao número 0, com o deslocamento de 4 unidades o A passa a ser o número 4.

Dessa forma a palavra JUNDIAÍ depois de criptografada ficará na forma “13 - 24 -17 - 7 - 12 - 4 - 12”.

b) BELEM DO PARÁ com um deslocamento de +10 unidades nos números da tabela 16.

Solução: Somando 10 a cada número correspondente as letras de BELEM DO PARA na tabela 16, concluímos que sua forma criptografada é “11 - 14 - 21 - 14 - 22 - 13 - 24 - 25 - 10 - 27 - 10”.

c) TEOREMA DE PITÁGORAS com um deslocamento de +5 unidades nos números da tabela 16.

RESPOSTA: “24 - 9 - 19 - 22 - 9 - 17 - 5 - 8 - 9 - 20 - 13 - 24 - 11 -19 - 22 - 5 - 23”.

d) ARAME com um deslocamento de +100 unidades nos números da tabela 16.

RESPOSTA: “100 - 117 - 100 - 112 - 104”.

Exercício 5: A palavra “ (-2) - 3 - 10 - (-2) - 10 - 7 - (-4) - 15 - 0 - (-3) - 13 - (-4) - 9 - (-2) - 10 foi criptografada por meio da tabela 16 com um deslocamento de -4 unidades nos números que se encontravam associados as letras do alfabeto. Sabendo dessa informação decodifique a palavra.

Solução: Para facilitar a compreensão da resolução do exercício vamos construir uma tabela na qual estão representados o alfabeto original(segunda linha) e o alfabeto criptografado que tem um deslocamento de -4.

Tabela 19- Tabela de associação de alfabetos

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25
12	13	14	15	16	17	18	19	20	21

(Tabela elaborada pelo autor do trabalho)

Com a tabela pronta é mais fácil fazer a decodificação da sequência numérica. Logo -2 = C, 3 = H, 10 = O, 7 = L, -4 = A, 15 = T, 4 = E, -3 = B, 13 = R, 9 = N, -2 = C e 10 = O. Logo a palavra em sua forma decodificada ficará como “CHOCOLATE BRANCO”.

As cifras de substituição as quais associam letras a números apresentam segurança similar a de Cifra de César, pois ambas apresentam um sistema semelhante de operação que é a troca de letras por caracteres ordenados que nesse caso podem ser letra ou número. Vale ressaltar que no contexto desse trabalho tais cifras são importantes para estudar propriedades de números inteiros e fazer pequenas conexões com o conceito de congruência e a ideia inicial de função. Para dificultar a operação das Cifras, a próxima atividade propõe o uso de chaves mais complexas e que serão combinadas com letras que nos darão a noção do ponto de partida da cifra.

2.3. Atividade 3: Introduzindo chave numérica e letra chave em cifras

Objetivo geral: Utilizar Cifras de substituição de letra por número por meio de chave numérica.

Objetivo específico: Entender o funcionamento de cifras de substituição, compreender a necessidade de elaboração de chaves de cifragem mais elaboradas, utilizar chaves numéricas e solucionar enigmas de raciocínio lógico.

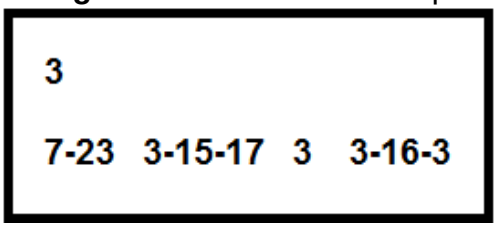
Série/ano: A partir do 6° ano do Ensino Fundamental.

A terceira atividade desse trabalho propõe o manuseio de cifras que substituem letras por números (como na atividade 2), porém com uma diferença, pois aqui são sugeridos exercícios com o uso de chaves um pouco mais complexas do que no capítulo anterior. Aqui as chaves propostas serão sequências de letras do alfabeto ou números (números compreendidos de 0 até 9) que serão combinadas com uma letra específica do alfabeto. Para facilitar o entendimento do que aqui foi falado, leia de forma mais minuciosa o exemplo que será descrito a seguir.

Na semana passada Fabio começou a usar uma cifra de substituição que associava letras a números, porém ao trocar mensagem com seus amigos Fred e Paulo alguns problemas aconteceram. Fabio deixou um bilhete que continha um segredo embaixo de sua carteira de escola com dizeres que ia repassar a Fred. Uma de suas colegas de sala Ana conseguiu interceptar um recado entre os amigos e fazer a sua decriptação. Ana realizou a decodificação, pois Fabio havia falado a ela como criptografava suas mensagens de acordo com as tabelas 16 e 17.

De posse da chave que foi usada (deslocamento de 3 unidades) Ana descobriu que o bilhete se tratava de uma declaração de amor, pois a fazer a decodificação da mensagem ela descobriu que a mensagem do bilhete de Fabio era “EU AMO A ANA”.

Figura 14 – Bilhete escrito por Fabio



(Elaborada pelo autor do trabalho)

Diante da facilidade encontrada por Ana em decifrar seu sistema de criptografia, Fabio se reuniu com seus amigos a fim de buscar uma solução e tornar a cifra de comunicação mais sofisticada e mais difícil de ser quebrada. A alternativa elaborada por Fabio consistia em ter uma chave mais complexa. Ele pensou em

uma chave como uma sequência de algarismos compreendidos entre 0 e 9, que seria inserida na tabela de criptografia com a primeira linha composta pelas letras do alfabeto e a segunda composta pelos algarismo de 0 a 25. Sendo que o primeiro algarismo da chave seria inserido embaixo de uma letra que seria, chamada de letra chave. Vamos a um exemplo da utilização desse novo modelo de cifra. Fabio quer criptografar a palavra “PARALELEPIPEDO” com a sequência chave 492, e letra chave L. Para se realizar a codificação o algarismo quatro será colocado embaixo da letra L, o nove embaixo da letra M e o dois embaixo da letra N. A partir do N a sequência numérica se iniciará do zero e se distribuirá de forma crescente. Vejamos:

Tabela 20 - Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
15	16	17	18	19	20	21	22	23	24	25	4	9	2	0	1

Q	R	S	T	U	V	W	X	Y	Z
3	5	6	7	8	10	11	12	13	14

(Tabela elaborada pelo autor do trabalho)

Repare que a partir da letra N a sequência de números se distribui normalmente, sendo que os algarismos utilizados na chave (492) são omitidos na continuação da sequência numérica. Dessa forma a palavra PARALELEPIPEDO ficará criptografada como 1- 15 - 5 - 15 - 4 - 19 - 4 - 19 - 1 - 23 - 1 - 19 - 18 - 0.

Exercício 1: Usando a nova técnica de Fabio, criptografe a palavra RIO DE JANEIRO, com chave numérica 8461 e letra chave R.

Solução: Para facilitar o nosso trabalho vamos construir uma tabela que associa letras a números, conforme as especificações de chave sugeridas.

Tabela 21 - Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Q	R	S	T	U	V	W	X	Y	Z
25	8	4	6	1	0	2	3	5	7

(Tabela elaborada pelo autor do trabalho)

Observando a correspondência entre as letras e números e fazendo as trocas das letras da palavra JANEIRO, teremos que J= 18, A= 9, N= 22, E= 13, I= 17, R= 8 E O= 23 concluímos que sua forma criptografada é “18 - 9 - 22 - 13 - 17 - 8 - 23”.

Exercício 2: Decodifique a expressão “1-9 16-1-14-14-23 7-1 25-1-2-11 13-17-1-9 16-1-9 17-9 11-6-0-11 1 14-1-3”, sabendo que ela foi codificada com a chave numérica 7771820 e letra chave D.

Solução: De início vamos construir uma tabela de correspondência entre as letras do alfabeto e os números já criptografados pelas chaves. Uma observação a se fazer é que o número 7, que é repetido três vezes na escrita da chave numérica vai ser inserido apenas uma vez na tabela. Isso se justifica pelo fato do número 7 não poder estar associado a três letras diferentes já que isso tornaria a criptografia da frase impossível. Dito isso vamos a construção da tabela de encriptação das letras.

Tabela 22 - Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
23	24	25	7	1	8	2	0	3	4	5	6	9	10	11	12

Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22

(Tabela elaborada pelo autor do trabalho)

Observando a tabela 22 temo que 1 =E, 9 =M, 16=T, 14=R, 23=A, 7=D, 25=C, 2=G, 11=O, 13=Q, 17=U, 6=L, 0=H, 3=I. ou seja, quando decodificamos 1-9 16-1-14-14-23 7-1 25-1-2-11 13-17-1-9 16-1-9 17-9 11-6-0-11 1 14-1-3”, obtemos a frase “EM TERRA DE CEGO QUEM TEM UM OLHO É REI”.

Exercício 3: Decodifique a resposta do ENIGMA “Três pessoas vão pescar: 2 pais e 2 filhos. Como isso é possível?-Resposta: “0-19 20-18-2-19 16-2-19-19-15-0-19 19-0-15 16-0-6 1-6-12-4-15 2 0-22-15”, sabendo que ela foi criptografada com chave numérica 907875252 com letra chave Z.

Solução: Vamos construir a tabela de encriptação dos dados obedecendo as regras da chave numérica e da letra chave. Fazendo as substituições adequadas obtemos:

Tabela 23 - Correspondência entre letras do alfabeto e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	7	8	5	2	1	3	4	6	10	11	12	13	14	15	16

Q	R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25	9

(Tabela elaborada pelo autor do trabalho)

Fazendo as trocas de número por letras obtemos que a resposta do Enigma é “AS TRÊS PESSOAS SÃO PAI FILHO E AVO”.

Exercício 4: A resposta do enigma “Em 1990 Rute tinha 40 anos, mas em 1995, tinha 35. De que forma isso pode acontecer? Resposta: 9-7-23 10-23-15-25-9-17 23-10-16-9-15 1-9 25-14-2-15-16-11 “ foi criptografada com a chave numérica 1990401995 com letra chave D. Decodifique a resposta do enigma.

Exercício 5: A resposta do Enigma “Duas pessoas se aproximam da margem de um rio. Na margem há apenas um barco que só carrega uma pessoa de cada vez. As duas pessoas atravessaram o rio. Como conseguiram isso?” é “14-21-10-9 14-9-4-10-24 14-22 22-10-3-16-14-23-9 24-25-24-9-4-10-9”
Resolva o enigma, sabendo que ele foi criptografado com chave numérica 839461 e letra chave Q.

2.4 Atividade 4: Quebrando cifras por meio de análise de frequência

Objetivo geral: Usar de ferramentas da Matemática para quebrar cifras de substituição.
Objetivo específico: Usar de análise estatística para decodificar textos cifrados..
Série/ano: A partir do 6° ano do Ensino Fundamental.

A última ideia de Fabio de usar duas chaves para se comunicar foi um sucesso, até que Ana novamente desvendasse o seu segredo. Fabio havia transmitido por mensagem a seus amigos que levaria hambúrgueres na aula do dia seguinte e que ia entregar um para cada um de seus amigos. Porém mais uma vez

Fabio não foi cuidadoso e deixou o bilhete com a mensagem criptografada na mesa do refeitório da escola. No dia seguinte quando Fabio se encaminhava para trás do pátio da escola, ele foi surpreendido por Ana, que pediu a ele um dos hambúrgueres. Sem entender o que havia ocorrido Fabio perguntou do que Ana estava falando, Ana por sua vez mostrou a Fabio o bilhete e explicou a ele que usou de análise de frequências para descobrir o recado do bilhete. Ana explicou a Fabio que analisou a frequência de aparição de cada letra, comparou com uma tabela de frequência de aparição das letras no alfabeto brasileiro e que por meio de alguns ajustes conseguiu deduzir o recado do bilhete.

Mas de uma forma mais detalhada no que consiste a análise de frequências? A análise de frequências consiste em um método de quebra de criptografia por meio do uso de ferramentas básicas de estatística, como confecção de tabelas e registro de frequência de elementos. Nesse método é registrada a frequência de aparição de cada letra em uma tabela simples, sendo o passo final a comparação da frequência de aparição das letras com uma tabela padronizada. Alguns ajustes de encaixe de letras (tentativas de substituição) são feitos, partindo sempre da substituição das letras com aparição maior, também são observados os encaixes de letras que aparecem sozinhas no texto (vogais) e repetindo o processo de ajuste das letras chegamos ao texto decodificado. Para a melhor ilustração do método de análise de frequências você pode ler o exemplo apresentado nas páginas 24 e 25 desse trabalho ou se ater a resolução dos exercícios que serão apresentados abaixo.

Exercício 1 - Construa uma tabela de frequência para registrar as letras que aparecem no texto a seguir. Depois responda os itens a, b e c.

"O que nós estamos querendo ressaltar é que o crescimento está lento quando você olha no agregado, quando você separa privado e público, o privado já mostra sinal de dinamismo, essa é a história que nós estamos contando, disse Sachsida"(Obtido em https:// economia.uol.com.br/noticias/reuters/2019/11/07/governo-eleva-projecoes-para-crescimento-do-pib-em-2019-a-09-e-232-em-2020.htm)

Solução: A tabela abaixo representa a frequência de aparição de cada letra no texto

Tabela 24 - Frequência de aparição de letras do alfabeto

A	B	C	D	E	G
$\frac{24}{195} = 12{,}3\%$	$\frac{1}{195} = 0{,}51\%$	$\frac{7}{195} = 2{,}55\%$	$\frac{10}{195} = 4{,}08\%$	$\frac{22}{195} = 11{,}2\%$	$\frac{2}{195} = 1{,}02\%$
H	I	L	M	N	O
$\frac{3}{195} = 1{,}5\%$	$\frac{11}{195} = 5{,}64\%$	$\frac{5}{195} = 2{,}56\%$	$\frac{6}{195} = 3{,}07\%$	$\frac{12}{195} = 6{,}15\%$	$\frac{25}{195} = 12{,}82\%$
P	Q	R	S	T	U
$\frac{4}{195} = 2{,}04\%$	$\frac{6}{195} = 3{,}06\%$	$\frac{10}{195} = 4{,}08\%$	$\frac{21}{195} = 10{,}76\%$	$\frac{8}{195} = 4{,}10\%$	$\frac{7}{195} = 3{,}58\%$
V					
$\frac{4}{195} = 2{,}04\%$					

(Tabela elaborada pelo autor do trabalho)

a) Qual o tipo de letra mais frequente no texto vogal ou consoante? Das vogais qual a de maior e a de menor frequência?

Solução: De acordo com os dados da tabela as vogais tem frequência de aparição maior que as consoantes. A vogal de maior frequência é o A e a de menor frequência é o U.

b) A soma da frequência das vogais é maior ou menor que a soma das frequências das consoantes?

Solução: A frequência acumulada das vogais representa 45,54% das letras do texto, enquanto as consoantes acumulam frequência de 54,46%. Considerando que em nosso alfabeto o número de consoantes é maior, podemos afirmar que proporcionalmente usamos mais vogais do que consoantes para escrever um texto. Pois 5 vogais representam quase a mesma frequência acumulada do que 21 consoantes.

c) Em sua opinião por que as letras K, W e Y tem frequência de aparição zero?

Solução: Uma resposta esperada é que tais letras tem origem em alfabetos de língua estrangeira.

d) Com um texto de 195 caracteres é possível construir algumas hipóteses sobre a frequência de aparição das letras do alfabeto português em um texto qualquer? Quais são as limitações para se generalizar em sua opinião?

Solução: A princípio podemos observar e fortalecer a ideia de que em um texto as vogais A, E e O tem mais frequência do que as consoantes. Porém o texto tem 195 letras e com um número de letras reduzido não é possível extrair outras conclusões a respeito da frequência de aparição das letras.

Exercício 2 - Em relação ao texto a seguir: “Corais, tartarugas, aves, peixes, ostras, mariscos. Não são poucos os grupos de animais na lista de mortos pelo óleo encontrado nas praias do Nordeste, mas pode haver ainda mais. Ainda não é possível saber a real extensão da devastação, que hoje completa dois meses. Vários ecossistemas da região foram afetados. Todos os ambientes costeiros foram afetados em diferentes intensidades, dependendo do tamanho da mancha que os atingiu, densidade no momento em que encostou, estágio da maré e hora do dia. Isso porque o calor ajuda a amolecer a mancha e, durante a noite, é mais difícil o trabalho de remoção, explica a oceanógrafa Mônica Costa, da Universidade Federal do Pernambuco. Para ela, o número de animais atingidos tem aumentado. "Inicialmente havia poucos registros de encalhes vivos e mortos. Mas isso vem crescendo significativamente agora. Devem estar ocorrendo em toda parte. Mas nós não temos registro e acesso à informação. Ainda", afirma. Costa diz que há relatos de pesquisadores de que uma parte do óleo está se enterrando na areia. A mancha já pode ser detectada a alguns centímetros da superfície da areia. Isso era esperado, pois é o comportamento que foi registrado em outros eventos que atingiram praias, diz. "Isso é extremamente preocupante, pois demonstra que esse óleo deverá permanecer na praia por algumas décadas, subindo e descendo no pacote sedimentar, mas com um movimento líquido para baixo.” Obtido em https://noticias.uol.com.br/reportagens-especiais/devastacao-pelo-oleo-no-nordeste/index.htm#tematico-1

Determine:

a) A tabela de frequência que relaciona a porcentagem de aparição das letras do texto com o total de letras.

Solução:

Tabela 25 - Frequência de aparição de letras do alfabeto

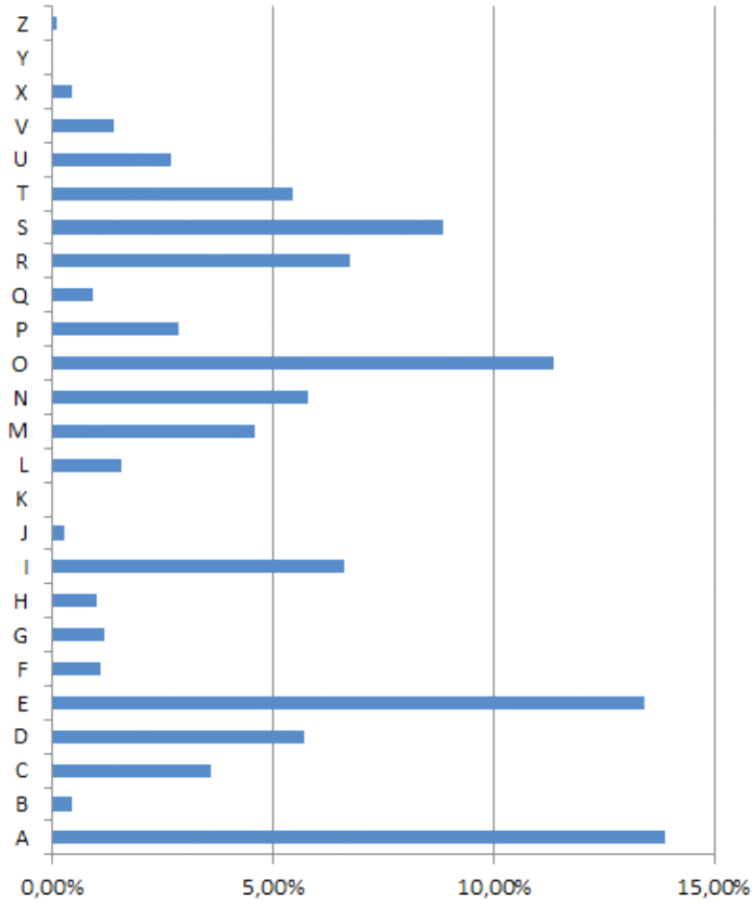
A	B	C	D	E	F
$\frac{151}{1086} = 13{,}9\%$	$\frac{5}{1086} = 0{,}46\%$	$\frac{39}{1086} = 3{,}59\%$	$\frac{62}{1086} = 5{,}7\%$	$\frac{146}{1086} = 13{,}4\%$	$\frac{12}{1086} = 1{,}1\%$
G	H	I	J	K	L
$\frac{13}{1086} = 1{,}19\%$	$\frac{11}{1086} = 1{,}01\%$	$\frac{72}{1086} = 6{,}62\%$	$\frac{3}{1086} = 0{,}27\%$	0	$\frac{17}{1086} = 1{,}56\%$
M	N	O	P	Q	R
$\frac{50}{1086} = 4{,}60\%$	$\frac{63}{1086} = 5{,}8\%$	$\frac{123}{1086} = 11{,}32\%$	$\frac{31}{1086} = 2{,}85\%$	$\frac{10}{1086} = 0{,}92\%$	$\frac{73}{1086} = 6{,}72\%$

S	T	U	V	W	X
$\frac{96}{1086} = 8{,}83\%$	$\frac{59}{1086} = 5{,}43\%$	$\frac{29}{1086} = 2{,}67\%$	$\frac{15}{1086} = 1{,}38\%$	0	$\frac{5}{1086} = 0{,}46\%$
Y	Z				
0	$\frac{1}{1086} = 0{,}09\%$				

(Tabela elaborada pelo autor do trabalho)

b) Construa um gráfico de barras que registre a frequência de aparição das letras no texto.

Figura 15 – Gráfico de frequência das letras do texto



(Imagem criada pelo autor do trabalho)

c) Qual a vogal mais frequente no texto? E a menos frequente?

Solução: A vogal de maior frequência é o A e a de menor frequência é o U.

d) Entre as tabelas 22 e 23 existe diferença entre as porcentagens de frequência do grupo de vogal? Se existo exiba uma possível justificativa pra esse fato.

Solução: Entre as tabelas existe uma diferença quanto a ordem de aparição das vogais. Na tabela 22 a letra o aparece com a segunda maior frequência, ficando

atrás apenas da letra A. Já na tabela 22 a segunda vogal mais citada é a letra E, perdendo apenas para a letra A. Na tabela 22 a letra o deixa de ser a segunda mais citada, passando a ocupar o lugar de terceira letra mais citada do texto. Uma possível explicação para esse fato é que o segundo texto apresenta mais letras, portanto estará mais próximo da estatística real da frequência de aparição das letras do nosso alfabeto.

Exercício 3 - Por meio da análise de frequência decodifique o seguinte texto:
“F FSYF J T RFNTW RFRNKJWT YJWWJXYWJ SFYNAT IT GWFXNQ J UJWYJSHJ F RJXRF TWIJR IJ HFAFQTX FXSTX EJGWFX J WNSTHJWTSYJX FUJXFW IJ XJZ STRJ XJW ZXFIT HTRT FIOJYNAT SJLFYNAT RZNYFX HZWNTXNIFIJX XTGWJ F JXUJHNJ STX FUWTCNRFR IF NIJNF IJ FSYF HTRT ZR JQTLNT”.

Solução: Em um primeiro momento vamos construir a tabela de análise de frequência de aparição das letras. O texto tem 200 letras, distribuídas na forma de razão entre a frequência da letra e o total de letras do texto.

Tabela 26 - Frequência de aparição das letras do texto

A	B	C	D	E	F
$\frac{4}{200} = 4\%$	0	$\frac{1}{200} = 0{,}5\%$	0	$\frac{2}{200} = 1\%$	$\frac{27}{200} = 13{,}5\%$
G	H	I	J	K	L
$\frac{1}{200} = 0{,}5\%$	$\frac{7}{200} = 3{,}5\%$	$\frac{11}{200} = 5{,}5\%$	$\frac{30}{200} = 15\%$	$\frac{1}{200} = 0{,}5\%$	$\frac{2}{200} = 1\%$
M	N	O	P	Q	R
0	$\frac{14}{200} = 7\%$	$\frac{1}{200} = 0{,}5\%$	0	$\frac{2}{200} = 1\%$	$\frac{13}{200} = 6{,}5\%$
S	T	U	V	W	X
$\frac{10}{200} = 5\%$	$\frac{24}{200} = 12\%$	$\frac{4}{200} = 2\%$	0	$\frac{15}{200} = 7{,}5\%$	$\frac{1}{200} = 0{,}5\%$
Y	Z				
$\frac{10}{200} = 5\%$	$\frac{5}{200} = 1\%$				

(Tabela elaborada pelo autor do trabalho)

O próximo passo é termos um parâmetro comparativo entre as frequências obtidas em nosso texto criptografado com as frequências da tabela 25. Para isso vamos utilizar o gráfico de barras (figura 15) para comparar as frequências de aparição de cada letra.

Figura 16 – Gráfico comparativo de frequências

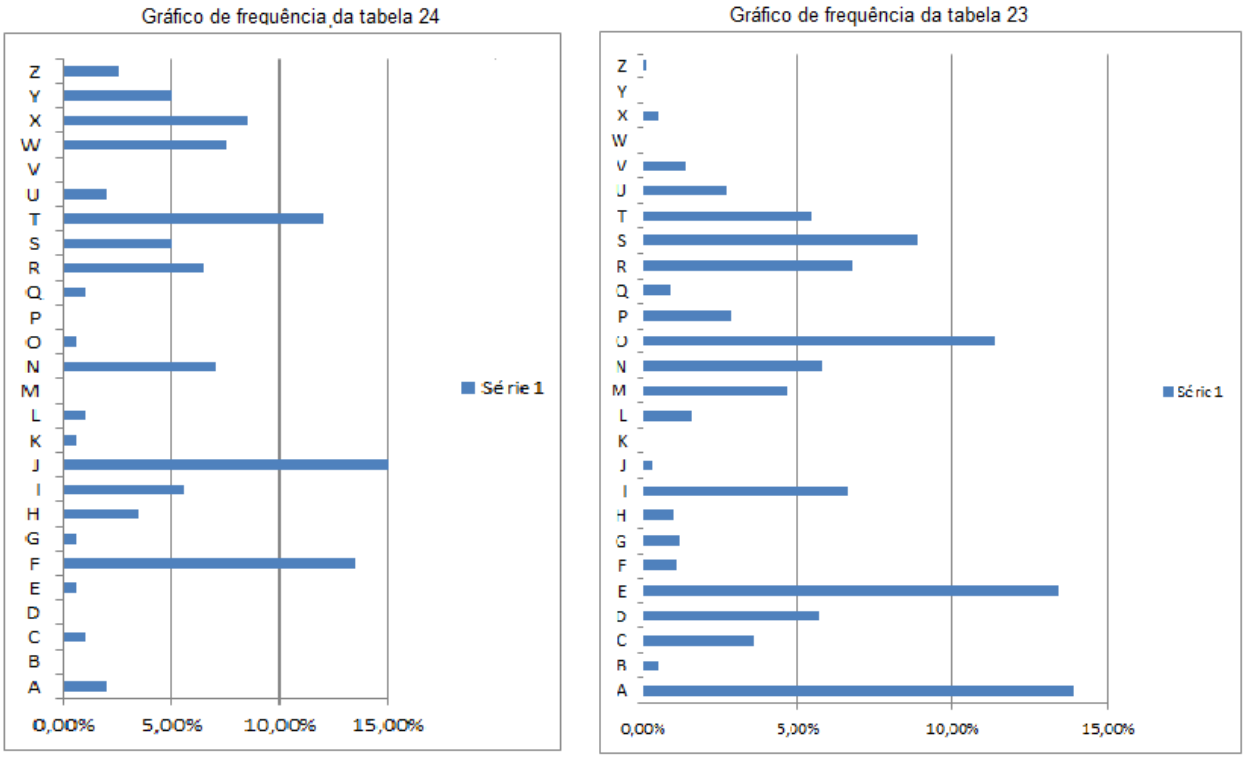


Imagem criada pelo autor do trabalho

As letras mais frequentes na tabela 25 são as letras A, E, O, S, R, I, N, T e M.

Por outro lado a tabela 26 que é a do texto criptografado apresenta como letras mais frequentes as letras J, F, T, X, W, N, R, I e S. A um primeiro momento poderíamos associar o A ao J, E ao F, O ao T, S ao X, R ao W, I ao N, N ao R, T ao I e M ao S. Antes de fazer a substituição das letras devemos fazer algumas observações quanto a escrita do texto. A primeira observação é que o texto se inicia por uma letra isolada, a letra F. Na língua portuguesa as letras isoladas que iniciam textos são A e O. No nosso texto o F é a segunda letra com mais aparições, logo provavelmente a letra F seria a letra A, pois O é a terceira letra em ordem de frequência. Nossa sequência de substituição ficará como F=A, J=E, T=O, X=S, W=R, N=I, R=N, I=T, S=M. Fazendo essa substituição no texto teremos:

“A AMYA E O NAIOR NANIKERO YERRESYRE MAYIAO TO GRASIQ E UERYEMHE A NESNA ORTEN TE HAAAQOS ASMOS EEGRAS E RIMOHEROMYES AUESAR TE SEZ MONE SER ZSATO HONO ATOEYIAO

MELAYIAO NZIYAS HZRIOSITATES SOGRE A ESUEHIE MOS AUROCINAN TA ITEIA TE AMYA HONO ZN EQOLIO”.

Após a primeira substituição as palavras começam a ter sentido e é possível perceber que no texto parcialmente decodificado que a letra N representa o M(NAIOR) e de forma recíproca o M representa o N(ASMO). A letra Y representa o T(YERRESYRE), T representa o D(ORTEN), U representa o P(AUESAR), G representa o B(SOGRE). Novamente vamos fazer as substituições de N por M e M por N e também das letras pretas do texto anterior pelos seus respectivos que foram deduzidos nesse parágrafo. Agora o texto assumirá a forma:

“A ANTA E O MAIOR MAMIKERO TERRESTRE NATIAO DO BRASIQ E PERTENHE A MESMA ORDEM DE HAAAQOS ASNOS EEBRAS E RINOHERONTES APESAR DE SEZ NOME SER ZSADO HOMO ADOETIAO NELATIAO MZITAS HZRIOSIDADES SOBRE A ESPEHIE NOS APROCIMAM DA IDEIA DE ANTA HOMO ZM EQOLIO”.

Nessa última passagem fica mais claro que K=F(MAMIKERO) A=V(NATIAO), Q=L(BRASIQ), H=C(PERTENHE), E=Z(EEBRAS), Z=U(ZSADO), O=J(ADOETIVO), L=G(NELATIVO), C=X(APROCIMAM). Dessa forma pelo método da análise de frequência conseguimos dar significado a um texto que passou pelo processo de cifragem, onde o texto decodificado é:

“A ANTA É O MAIOR MAMÍFERO TERRESTRE NATIVO DO BRASIL E PERTENCE A MESMA ORDEM DE CAVALOS, ASNOS ZEBRAS E RINOCERONTES. APESAR DE SEU NOME SER USADO COMO ADJETIVO NEGATIVO MUITAS CURIOSIDADES SOBRE A ESPECIE NOS APROXIMAM DA IDEIA DE ANTA COMO UM ELOGIO”.

Repare que para decifrar o fragmento de texto não foi necessário conhecer qual o método de cifragem utilizado e muito menos a chave utilizada no processo. O método de análise de frequência se mostrou útil para desvendar o que estava escrito no texto, tudo isso graças a comparação das frequências das letras do texto com a tabela de frequência da tabela 25.

2.5. Atividade 5 – O uso de mapas na troca de mensagens como forma de criptografia assimétrica

Objetivo geral: Usar de mapas de circuito para o entendimento de criptografia de chave privada

Objetivo específico: Estabelecer entendimento do processo de criptografia de chave privada, usar raciocínio lógico na resolução de problemas e trabalhar com os alunos o conceito de cooperação.

Série/ano: A partir do 6° ano do Ensino Fundamental.

A atividade dos mapas tem como objetivo proporcionar ao leitor uma breve noção do que é a criptografia assimétrica. Na atividade os mapas serão como chaves e os números a unidade de informação que se deseja transmitir. A atividade apresenta o conceito de criptografia assimétrica na troca de mensagens. A fim de comparação vamos retomar os conceitos de cifragem simétrica e de cifragem assimétrica, que já foram explicados no primeiro capítulo desse trabalho.

Criptografia simétrica é o processo em que o emissor e o destinatário da mensagem usam a mesma chave para criptografar e decodificar dados, pelo fato das chaves usadas nas duas partes serem as mesmas essa criptografia recebe o nome de criptografia simétrica. A figura abaixo ilustra o funcionamento de um algoritmo de criptografia simétrica.

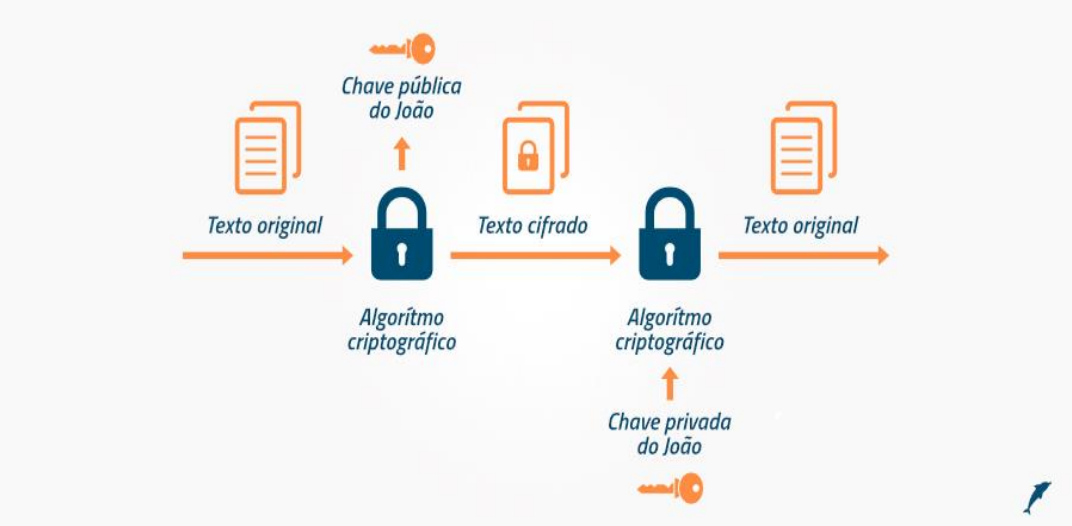
Figura 17 - Esquema ilustrativo criptografia simétrica

(Obtida em: https://www.evaltec.com.br/criptografia-de-dados-e-gerenciamento-de-chaves/)

Nesse processo para se realizar a criptografia é necessário apenas uma chave e o algoritmo de cifragem. Uma vantagem da criptografia simétrica é que ela é de rápida execução devido a baixa complexidade dos seus algoritmos quando comparados aos algoritmos de criptografia assimétrica. Caso ocorra da chave ser desvendada basta fazer a sua troca por outra, sem a necessidade de troca do algoritmo usado. As desvantagens da criptografia simétrica residem no fato de que quanto mais pessoas tem acesso a chave, mais difícil se torna fazer a sua distribuição de forma segura. Desse fato temos o problema da distribuição de chaves que já foi descrito de forma mais detalhada nas páginas 45 e 46 dessa dissertação. Outra desvantagem de um sistema simétrico é que não é possível identificar quem envia ou recebe o conteúdo de uma conversa.

Criptografia assimétrica é o tipo de criptografia que usa uma chave para criptografar (chave pública) e outra para decodificar informações (chave privada). Como as chaves usadas no processo de comunicação são distintas temos a ideia de assimetria, portanto daí a justificativa pra esse tipo de criptografia ser chamada de assimétrica. Nesse modelo o emissário precisa conhecer apenas a chave pública, pois ela que é usada pra cifrar os dados. A chave privada é de posse do receptor das mensagens, garantindo assim maior segurança na conversa. A ilustração abaixo apresenta a forma como se realiza uma comunicação por criptografia assimétrica.

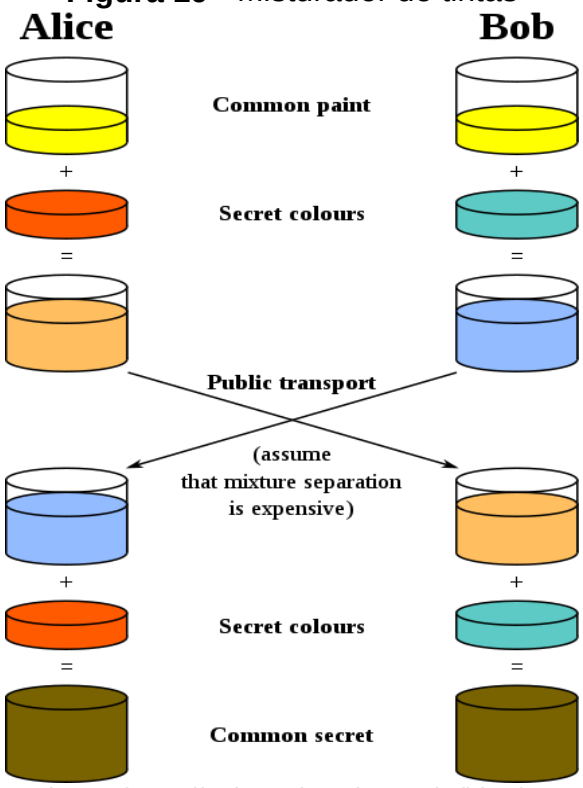
Figura 18 – Algoritmo de chave assimétrica



(Figura obtida em: https://www.evaltec.com.br/criptografia-de-dados-e-gerenciamento-de-chaves/)

A desvantagem da cifra assimétrica é que seus algoritmos são mais complexos, em razão disso são de execução bem mais lenta que os algoritmos de criptografia simétrica. Em situações do dia a dia como compras por lojas virtuais e em transações bancárias não usamos a criptografia simétrica devido ao fato de que seria necessário dispor de uma quantidade muito grande de chaves a serem distribuídas entre clientes dispostos a usar esses serviços. E também pelo fato de que se o hacker tem acesso a chave usada no processo e a mensagem basta utilizar a chave para decifrar o conteúdo da mensagem. Nesse sentido é bem mais seguro e prático fazer o uso de criptografia assimétrica, pois por mais que um invasor tenha acesso a chave usada para criptografar (chave pública) e a mensagem trocada, o processo de decodificação só poder ser feito pelo proprietário da chave privada. Essa impossibilidade de decifrar o texto dado a mensagem cifrada como ocorre na criptografia assimétrica nos remete as funções de mão única, aquelas que são fáceis de fazer (criptografar por chave pública), mas muito difícil de desfazer, pois nesse caso um invasor não teria acesso a chave privada. Um exemplo de situação que pode ser correlacionada a noção de função de mão única é quando fazemos o processo de mistura de tintas

Figura 19 - Misturador de tintas



(Figura obtida em: https: https://enigma.ic.unicamp.br/blog/2018s2/asymmetric-encryption/)

Nesse exemplo as informações a serem criptografadas são as cores secretas de Alice e Bob (laranja e azul). Repare que se o invasor tem acesso ao último pote que é o de cor marrom, dificilmente ele saberá quais foram as cores iniciais usadas por Alice e Bob. O misturador de tintas é um exemplo clássico de função de mão única. As funções de mão única são importantes na implementação dos algoritmos de chave assimétrica, pensando na atividade que será realizada os mapas a serem utilizados nessa atividade constituem um exemplo de função de mão única.

Vamos usar um exemplo para poder ilustrar de melhor forma o conceito de criptografia assimétrica. Imagine que Maria quer mandar uma mensagem a João e imagine também que João deixou seus cadeados abertos na agência de correios da cidade. Se Maria quer mandar uma mensagem de forma segura a João, ela deve pegar sua mensagem, colocar na caixa e trancar com o cadeado de João. A menos que outra pessoa tenha a chave do cadeado, esse método é seguro pra se comunicar por meio de um canal onde haja terceiros interessados na interceptação da mensagem. A atividade proposta traz elementos do processo de cifragem assimétrica. A criptografia quando usada na forma assimétrica tem uma chave pública que é usada para o envio da mensagem, onde qualquer pessoa tem acesso a essa informação e uma chave privada, que só o receptor da mensagem tem conhecimento para decodificar e ter o entendimento do que lhe é transmitido.

Diante de tudo que foi exposto até aqui o professor pode propor aos alunos situações didáticas que recorram ao uso de criptografia de chave simétrica. Aqui nesse espaço serão apresentadas algumas sugestões. Vamos iniciar o desenvolvimento das atividades com a história fictícia do professor Jean.

“Na semana passada o professor Jean que dá aulas no 8° ano do Ensino Fundamental da escola Raio de Luz, tentou deixar as aulas de Raciocínio Lógico um pouco mais atrativas. Para isso ele propôs atividades e situações-problema que fizessem o uso de criptografia, seja ela apresentada na sua forma simétrica ou assimétrica.

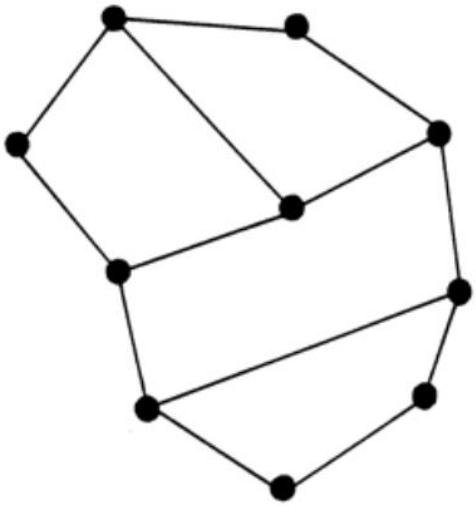
Na aula da última semana ele propôs a seus alunos que utilizassem a Cifra de César para criptografar mensagens. A primeira atividade proposta pelo professor pedia aos alunos que utilizassem da Cifra de César com um deslocamento de sete

unidades para redigir mensagens de otimismo aos seus melhores amigos da sala. O professor explicou que nesse caso a chave de cifragem era o deslocamento do alfabeto que conhecemos em sete unidades para a direita. Como a chave para cifrar e decifrar era a mesma, essa primeira atividade se constituiu de cifragem simétrica. Ao fim da aula como desafio o professor propôs que durante a semana os alunos trocassem segredos entre si utilizando a Cifra de César. A ideia do professor de utilizar cifras foi um sucesso e os alunos se familiarizaram com o novo jeito de se comunicar, eles compreenderam a ideia de que às vezes é necessário se comunicar de forma secreta para preservar o sigilo de algumas informações. Porém na quarta-feira, dia da aula de Jean surgiu um imprevisto. Maria que era sua aluna decidiu escrever um bilhete se declarando a João, seu amigo de sala usando a Cifra de César com um deslocamento de sete unidades. Maria escreveu o bilhete e na hora do recreio o deixou embaixo da carteira de João. Analice que era uma amiga em comum de João e Maria num surto de curiosidade abriu o bilhete e por ter conhecimento da Cifra de César e da chave utilizada descobriu que Maria tinha uma paixão secreta por João. A situação de intercepção do bilhete foi levada ao professor Jean que explicou a Analice que não era correto violar correspondências alheias e que em muitas situações isso é considerado crime. Jean se aproveitou da situação e fez uma correlação da violação do conteúdo do bilhete com a fragilidade de uso das cifras simétricas. Jean explicou aos alunos que a criptografia simétrica apresenta limitações e que assim como ocorreu na sala de aula, a segurança do processo diminui conforme um número grande de pessoas tem acesso a uma mesma chave de criptografar. O professor abriu um parêntese e disse que devido a essa fragilidade de segurança do sistema simétrico, o mesmo não era utilizado em transações comerciais e bancárias.

Após esses esclarecimentos o professor apresentou aos alunos uma alternativa as cifras simétricas, para isso ele definiu com os alunos o que é uma cifra assimétrica e também o que eram funções de mão única. Aproveitando esse momento o professor elaborou uma proposta de atividade que consistia na transmissão de números através de mapas constituídos por ligação de pontos do plano. Através do Datashow o professor projetou na lousa o mapa da figura 18. Na proposta pedagógica de Jean os alunos iriam o usar o mapa da figura 18 (chave

pública) para lhe enviar um número. Jean explicou que existiam algumas regras para enviar o número pensado. A primeira regra na verdade era mais uma convenção, os alunos deveriam enviar inicialmente apenas números inteiros ao professor. Depois da escolha do número os alunos deveriam fazer a sua decomposição em forma de soma, o número de parcelas deveria ser igual ao número de nós do mapa.

Figura 20 - Mapa público usado por Maria

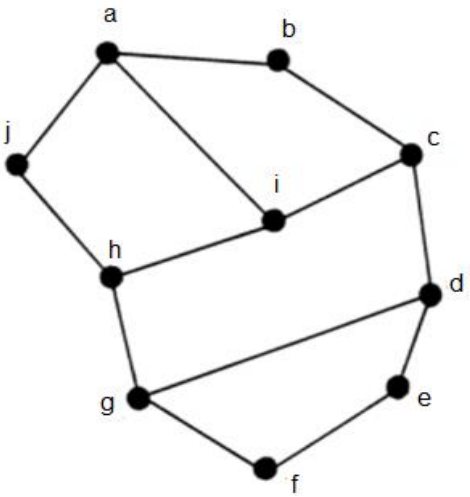


(obtido em https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf)

Vamos supor que um aluno escolha o número N. O mapa da figura 20 tem 10 nós, nesse caso N deve ser decomposto em dez parcelas. Então N será decomposto na forma $N = a + b + c + d + e + f + g + h + i + j$.

A configuração do mapa após a inserção das parcelas de N será:

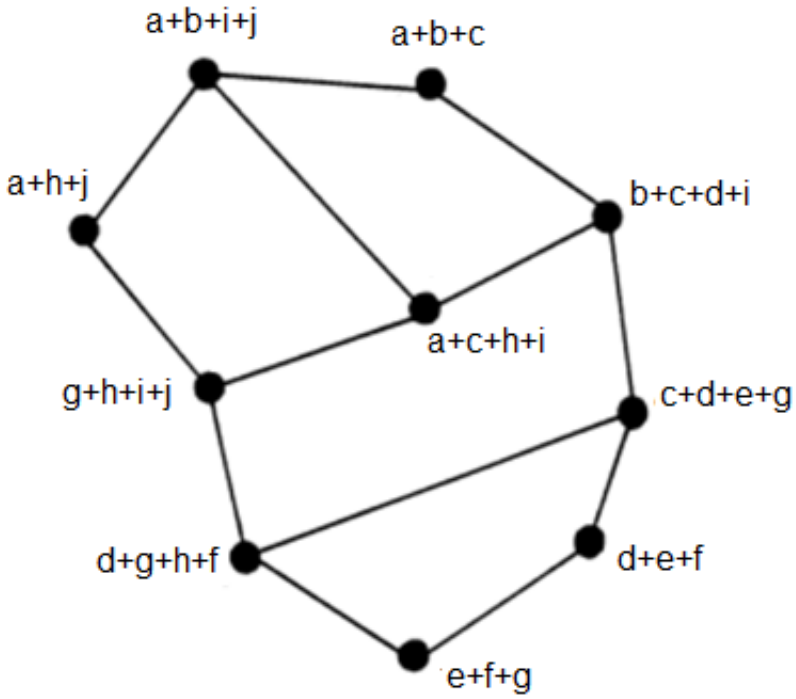
Figura 21- Mapa público com nós preenchidos



(editado pelo autor do trabalho)

O último passo é colocar em cada vértice do mapa a soma dos números que se encontram conectados a ele para enfim o mapa ser enviado ao professor. Por exemplo, o vértice A se conecta ao vértice B, J e I, portanto o mapa a ser enviado ao professor deve ter sobre o vértice a soma (a+b+i+j). O vértice F se encontra ligado aos vértices G e E, logo sobre o vértice F deveremos colocar a soma (e+f+g). Esse processo deve ser repetido até se esgotarem todos os vértices do mapa. Ao fim do processo o mapa a ser enviado ao professor será:

Figura 22- Mapa público



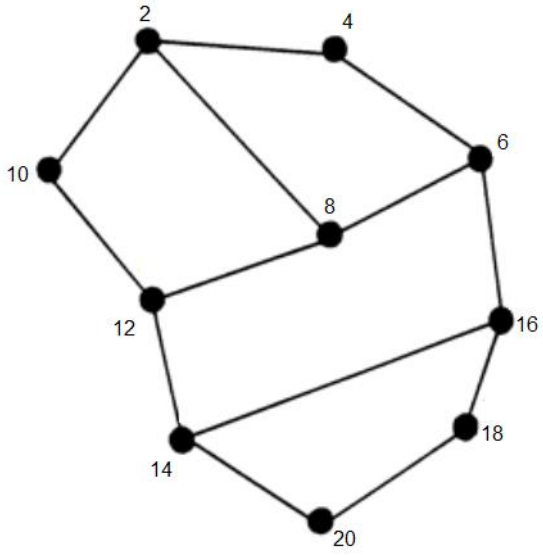
(Figura 22 - Mapa público editado pelo autor do trabalho)

Vamos fazer agora um exemplo numérico, para que as instruções sejam assimiladas mais facilmente.

Para um entendimento mais didático da situação que será apresentada vamos recorrer novamente aos alunos João e Maria.

Maria deseja enviar a João o número 110. Os números escolhidos por Maria na decomposição de 110 são os apresentados no mapa abaixo:

Figura 23- Mapa público usado para enviar o número 110

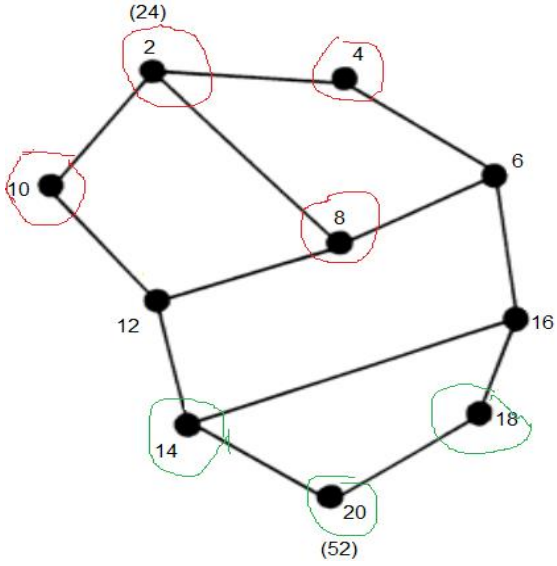


(editado pelo autor do trabalho)

Após a inserção dos números em cada nó, Maria deve registrar entre parênteses a soma dos números que se ramificam e se encontram em cada nó, incluindo o número que se encontra sobre o nó. Considerando os ramos que se encontram no ramo com número 2, a soma a ser realizada será a dos números circulados de vermelho que seria (2+10+4+8 = 24).

Considerando os ramos do mapa que convergem ao nó de número 20, temos a soma dos números circulados de verde que é (14+20+18 = 52). Esse processo é repetido para todos os nós do mapa e suas respectivas ramificações.

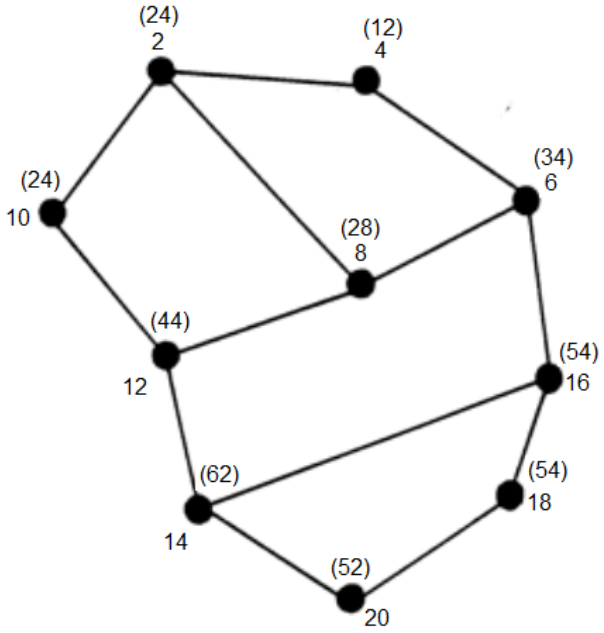
Figura 24- Mapa público com a decomposição do número 110



(editado pelo autor do trabalho)

Após esse processo o mapa ficará configurado da seguinte forma:

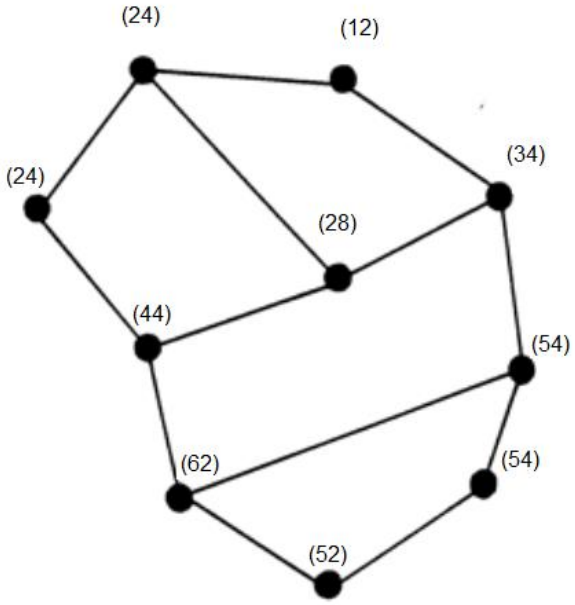
Figura 25- Mapa público



(editado pelo autor do trabalho)

A última parte do processo de criptografar é deixar no mapa apenas os números entre parênteses, apagando os números iniciais que foram colocados em cada nó do mapa.

Figura 26- Mapa público recebido por João

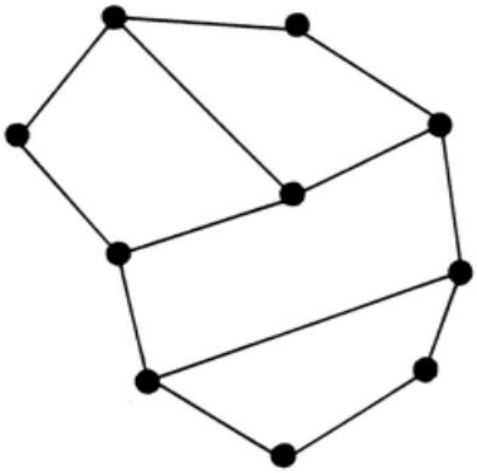


(editado pelo autor do trabalho)

A figura 26 representa a informação que será enviada a João, apagar os números iniciais proporciona segurança, de modo que se a mensagem cair em mãos erradas, dificilmente alguém saberá qual o número enviado.

Exercício 1 - Use o mapa da figura 18 para enviar o número 300 criptografado para o professor Jean.

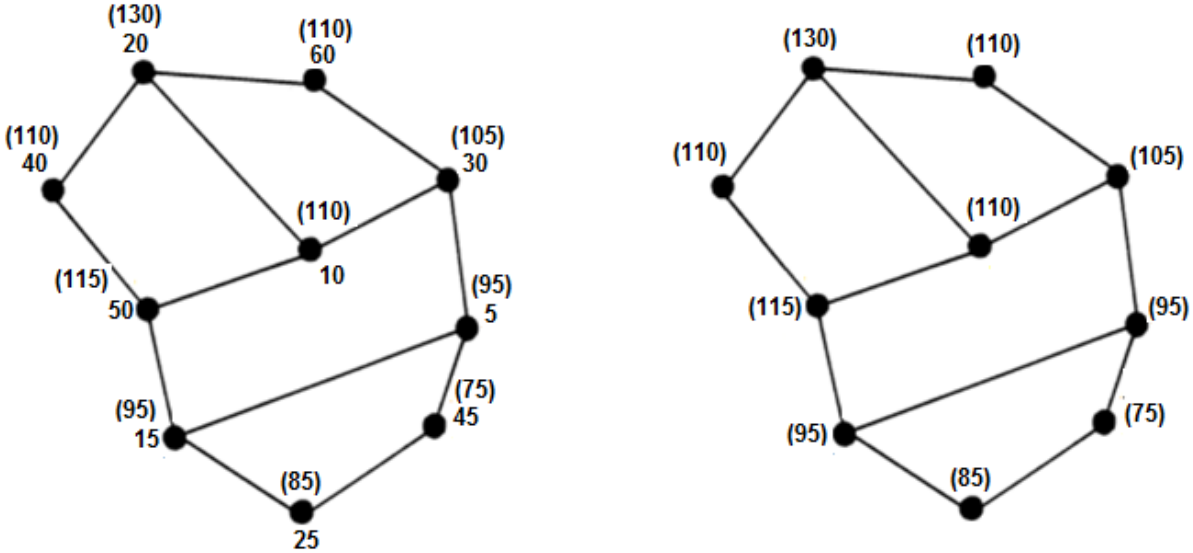
Figura 27- Mapa público



(obtido em https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf)

Solução: Basta seguir o roteiro de como enviar um número por mapa, que foi explicado no início dessa seção.

Figura 28 - Mapas públicos usados para enviar o número 300

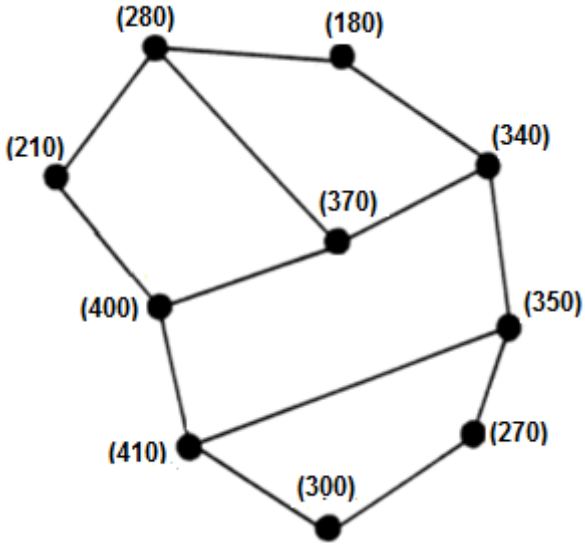


(editado pelo autor do trabalho)

Ou seja, é necessário fazer a decomposição do número 300 como a soma (40+20+60+30+5+45+25+15+50+10). Essa soma deve ser distribuída nos nós de um mapa público como no mapa da esquerda na figura 28. Depois da distribuição inicial das parcelas basta somar o número do nó com as suas ramificações. Por exemplo, o número 40 vai ser somado aos números 20 e 50, resultando em 110 que vai ser colocado entre parêntese sobre o número 40. O número 20 se encontra ligado aos números 40, 60 e 10. Portanto sobre o número 20 será colocada a soma 130 entre parêntese. Isso deve ser feito sobre todos os nós do mapa. No fim do processo deve-se apagar os números que somam 300 e deixar sobre o mapa somente os números escritos entre parêntese. Desse modo o professor Jean vai receber o mapa da direita da figura 28.

Exercício 2 – O professor Jean recebeu o seguinte mapa de um de seus alunos

Figura 29 - Mapa enviado pelo aluno

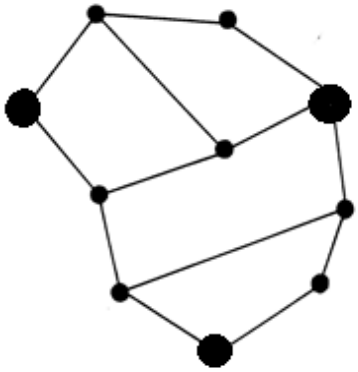


(editado pelo autor do trabalho)

Descubra qual foi o número enviado pelo aluno.

Solução: Para descobrir qual foi o número enviado o professor Jean faz uso do seu mapa privado, o da Figura 30.

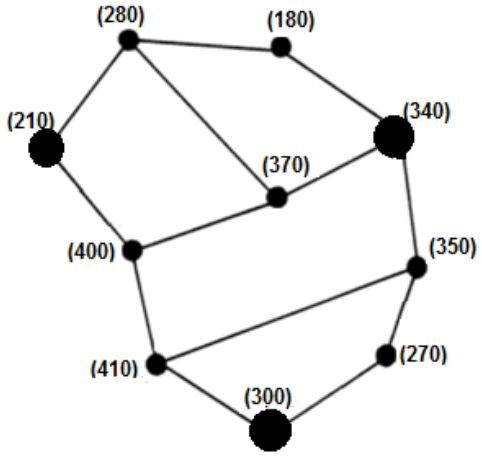
Figura 30 - Mapa privado do professor Jean



(editado pelo autor do trabalho)

Observe que o mapa público e o mapa privado são iguais, exceto que o mapa privado tem alguns nós aumentados. No mapa com a mensagem codificada, o professor Jean marca os nós ampliados como no mapa privado, veja Figura 31, somando os números nos nós ampliados, 210+340+300=850 ele obtém a mensagem enviada. Portanto, a mensagem enviada pelo aluno é o número 850.

Figura 31 - Mapa enviado pelo aluno com os nós ampliados

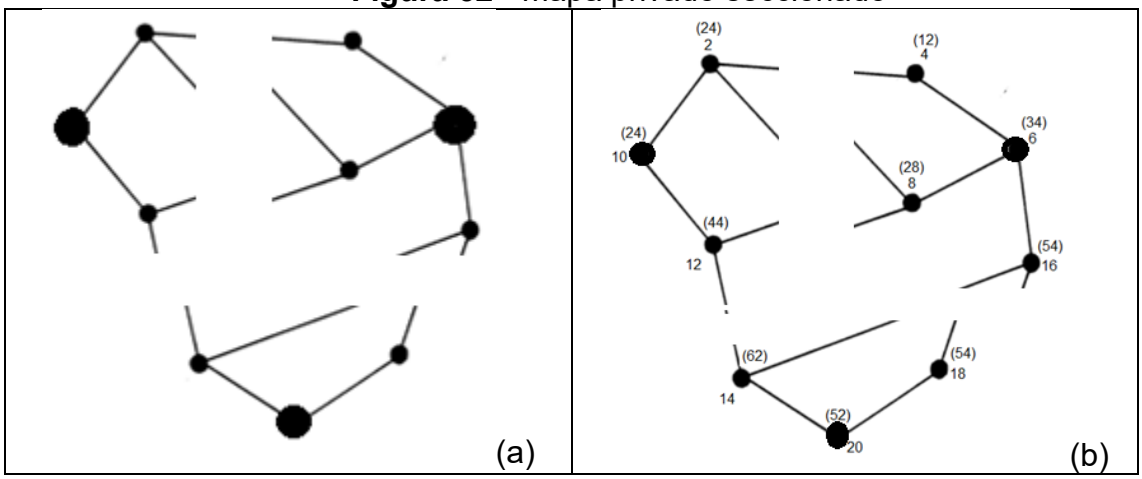


(editado pelo autor do trabalho)

O que garante o funcionamento desse processo de codificação e decodificação é a escolha precisa do mapa. Os nós ampliados no mapa privado dividem o mapa de tal modo que, qualquer outro nó do mapa está conectado a apenas um nó ampliado, a Figura 32 (a) ilustra este fato. No processo de codificação o número escolhido é decomposto em soma, cada parcela da soma é colocada em um dos nós do mapa. No passo seguinte, soma-se o valor de cada nó com seus nós

adjacentes, como qualquer outro nó não ampliado está conectado a apenas um nó ampliado, então a soma dos nós ampliados fornece o número enviado. Como exemplo numérico, a Figura 25, mostra o processo de codificação do número 110, na figura 32(b) dividimos o mapa da Figura 25 pelos nós ampliados do mapa privado. Observe que a soma dos números sem os parênteses em cada nó totaliza 110 o mesmo acontece quando somamos os números entre parênteses dos nós ampliados.

Figura 32 - mapa privado seccionado

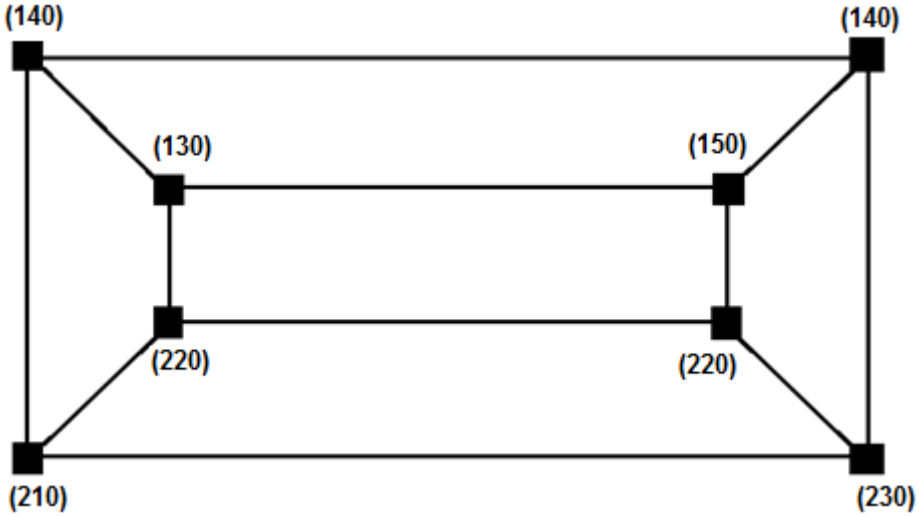


(editado pelo autor do trabalho)

Nesta altura poderíamos nos perguntar, Qual a dificuldade de se desvendar o número enviado tendo acesso apenas aos números do mapa público. No caso do Exercício 2 a pessoa que interceptar o mapa tem que descobrir que o número que está sendo enviado é o número 850. Por que é tão difícil descobrir o número enviado apenas com as informações do mapa público? A explicação consiste no fato de que a criptografia por mapa usa de funções de mão única, aquelas funções que são fáceis de fazer e difícil de desfazer. No caso em questão qualquer um pode decompor o número 850 em parcela de dez somas e escrever o mapa público, mas é muito difícil obter o número 850 a partir dos números colocados entre parêntese no mapa da figura 32 sem saber a “regra” do mapa privado. Tirando a hipótese de você ter sido o autor do mapa privado uma das poucas hipóteses de descriptografar a mensagem é por tentativas. E nesse caso tudo fica mais complicado, pois são várias as possibilidades de operação entre os números do parêntese.

Exercício 3 - Seguindo a ideia do professor Jean. João enviou o mapa público da figura 27 para Maria com números entre parênteses.

Figura 33 - Mapa público que João enviou a Maria



(Criado pelo autor do trabalho)

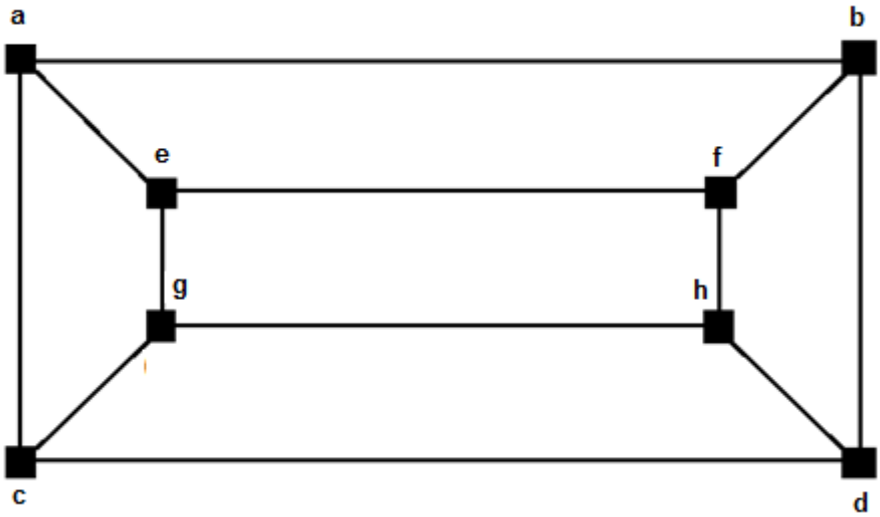
Em relação ao mapa recebido por Maria determine:

a) Como deve ser feita a escolha dos nós a serem somados a fim de se obter o mapa privado?

b) Ajude Maria a descobrir o número enviado por João.

Solução do item a: Vamos inicialmente utilizar o mapa da figura 33 para enviar um número qualquer X. Onde X = a + b + c + d + e + f + g + h. As parcelas que compõe X serão representadas nos nós da figura 34. A intenção com isso é buscar uma regra para obter o mapa privado a partir do desenho do mapa público

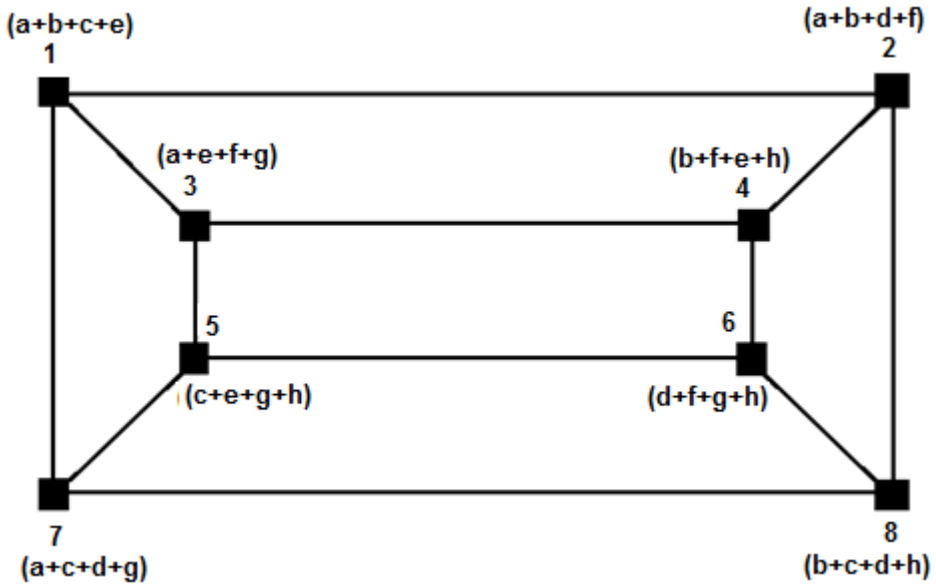
Figura 34 - Mapa público com a decomposição do número X



(Criado pelo autor do trabalho)

Seguindo as instruções dadas pelo professor Jean o próximo passo é representar em cima de cada nó a soma do número do nó com as suas ramificações. Por exemplo, sobre o nó do ponto a, deve ser registrada a soma (a + b + c + e). O nó do ponto b se liga aos pontos a, f e d, portanto sobre o nó do ponto b deve ser registrada a soma (a + b + f + d). Esse processo deve ser feito sobre todos os nós, resultando no mapa da figura 35.

Figura 35 - Mapa público

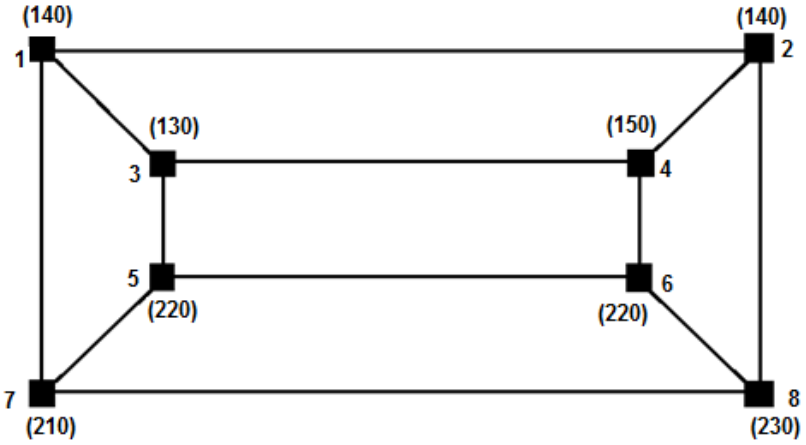


(Criado pelo autor do trabalho)

A partir da figura 35, temos condições de saber quais números devemos somar para obter o mapa privado, que é usado para descriptografar uma mensagem enviada com o mapa público da figura 34. O número a ser enviado pelo mapa foi descrito como X, onde X = a + b + c + d + e + f + g + h. Logo se quisermos obter o mapa privado basta encontrarmos os nós do mapa que quando somados resultam em X. Vale ressaltar que há mais de uma resposta para esse problema. A primeira delas é obtida quando fazemos a soma dos números dos nós 1(a + b + c + e) e 6(d + f + g +h) que resulta em (a + b + c + e + d + f + g +h = X). As outras respostas são dadas pelas somas dos nós de número 8(b + c + d +h) e 3(a + e + f +g) , 2(a + b + d +f) e 5(c + e + g +h) e os nós de número 4(b + f + e +h) e 7(a + c + d +g).

Solução do item b: Para obter o número enviado por João vamos usar a técnica descrita no item a com auxílio visual da figura 35.

Figura 36 - Mapa público recebido por Maria



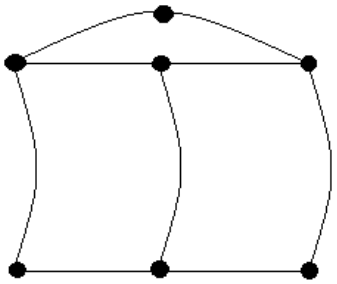
(Criado pelo autor do trabalho)

O número enviado por João pode ser obtido pela soma dos nós 1 e 6, que no mapa da figura 30 corresponderia a soma (120 + 240 = 360). Ou pela soma dos nós 3 e 8 (130 + 230 = 360). Ou pela soma dos nós 2 e 5 (140 + 220 = 360). Obedecendo a técnica do item a, para qualquer par de nós dado na solução do problema vamos obter o número 360. Portanto o número enviado por João a Maria é 360.

Exercício 4 - Dados os mapas públicos de envio de mensagem, determine a partir deles o mapa privado que é usado pelo receptor da mensagem no processo de decriptação. Após descobrir como obter o mapa público indique quais dos mapas representariam “códigos” mais difíceis de serem quebrados. Distribua os alunos em dupla e distribua os mapas dos itens a, b e c para a realização dessa tarefa.

a)

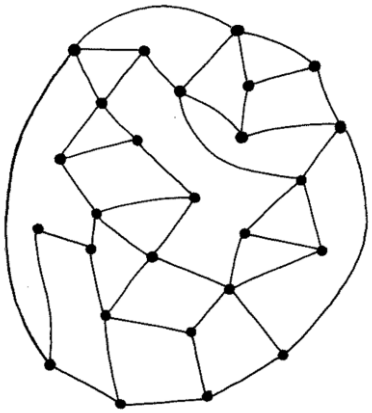
Figura 37- Mapa público



(Criado pelo autor do trabalho)

b)

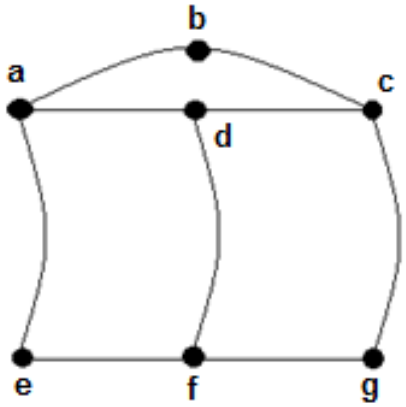
Figura 38- Mapa público



(obtido em https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf)

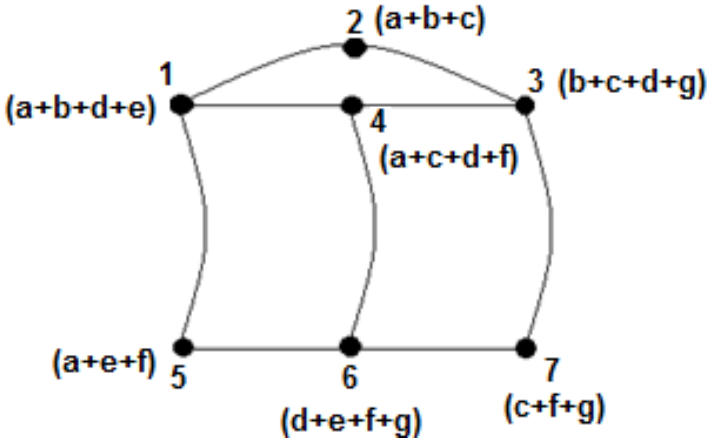
Solução do item a - O mapa do item a tem sete pontos e sete ligações entre seus nós, devido às poucas ligações entre os nós é um mapa de baixa complexidade. Então se a intenção é descobrir o mapa privado vamos enviar por esse mapa um número Y que aqui será decomposto em soma por Y = a + b + c + d + e + f + g +h. Vamos representar as parcelas da soma na figura 39. A figura 40 apresentará a soma das ramificações de cada nó.

Figura 39- Mapa público decomposto



(Criado pelo autor do trabalho)

Figura 40- Mapa público decomposto



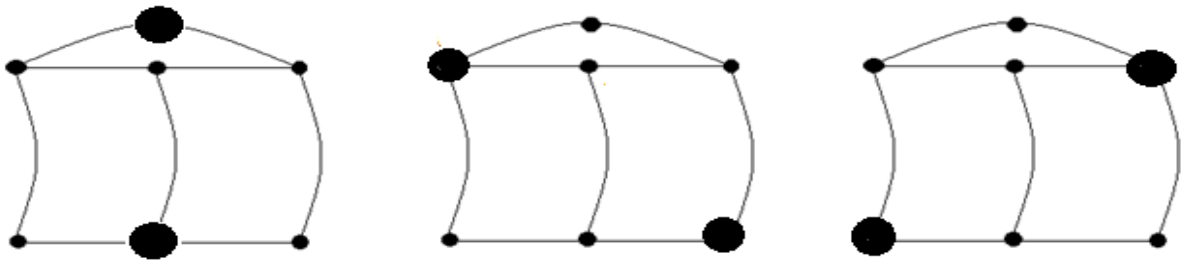
(Criado pelo autor do trabalho)

Para obter o mapa privado basta observar a figura 40 e ver quais nós do mapa que somados resultam em y. Apenas por observação da figura notamos que os pontos do mapa que oferecem essa soma são:

- 2 e 6, pois a + b + c + d + e + f + g = Y.
- 1 e 7, pois a + b + d + e + c + f + g = Y.
- 3 e 5, pois b + c + d + g + a + e + f = Y.

Diante dessa informação concluímos que os mapas privados podem ser representados por:

Figura 41- Mapa privado obtido a partir do mapa público



(Criado pelo autor do trabalho)

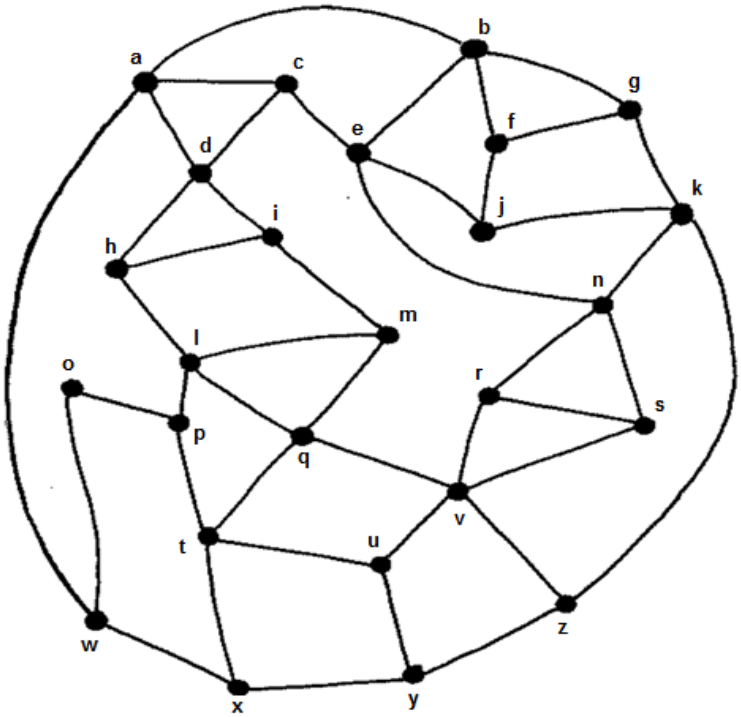
Sobre o mapa privado (e essa dica é importante para achar o mapa privado a partir do mapa público) é possível observar que os nós maiores não se conectam por ramificação, ou seja, pegando o primeiro mapa privado da figura 41 e fazendo uma relação com a figura 39 observamos que os nós maiores que são b e f não se

ligam pelo circuito do mapa. Na mesma figura 41, no mapa central os nós maiores a e g também não se conectam por ramificações. Então sempre que formos procurar um mapa privado a partir do mapa público, é importante observar que o mapa privado será composto por nós que não se conectam pelos circuitos do mapa.

Para a atividade de envios de número na sala de aula esse mapa apresenta nível de segurança baixo, pensando novamente como código, o mapa do item (a) representariam códigos que são fáceis de serem quebrados. Isso ocorre, porque o mapa apresenta poucos nós e ramificações. Uma curiosidade a se observar no mapa privado é que entre dois nós maiores sempre há dois nós menores.

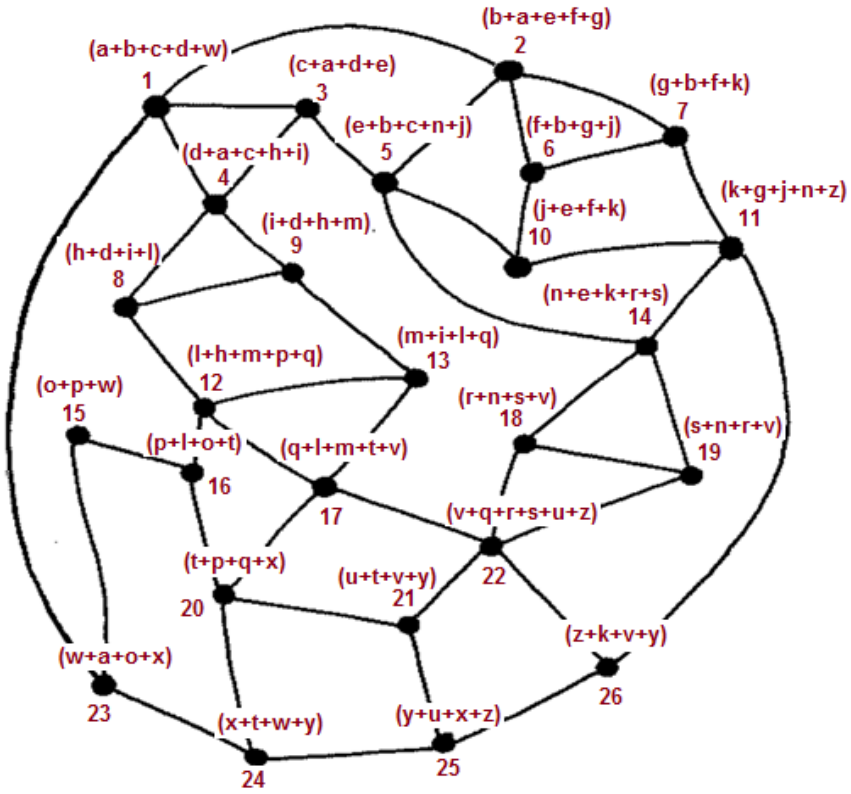
Solução do item b - O mapa do item b apresenta 26 nós, portanto se formos enviar um número W por esse mapa, W deverá ser decomposto em 26 parcelas. Assim teremos que W = a+b+c+d+e+f+g+h+i+j+k+l+m+n+o+p+q+r+s+t+u+v+w+x+y+z. Para facilitar a tarefa de encontrar um mapa privado do item c vamos usar as figuras 42 que vai apresentar as 26 parcelas de W registradas em um mapa e a figura 43 que é aquela que vai apresentar as somas dos números que se conectam com cada nó do mapa.

Figura 42- Mapa público com a decomposição do número W



(Obtido em https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf)

Figura 43- Mapa público com a decomposição do número W



(Obtido em https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf)

O mapa do item c é o mais complexo desse exercício, pois ele tem 26 nós e 43 ramificações que ligam os nós de dois a dois. E diferente do item a desse exercício, não conseguimos encontrar de forma imediata os nós que somados resultam no número W. Pelo método de "força bruta" que consiste em tentativa e erro, depois de várias tentativas chegamos que a soma dos nós de número 4, 6, 14, 15, 17 e 25 resultam no número W. Pois:

- (d+a+c+h+i)+(f+b+g+j)+(n+e+r+k+s)+(o+p+w)+(q+l+m+t+v)+(y+u+x+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+z) = W

Novamente fazendo uma analogia entre o envio do número por mapa como uma forma de codificação, teremos que o mapa do item c é um mapa seguro, com código difícil de ser quebrado. Especialmente se considerarmos que na aplicação da atividade os códigos são quebrados por meio de tentativa e erro. Logo dos três itens do exercício o item c é o que apresenta o mapa mais seguro.

Exercício 5 - A tarefa de encontrar mapas privados a partir de mapas públicos se torna mais difícil conforme os mapas se tornam mais complexos, isso é quando os mapas apresentam mais nós e ramificações. Por outro lado construir mapas públicos a partir de fragmentos de mapas privados é uma operação mais simples. Entregue aos alunos da sala uma cópia do fragmento de mapa da figura 42, em seguida peça aos alunos que obtenham o mapa público do item c a partir do impresso recebido pelo professor.

Figura 44- Fragmento de mapa público

(Editado pelo autor do trabalho)

Exercício 6 - “Agora é com você”. Usando as estratégias dos exercícios anteriores dessa seção construa um mapa público que sirva para troca de informação numérica, em seguida faça uma troca do mapa que você fez com um colega e tente determinar o mapa privado dele.

Os exercícios da atividade 5 se baseiam no uso de funções de mão única. Como descrito aqui anteriormente, as funções de mão única são aquelas que são fáceis de calcular ou fazer, mas que são muito difíceis de serem revertidas ou desfeitas. Uma caixa de correio representa uma analogia adequada ao uso das funções de mão única no processo de criptografia assimétrica. Qualquer um pode

jogar uma carta dentro da caixa do Correio (a abertura da caixa é pública), em contrapartida somente o funcionário do correio consegue retirar a carta de dentro da caixa, pois o funcionário do correio tem a caixa privada. O exemplo também pode ser associado a troca de e-mails. Conhecendo o seu endereço eletrônico qualquer um pode lhe enviar um e-mail, porém só você e quem tem acesso a sua senha pode abrir a caixa de entrada e ler as mensagens recebidas. Uma caixa de correio é uma boa comparação que pode ser feita com estas funções especiais: a abertura da caixa é pública, qualquer um pode jogar uma carta dentro da caixa. Abrir a caixa de correio já é outra conversa: é preciso detonar a caixa com uma marreta ou a pessoa autorizada pode abri-la sem muito esforço porque possui a chave. A criptografia de chave pública funciona baseada neste princípio. O uso de uma chave pública para envio de mensagem e uma chave privada para que o receptor tenha acesso ao conteúdo da mensagem.

No nosso exercício os mapas que eram usados para enviar as mensagens eram os mapas públicos, os mapas com os nós destacados eram os mapas privados. É importante observar também que o uso de mapas remete a funções de mão única, pois era muito mais fácil distribuir os números nos nós dos mapas do que obter a regra do mapa privado e fazer a decodificação da mensagem. De forma geral as funções de mão única são a base da criptografia assimétrica e nesse sentido a atividade 5 traz noções ao leitor de como a criptografia assimétrica funciona e como se dá o seu processamento em algoritmos.

CONSIDERAÇÕES FINAIS

O presente trabalho se constitui como trabalho de conclusão de concurso do mestrado profissionalizante do PROFMAT. A ideia inicial do trabalho era apresentar o contexto histórico e três atividades relacionadas a criptografia de chave simétrica e assimétrica. Como o passar dos meses as ideias foram amadurecendo até que em conjunto com o orientador do trabalho chegamos a essa estrutura que aqui se encontra.

A criptografia se encontra muito presente em nosso dia a dia. Seja na troca de correspondência eletrônica, compras pela internet ou até mesmo em transações bancárias via smartphone. Dito isso a pesquisa do contexto histórico foi feita de forma detalhada, onde buscamos entender as origens da criptografia culminando na descrição de como a criptografia é feita hoje em dia. A intenção é que o primeiro capítulo ofereça informações relevantes ao leitor do trabalho para que ele possa entender o ponto de partida da criptografia e que com o passar do tempo a criptografia evolui buscando sempre formas seguras de transmissão e recepção de dados.

O segundo capítulo do trabalho apresenta atividades lúdicas que podem ser aplicadas no ensino básico, a partir do sexto ano do ensino fundamental. Toda atividade tem uma breve descrição do contexto histórico e dos termos específicos da criptografia que são usados no texto da questão.

As atividades que foram desenvolvidas envolvem aplicações da Cifra de César, Análise de Frequências, Criptografia Simétrica e Assimétrica. Reunindo a análise histórica e o uso das atividades o trabalho busca mostrar a importância da criptografia, mas sobretudo de apresentar um material rico de informações para que professores possam tomar como referência para elaboração de aulas e projetos.

REFERÊNCIAS BIBLIOGRÁFICAS

BEISSINGER , J; PLESS, V. **The Cryptoclub Workbook: Using Mathematics to Make and Break Secret Codes.** A K Peters/CRC Press; Edição: 1 , 2018.

BELL, T., WITTEN, I. H., FELLOWS, M. **CS Unplugged An enrichment and extension programme for primary-aged students**, disponível me https://classic.csunplugged.org/

BOYER, Carl B. **História da matemática**, 2a. ed. - São Paulo: Edgard Blucher, 1996.

COUTINHO, S. **Números Inteiros e Criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2005.

DAVIES, N. **A Europa em Guerra** (1939-1945)*. Lisboa: Edições 70, 2008. pp. 55.*

FIARRESGA, V. M. C. **Criptografia e Matemática**. Dissertação (Mestrado)- Universidade de Lisboa, 2010.

KAHN, David. **The Codebreakers**. Nova York: Macmillan, 1967.

LOUREIRO, F. O. **Tópicos de criptografia para o ensino médio**. Dissertação (Mestrado) -Universidade Estadual Norte Fluminense, 2014.

MATSUMOTO, M. S. **Despertando o interesse do aluno pela matemática com a criptografia**. Dissertação (Mestrado) — Universidade Federal da Grande Dourados, 2014.

OLIVEIRA, Ronielton Rezende, **Criptografia tradicional simétrica de chave privada e Criptografia assimétrica de chave pública: análise das vantagens e desvantagens.** Trabalho da pós-graduação Criptografia e Segurança em Redes da UFF, Niteroi, (2006).

Parâmetros Curriculares Nacionais: matemática. Secretaria de Educação Fundamental. Brasília: MEC, SEF, 1997. Disponível em: http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf. Acesso em 18 agosto 2019.

SANTOS, J.L. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica**. Dissertação (Mestrado) - Universidade Federal da Bahia - UFBA, 2013.

SCHÜRMANN, A.H. **CRIPTOGRAFIA MATRICIAL APLICADA AO ENSINO MÉDIO**. Dissertação (Mestrado) - Universidade Estadual de Londrina - UEL, 2013.

SINGH, Simon. **O Livro dos Códigos.** Rio de Janeiro. Record, 2001.

TKOTZ, V. Criptografia - **Segredos Embalados para Viagem**. [S.l.: s.n.], 2005.