UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Ilha Solteira - SP

NÁDIA MARQUES IKEDA PEREIRA

Criptografia: uma nova proposta de ensino de matemática no ciclo básico

Ilha Solteira - SP
2015

NÁDIA MARQUES IKEDA PEREIRA

Criptografia: uma nova proposta de ensino de matemática no ciclo básico

Dissertação apresentada ao Programa de Pós-Graduação - Mestrado Profissional em Matemática em Rede Nacional como parte dos requisitos para obtenção do título de Mestre.

Prof. Dr. Edson Donizete de Carvalho
Orientador

Ilha Solteira - SP
2015

Nádia Marques Ikeda Pereira

Criptografia: uma nova proposta de ensino de matemática no ciclo básico

Dissertação como parte dos requisitos para obtenção do título de Mestre, junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto, polo Ilha Solteira.

Comissão Examinadora

Prof. Dr. Edson Donizete de Carvalho
UNESP – Ilha Solteira
Orientador

Prof. Dr. Jaime Edmundo Apaza Rodriguez
UNESP – Ilha Solteira

Prof. Dr. Osmar Aléssio
UFTM – Uberaba

Ilha Solteira, SP
20 de fevereiro de 2015

À minha família, em especial aos meus filhos Felipe e Flávia, e ao meu marido Edson, por todo amor, apoio, compreensão, confiança e incentivo em todos os momentos.

AGRADECIMENTOS

Meus agradecimentos à minha família e professores da FEIS-UNESP, que direta ou indiretamente contribuíram para a realização deste trabalho. Em especial, dedico meus agradecimentos:

- A Deus, por ter me dado força e saúde para chegar até aqui;
- Aos meus filhos Felipe e Flávia pelo carinho e compreensão;
- Ao meu marido Edson pelo amor, apoio, confiança e incentivo em todos os momentos;
- Ao Prof. Dr. Edson Donizete de Carvalho, por todo ensinamento, incentivo, confiança, orientação e paciência ;
- Aos Professores do Departamento de Matemática por todo ensinamento, incentivo, confiança.

"O sol é para todos,"

mas a sombra é para quem.

chega primeiro.

Geremias Ludu

RESUMO

O objetivo deste trabalho foi evidenciar a criptografia como uma forma de enriquecer o ensino da Matemática. Foram levantados os aspectos históricos relevantes, mostrando a evolução da criptografia, a relevância do desenvolvimento da criptografia na história da humanidade e a matemática necessária para seu desenvolvimento. Ainda evidenciando que quanto mais a Matemática é aprimorada, mais o homem dispõe de ferramentas para desenvolver a criptografia e assim garantir a segurança das informações. Em contrapartida, muitos conceitos matemáticos utilizados em criptografia fazem parte da grade curricular do ensino da Matemática. Dessa forma, associar os conceitos à uma aplicação tão corrente nos dias de hoje, torna o aprendizado mais significativo.

Palavras-chave: Criptografia, Códigos, Ensino de Matemática

ABSTRACT

The goal of this work, was highlight the cryptography as a way to improve the teaching of mathematics, important historical aspects showing were listed showing the cryptography evolution. The great importance of the cryptography's development in human history and the Mathematics required for this development. Showing also that the more mathematics is improve, the man has more way to encryption's development and then ensure the security of information. By the other hand, many mathematical concepts used in cryptography are part of the educational grade math. This way, mathematics concepts are associates with a applied form in cryptography now, makes the most significant learning experience for the student .

Keywords: Cryptography, Codes and Education Mathematics.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A criptografia tem se tornado um dos principais temas de discussões na matemática, principalmente devido à sua relevância nos dias atuais. A segurança da informação é uma das maiores preocupações a serem desenvolvidas pela sociedade contemporânea.

As mais simples transações on-line requerem algum nível de segurança, e esse tipo de atividade se torna a cada dia mais comum na vida dos usuários. Mas será que eles sabem quanta matemática está envolvida nessas ações? Navegar por redes sociais, compartilhar arquivos, enviar e receber emails, realizar compras em lojas on-line, consultar e realizar transações bancárias, todas essas ações são consideradas comuns na vida da maioria das pessoas, mas como realizar tudo isso com tranquilidade, confiando que as correspondências não serão lidas por terceiros, que terceiros não poderão acessar a sua conta, entre outras ações.

A grande responsável para garantir que a segurança ocorra de forma eficiente é a Criptografia, ou ainda os sistemas criptográficos. A criptografia é um tema matemático que apesar de ser largamente utilizado nos dias atuais, surgiu há muitos séculos atrás. Foi protagonista na decaptação de uma rainha, foi protagonista como comunicação de guerra, comunicação entre reis, foi utilizada como arma de guerra nas duas grandes guerras. Muitos feitos são atribuídos à criptografia, e no decorrer deste período foi necessário que a matemática se desenvolvesse, pois sempre que um código criptográfico surgia, também surgia a necessidade de quebrá-lo. Existe até os dias atuais uma guerra silenciosa, a gerra dos criadores de códigos e os quebradores de código.

Os aspectos históricos e a evolução da criptografia serão abordados mais detalhadamente nos capítulos iniciais. Em conjunto com os aspectos históricos também serão desenvolvidos alguns temas matemáticos relacionados à criptografia. A história nos mostra que a matemática propiciou a criação dos códigos criptográficos, mas a matemática também lança mão de ferramentas para quebrar esses códigos. E, conforme os códigos foram sendo quebrados ao longo da história, o homem sempre continuou e continua em busca de novas ferramentas para criar um código cada vez mais poderoso.

Nesse universo de guerras entre criptógrafos e criptoanalistas a matemática é a protagonista, sempre desafiando ambos os lados. Os temas matemáticos relacionados a esse tema serão abordados do capítulo 3 em diante. Outro foco deste trabalho é relacionar esses temas com o

ensino da matemática. Muitos dos temas aqui abordados estão presentes na grade currícular do ensino básico, ou seja, no ensino médio e no ensino fundamental anos finais.

1.1 O Ensino e a Criptografia

O processo de ensino e aprendizagem está em constante evolução, buscando melhores formas e inspirações para o ensino. Maneiras mais contextualizadas, práticas e concretas de ensinar determinado tema tornaram-se cada vez mais relevantes nesse processo. Fazer com que o aluno consiga atribuir a real importância da temática, elencar os aspectos históricos e também saber contextualizar o que está sendo discutido é de fundamental importância no processo de ensino aprendizagem.

A Proposta Curricular do Estado de São Paulo em consonância com as Leis de Diretrizes e Bases Nacionais ressaltam como prioritário o desenvolvimento das competências leitora e escritora dentro de todo o processo educacional, sendo contemplado em todos os segmentos, não somente em linguagens e códigos, mas também em ciências humanas e exatas. Essa perspectiva educacional reflete a importância da interdisciplinaridade entre as áreas bem como uma forma diferenciada no tratamento da Matemática.

Uma abordagem dos tópicos matemáticos deve contemplar desde os aspectos históricos, fundamentação teórica e aplicação prática para que o educando possa conhecer o tema em todas as suas dimensões.

Neste trabalho, pretende-se abordar alguns tópicos matemáticos que são desenvolvidos na educação básica, desde o ensino fundamental ciclo II até o ensino Médio, sendo evidente que a abordagem pode ser estendida para os demais níveis de ensino. Inicialmente a discussão sobre os aspectos históricos que propiciaram o desenvolvimento dos códigos e ainda a relevância da criptografia nos tempos atuais indica ser uma boa alternativa para o desenvolvimento da competência leitora, além de tornar, para o educando, o tema mais interessante e de aplicação tecnológica.

A criptografia aborda temas em diferentes níveis do processo de ensino e aprendizagem, além de propiciar a interdisciplinaridade com as áreas de códigos e linguagens bem como a área de humanas. O conhecimento profundo da própria linguagem, bem como a análise da frequência com que as letras aparecem no alfabeto, as palavras e pronomes mais utilizados relacionam profundamente a criptografia com as disciplinas da área de códigos e linguagens. O desenvolvimento histórico da criptografia, bem como a sua importância histórica em fatos relevantes da humanidade estão intimamente ligados à área de ciências humanas. Também

pode relacionar a criptografia com o desenvolvimento histórico e tecnológico.

Desta forma, o escopo deste trabalho é fazer com que o educando tenha toda essa percepção e consiga atribuir um real significado à sua aprendizagem.

2 ASPECTOS HISTÓRICOS DA CRIPTOGRAFIA

Neste capítulo, pretendemos fornecer um breve histórico da criptografia e como se deu sua evolução ao longo do tempo. Algumas passagens históricas que julgamos marcantes para a humanidade e que reforçam como esta arte de ocultar mensagens foi decisiva em diferentes épocas. A criptografia foi relevante na decisão de batalhas, segredos de estado e, nos dias de hoje, é de fundamental importância para proteger as informações na web, seja de natureza pessoal, militar ou política.

Iniciaremos esta abordagem com a história de Maria, que ocorreu ao longo do século XVI. Apesar de a criptografia ter sua origem muitos séculos antes, a história de Maria Stuart nos permite evidenciar a importância da criptografia e como esta foi decisiva na vida de Maria. Em seguida, voltamos ao século 1 a.C com o ditador romano Júlio César explorando não só a história mas também a matemática empregada nos sistemas criptográficos.

Figura 1 - Maria, a rainha da Escócia.

Fonte: Adaptado de Revista El Reservado on line

Maria, rainha da Escócia nascida no palácio de Linlithgow, na Escócia, dotada de habilidade política, ambição e beleza, filha única de Jaime V, rei da Escócia, e da francesa Maria de Guise, foi educada na França, na corte de Henrique II e Catarina de Medici. Casou-se (1558) com o

herdeiro do trono francês, Francisco e ficou viúva aos 18 anos, quando voltou à Escócia para assumir o trono, entretanto Maria era católica o que causava sérios inconvenientes tanto para a Escócia protestante quanto para a Inglaterra.

Em 1567, depois de vários episódios de desagrado à nobreza escocesa, Maria abdicou de seu trono em favor de seu filho, e fugiu para a Inglaterra, onde sua prima Elizabeth era soberana.

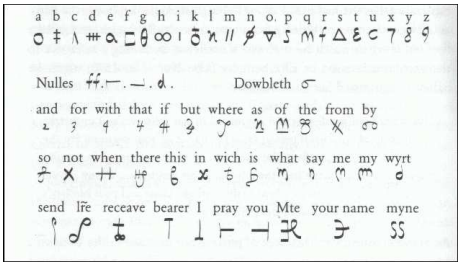
Na Inglaterra, Maria era considerada uma forte ameaça à sua prima, pois Elizabeth era protestante, Maria, católica e os nobres católicos ingleses acreditavam na legitimidade de Maria em substituir Elizabeth no trono inglês.

Dessa forma, Maria foi aprisionada em vários castelos e solares. Após dezoito anos de prisão Maria perdeu todos seus privilégios, tais como ir à estação de águas de Buxton, ficou aprisionada então no Chartley Hall em Staffordshire. Mas o fato é que Maria realmente aspirava ao trono da coroa inglesa, e, dentro da prisão, ela recebeu um pacote de cartas de seus simpatizantes, que foram contrabandeadas por Gilbert Gifford, que as colocou dentro de uma tampa oca de um barril de cerveja a ser levado à prisão e então um dos servos de Maria o abriu a tampa e levou o conteúdo para a rainha dos escoceses. Da mesma forma era o procedimento inverso para retirar cartas de Maria para seus simpatizantes de dentro da prisão.

As políticas anticatólicas do estado inglês, tais como perseguição e tortura, causaram muitos ressentimentos em vários integrantes de famílias inglesas, entre eles estava o jovem Anthony Babington de 24 anos, que juntamente com outros católicos, iniciou uma conspiração em favor da libertação de Maria e ainda a excomunhão de Elizabeth pelo papa Pio V tornando legítimo o seu assassinato.

Logo Maria tomou conhecimento do complô para sua libertação e da mesma forma estabeleceu uma comunicação com Babington através das cartas escondidas na tampa do barril de cerveja, mas com um cuidado a mais, as cartas eram cifradas, de modo que, mesmo se fossem interceptadas, o seu conteúdo se manteria em segredo.

Figura 2 - Nomenclador de Maria



Fonte: Adaptado de Revista El Reservado on line

Porém a coroa inglesa contava com Walsingham, que além de primeiro secretário da corte inglesa, era o chefe do departamento de espionagem da coroa. Walsingham interceptou algumas das correspondencias de Maria e o conspiradores, mas, como as mensagens eram cifradas, não foi possível tomar conhecimento de seu conteúdo, não inicialmente.

Depois de alguns estudos e tentativas, Walsingham conseguiu quebrar o código utilizado por Maria e Babington e dessa forma tomou conhecimento de todos os nomes dos conspiradores e o que haviam planejado. Em posse de todas essas provas e informações, Walsingham revelou à rainha Elizabeth e propôs um julgamento aos traidores da coroa.

Maria foi levada ao castelo de Fotheringhay para seu julgamento por participar de um complô cujo objetivo era assassinar a rainha da Inglaterra. Maria, no entanto, se manteve confiante, negou qualquer tipo de conhecimento e participação no complô, ela estava confiante de que mesmo em posse das cartas, Walsingham não teria tomado conhecimento de seu conteúdo, uma vez que as mensagens estavam cifradas.

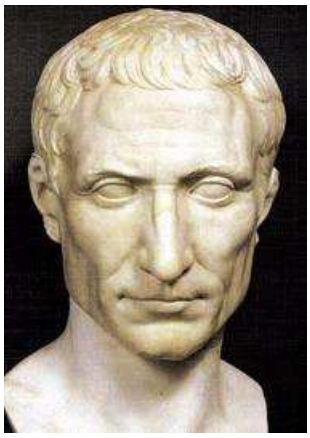
No entanto Walsingham já havia decifrado todas as cartas, e as provas contra Maria foram incontestáveis. Dessa forma, no dia 8 de fevereiro de 1587 Maria foi condenada e como forma de execução foi decapitada.

Figura 3 - Execução de Maria

Fonte: Adaptado de Revista El Reservado on line

2.1 Júlio César de Roma

Figura 4 - Julio César de Roma

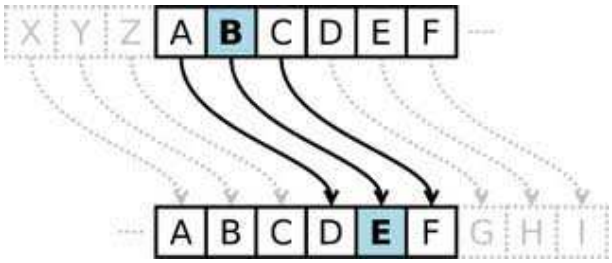


Fonte: Adaptado de *This is war.blogspot*

Júlio César foi um líder militar e político romano, desempenhou um papel crítico e dramático na história da Europa como consequência de suas conquistas, que se estenderam da Gália até o oceano Atlântico. Perto do fim de sua vida, tornou-se ditador vitalício e iniciou uma série de reformas administrativas e econômicas em Roma. Para César, a segurança de suas informações era primordial para garantir o êxito em seus feitos, dessa forma César foi responsável por desenvolver um sistema no qual se pretendia garantir a segurança de suas mensagens, que se interceptada por inimigos não poderiam ser decifrada sem uma chave.

O Código de César, ou ainda criptografia de César, é um dos métodos de criptografia mais antigos e difusos de que se tem notícia. Seu funcionamento é simples, consiste em deslocar as letras do alfabeto de acordo com uma chave. Assim, se a chave era 3, como na imagem abaixo, transformava-se a letra B em E, a letra A virava D e assim sucessivamente. Nesse sistema o alfabeto sofre apenas um deslocamento de acordo com a chave utilizada e nos permite ter no máximo 25 chaves possíveis, uma vez que a chave 0 e 26 não resulta em codificação, no entanto se utilizarmos as letras do alfabeto de forma desordenada aumentamos consideravelmente o número de possibilidades. Algumas possibilidades de deslocamento são descritas nas figuras a seguir:

Figura 5 - Código de Cesar com deslocamento



Fonte: Adaptado de Wikipedia

Figura 6 - Troca de Vizinhos

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

P	Q	R	S	T	U	V	W	X	Y	Z
O	R	Q	T	S	V	U	X	W	Z	Y

Fonte: Adaptado de Wikipedia

Figura 7 - Alfabeto quebrado ao meio

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

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

Fonte: Adaptado de Wikipedia

Se considerarmos apenas o deslocamento do alfabeto como possibilidade para criar um códigos, teremos um número muito restrito de possibilidades, ou seja, teremos no máximo 26 formas de codificar a mensagem, no entanto se desordenarmos a ordem do alfabeto, o número de possibilidades aumenta consideravelmente. Por exemplo, consideremos inicialmente as vogais.

a	e	i	o	u

Para a letra "a"temos 5 possibilidades de permutação, ou seja, ela pode assumir na codificação qualquer uma das letras, inclusive ela mesma, dessa mesma forma a letra "‘e"’assume 4 possibilidade e assim por diante. Pelo **Princípio Multiplicativo da Contagem** são:

$$5.4.3.2.1 = 120 \text{ possibilidades ou ainda } 5!$$

Portanto, se nossa escrita fosse composta apenas por vogais, teríamos 5! maneiras diferentes de criptografar. Similarmente ocorre a criptografia com o nosso alfabeto, temos 26 letras, então existem 26! maneiras diferentes de criptografar, o que sugere 403291461126605635584000000 possibilidades, um número consideravelmente maior do que as possibilidades quando apenas deslocamos o alfabeto respeitando a sua ordenação.

Em geral, se tivermos k letras, teremos *k* permutações, dentro dessas possibilidades teremos que k respeitam a ordenação inicial e o número de desordenamentos é dado por:

$$n!(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ... + \frac{(-1)^n}{n!})$$

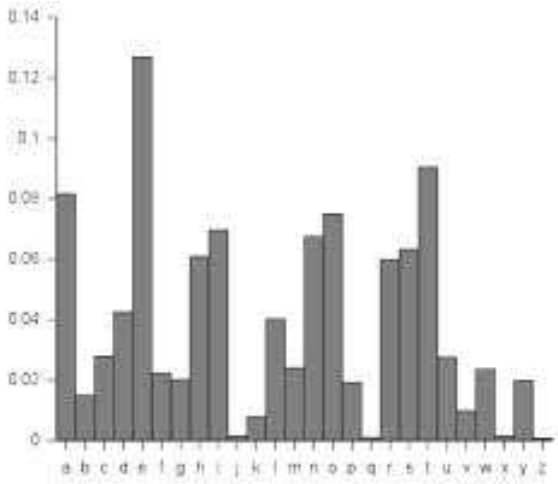
A conclusão que identificamos do código de César é que existe uma vasta possibilidade de combinações, o que gera uma sensação de segurança, pois com tantas possibilidades seria muito difícil quebrar esse código sem o conhecimento da chave. Todavia a história dos códigos nos revela que sempre existiu uma árdua disputa em codificar e decodificar uma mensagem, ou seja, como quebrar um código. E com o código de César não foi diferente, surgiram métodos para quebrá-lo.

O escritor americano Edgar Allan Poe contemplou em sua obra "História de Mistério e Imaginação", no conto "O escaravelho de ouro"uma mensagem criptografada em um pergaminho que seria a referência para um mapa do tesouro.

$(53+305))6*;4826)4.)4);806*;48+8pi60))85;1(;:\ *8+83(88)5*+;46(;88*96*?;8)*(;485);5*+2:*(;4956*2(5*-4)8pi8*;4069285);)6+8)4;1(9;48081;8:81;48+85;4)485+528806*81(9;48;(88;4(?34;48)4;161;:188;?$

Essa mensagem pode ser decifrada, assim como o código de César utilizando uma técnica denominada análise de frequência. Esta técnica se baseia fundamentalmente em analisar qual a frequência do alfabeto em determinado idioma. No código de Poe basta realizar a análise de frequência do idioma inglês , e iniciar o processo de decifragem. No alfabeto inglês, a letra que aparece com maior frequência é a letra e, no código de Poe o número 8 aparece mais vezes, e em algumas ocasiões aparece de forma dobrada 88, que segundo a nossa análise poderia ser interpretado por ee e muito utilizado na língua inglesa.

Figura 8 - Frequência do alfabeto inglês



Fonte: Adaptado de Wikipedia

Realizando uma análise no trecho da obra observamos que:

Tabela 1 - Frequência que os caracteres aparecem no trecho da obra

caracter	frequência
8	33
;	26
4	19
)	16
*	13
5	12
6	11
+	8
0	6
9	5
:	4
?	3
pi	2
-	1

Comparando a tabela que indica a frequência dos caracteres no conto com o gráfico de frequência da língua inglesa, verificamos que o caracter 8 aparece por 33 vezes na mensagem, e a letra mais frequente no alfabeto inglês é a letra "e", também é muito comum na língua inglesa sequência "ee"e verificamos a ocorrência do caracter 88, prosseguindo dessa forma a mensagem cifrada toma a seguinte forma:

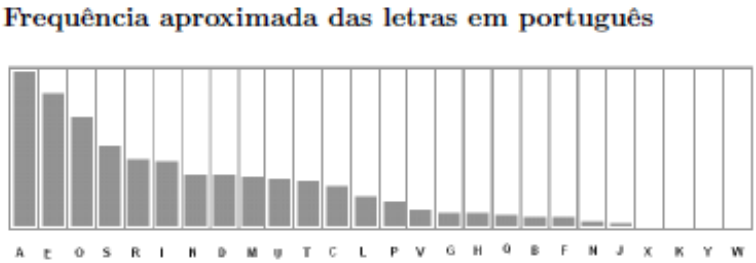
"*A good glass in the bishopt's hotel in the devilt's seat forty-one degrees and thirteen minutes north east and by north main branch seventh limb east side shoot from the left eye of the deatht's-head a bee line form the tree through the shot fifty feet out*"

A tradução dessa mensagem para a língua portuguesa:

" *Um bom vidro na hospedaria do bispo na cadeira do diabo quarenta e um graus e treze minutos nordeste e quarta de norte ramo principal sétimo galho do lado leste a bala através do olho esquerdo da cabeça do morto uma linha de abelha da árvore através da bala cinquenta pés para fora.*"

A técnica utilizada no conto para decodificar a mensagem é denominada análise de frequência, e é baseada em analisar as letras de maior incidência em um determinado idioma e comparar com a letra ou caracter que possui maior frequência na mensagem codificada, a partir de então iniciar o processo de decodificação.

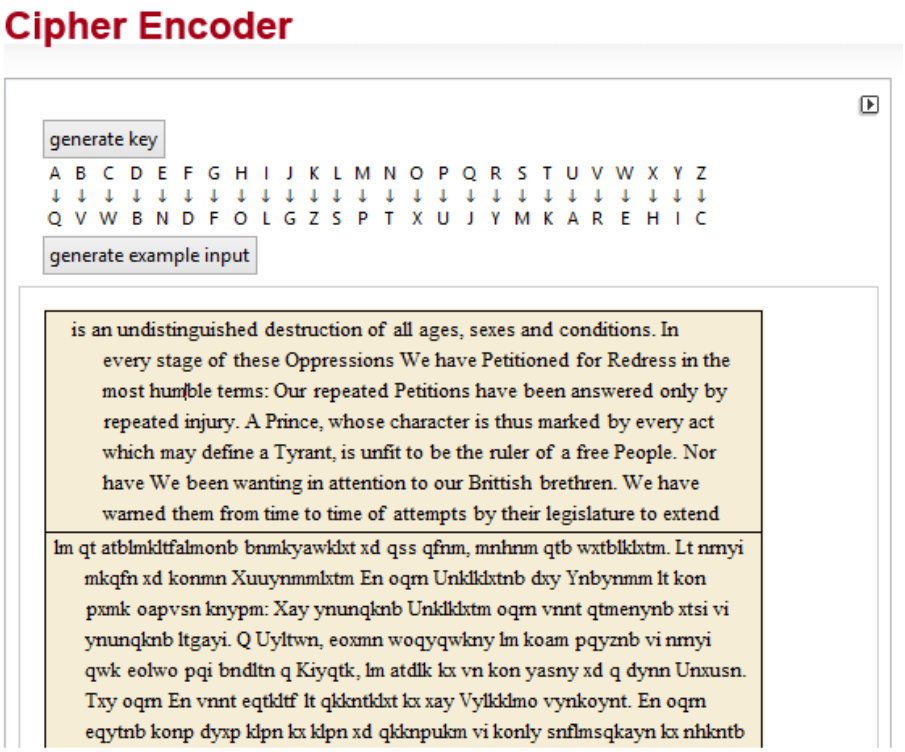
Figura 9 - Frequência do alfabeto português



Fonte: Adaptado de Wikipedia

A análise de frequência é uma alternativa muito eficaz para os criptoanalistas quebrarem os códigos. No entanto, no século XV era uma tarefa árdua analisar um texto elencando à frequência das letras ou símbolos descritos nas mensagens. Mas apesar de árdua não era impossível, demandava algum tempo uma vez que a tecnologia daquela época era muito modesta. Na atualidade temos alguns softwares que realizam essa tarefa em apenas alguns segundos, por exemplo, no site *http://demonstrations.wolfram.com/CipherEncoder*, existe um ambiente em que é possível escolher como o alfabeto cifrado será disposto e, digitando a mensagem em um campo, esta já aparece cifrada automaticamente abaixo.

Figura 10 - Cifragem Wolframcipher



Fonte: Adaptado de wolfram.com

A comunicação secreta ao longo da história, serviu como uma verdadeira arma de guerra. Foi a principal responsável pelo desenvolvimento da criptografia. Inicialmente a esteganografia, que é a arte de ocultar a mensagem, foi a mais utilizada, paralelamente começaram a ser desenvolvidas as técnicas de criptografia.

A palavra criptografia deriva do grego *kriptos*, que significa "oculto", ou seja, a criptografia é a arte de ocultar o significado da mensagem. O processo de ocultar o significado da mensagem é conhecido por encriptação. O desenvolvimento da criptografia ocorreu como consequência da proteção da informação, seja esta de qual natureza for, não estando mais restrita nos dias de hoje apenas no campo militar ou político.

Na mais simples transação bancária, nos tempos atuais, é necessário que as informações sejam protegidas, a comunicação pela internet, o comércio eletrônico também requerem uma certa segurança para os usuários, além de haver necessidade da autenticidade dos dados. A responsável pelas técnicas de segurança e proteção dos dados é a *criptografia.*

Cifra é um sistema utilizado para esconder o significado de uma mensagem substituindo cada letra da mensagem original por outra letra. O sistema deve ter alguma flexibilidade em-

butida, conhecida como chave. A chave é o elemento que transforma o algoritmo de cifragem geral num método específico de cifragem. De um modo geral, o inimigo pode saber qual é o algoritmo de cifragem sendo usado pelo remetente e o destinatário da mensagem, mas não pode conhecer a chave.

Existem vários tipos de chave: a chave pública, a chave particular e chave de depósito. A chave pública é a chave usada pelo remetente da mensagem para cifrá-la em um sistema de criptografia de chave pública. A chave particular é a chave usada pelo receptor para decifrar uma mensagem num sistema de criptografia de chave pública, a chave particular deve ser mantida em segredo. A chave de depósito é um esquema no qual os usuários entregam cópias de suas chaves secretas para uma terceira pessoa, confiável, o agente de depósito, que entregará essas chaves aos agentes da lei somente sob certas circunstâncias, como por exemplo, sob ordem judicial.

A cifragem por computador que é o tipo mais utilizado atualmente, envolve chaves que são caracteres. O comprimento de chave se refere ao números de dígitos ou bits na chave e dessa forma indica o maior número que pode ser usado como chave, determinando dessa forma o número de chaves possíveis. Assim, quanto mais longo for o comprimento , mais tempo o criptoanalista levará para testar todas as chaves. O nível de segurança da informação está intimamente ligado aos recursos computacionais. Por exemplo, na época em que estava em uso o código tipo Júlio César era possível decodificar a mensagem, porém esse processo era baseado na análise de frequência e demandava muito tempo, entretanto com o desenvolvimento da tecnologia podemos realizar o mesmo processo em frações de segundos.

O nível da segurança da informação está relacionado ao tipo de criptografia empregada para proteger tal informação. O desafio nos dias de hoje é o de criar técnicas criptográficas, ou seja, criar algoritmos tão complexos que até mesmo com o auxílio do computador seria difícil decodificar a mensagem.

Na atualidade os algoritmos são considerados seguros devido ao comprimento da chave ser muito extenso e que as interações matemáticas envolvidas na decodificação do algoritmo tenham uma alta ordem de complexidade. A criptografia moderna é classificada em dois tipos, a criptografia simétrica e a criptografia assimétrica.

2.2 Criptografia Simétrica

A criptografia simétrica é aquela na qual temos apenas uma chave, ou seja, depois de definida a chave, a mesma será utilizada para encriptar e decriptar a mensagem, a sua segurança

está relacionada a apenas que o rementente e o destinatário conheçam essa chave. O princípio utilizado é uma função que gera a mensagem codificada, e para decodificá-la basta aplicar a função inversa.

2.3 Criptografia Assimétrica

A criptografia assimétrica é aquela na qual temos dois tipos de chave, a chave pública e a chave privada. A chave pública é aquela de conhecimento geral, ou seja, de conhecimento de um ou mais remetentes que queiram enviar uma mensagem codificada a um receptor, porém somente o receptor legítimo deve conhecer a chave privada, sendo o único capaz de decodificar a mensagem. Uma vez a mensagem encriptada, esta pode ser de conhecimento público, mas para decifrá-la sem o conhecimento da chave correta será muito complexo. Um algoritmo que utiliza esses princípios e muito utilizado é o algoritmo RSA.

2.3.1 Algoritmos de Chave Pública

O conceito de chave pública foi inventado por Whitfield Diffie e Martin Hellman, e, simultaneamente de forma isolada, por Ralph Merkle. A principal contribuição para a criptografia foi a noção de que as chaves poderiam ocorrer em pares, uma chave para encriptação e uma chave para decriptação.

Desde 1976, numerosos algoritmos de chave pública, foram propostos, muitos inseguros e outros impraticáveis, onde o texto cifrado é muito maior do que o texto original.

Poucos algoritmos garantiam a segurança e praticidade. Alguns algoritmos eram para a distribuição de chave, outros apenas para encriptação e outros para segurança digital. Somente três algoritmos garantiam a encriptação e a segurança digital: o RSA, o El Gamal e Rabin.

2.3.2 Segurança dos Algoritmos de Chave Pública

Desde que um criptoanalista tenha acesso a uma chave pública ele pode encriptar qualquer mensagem. Os algoritmos de chave pública foram desenvolvidos para resistirem à interceptações e sua segurança é baseada na complexidade de deduzir a chave secreta da chave pública e na complexidade de deduzir o texto cifrado para o texto original.

2.4 Cifra de Substituição Monoalfabética

Todo esse sistema no qual cada letra é substituída por outro caracter é chamado de **cifra de substituição**. O código de César é um exemplo de cifra de substituição, mais especificamente um modelo de **cifra de substituição monoalfabética** no qual o alfabeto cifrado permanece fixo durante toda a cifragem.

Durante muitos séculos a cifra de substituição monoalfabética simples foi suficientemente segura para manter os segredos, mas o desenvolvimento da técnica de análise de frequência primeiro no mundo árabe e depois por toda a Europa, fragilizou esse tipo de cifragem. Qualquer pessoa que utilizasse dessa forma de cifragem estaria vulnerável a um estudo de um criptoanalista. Surgiu então uma forte necessidade dos criptógrafos criarem uma nova forma de cifragem, mais forte, que garantisse a segurança dos dados.

2.5 Cifra de Substituição Polialfabética

Com essa nova perspectiva, o polímata florentino Leon Battista Alberti, no século XV, propôs uma cifra de substituição diferenciada, na qual o alfabeto mudava durante a cifragem. Este sistema de substituição é denominado **cifra de substituição polialfabética**. Com a mudança do alfabeto durante o processo de cifragem, seria muito mais árduo realizar uma análise de frequência das letras do alfabeto, aumentando consideravelmente o nível de segurança da mensagem.

Inspirado no trabalho de Alberti, ainda no século XV, surge Blaise Vigenère, que utiliza de 26 alfabetos cifrados distintos para criar uma mensagem cifrada. Vigenère combina de uma forma muito eficaz o trabalho de vários criptógrafos da época. Seu trabalho consiste em montar inicialmente um quadrado com 26 alfabetos cifrados, e cada alfabeto cifrado obedece ao princípio do Código de César, ou seja, é apenas um deslocamento do alfabeto original, respeitando a ordem das letras.

O quadrado de Vinègere é da seguinte forma:

Figura 11 - Quadrado de Vigenère

O quadrado de Vigenère

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

Fonte: Adaptado de http/danieldonda.wordpress.com

Cada letra da mensagem pode ser cifrada de acordo com uma linha do quadrado de Vigenère, ou seja, a primeira letra pode ser cifrada com a linha 20, a segunda letra com a linha 3, e dessa forma seria muito difícil realizar uma análise de frequência, mas também seria muito difícil para o receptor da mensagem conseguir as informações contidas nela. Para isso é necessário que haja uma combinação entre a pessoa que irá enviar a mensagem e o receptor, essa combinação seria uma chave, podendo ser uma sequência de números ou mesmo uma palavra que descreveria como deveria proceder o processo de decifragem.

Por exemplo, queremos ocultar a seguinte frase "A CHAVE ESTA OCULTA"e utilizaremos a palavra chave "PROFMAT".

Tabela 2 - Cifragem com a chave PROFMAT

palavra chave	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R
texto original	A	C	H	A	V	E	E	S	T	A	O	C	U	L	T	A
texto cifrado	p	t	v	f	h	e	x	h	k	o	t	o	u	e	i	r

Dessa forma a mensagem "A CHAVE ESTÁ OCULTA", cifrada com a chave "PROFMAT", fica da seguinte forma "*ptvfhexhkotoueir*", e mesmo tentando aplica a análise de frequência

nessa frase, seria impossível decifrá-la sem conhecer a chave, pois cada letra corresponde á um alfabeto diferente do quadrado de Vigenère.

O quadrado de Vigenère com as linhas definidas pela palavra PROFMAT.

Figura 12 - Quadrado de Vigenère PROFMAT

O quadrado de Vigenère

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

Fonte: Adaptado de o próprio autor

Por volta do ano de 1586, Vigenère publicou o seu trabalho "Um tratado sobre a escrita secreta", ou ainda, "*Traicté des Chiffres*", e apesar de seu nível de segurança frente à análise de frequência da cifra monoalfabética, a cifra de Vigenère não foi muito difundida nem utilizada, uma vez que a sua segurança era alta, também a complexidade para a decifragem era muito alta e ainda demandava algum tempo tanto para escrever quanto para ler uma mensagem com essa forma de cifragem.

A cifragem neste momento da história era utilizada para os mais variados fins, desde senhores que não queriam que seus servos tivessem conhecimento de sua correspondência, as senhoras e seus diários, e assim por diante, a cifra de substituição monoalfabética era mais simples de ser empregada apesar de sua segurança. No entanto, as operações militares tinham uma

intensa necessidade de proteger suas informações de forma segura, e a cifra monoalfabética era muito frágil para essa finalidade, a cifra polialfabética era demasiada complexa mas demandava tempo para ser feita e as mensagens necessitavam de uma certa rapidez.

2.6 Cifra de substituição homofônica

A disputa entre os criptógrafos profissionais e os criptoanalistas frente à esse novo cenário fez surgir uma cifra alternativa, nem tão complexa quanto a cifra polialfabética, mas nem tão frágil quanto a cifra monoalfabética. A esse novo sistema de cifragem denominamos **cifra homofônica**, cujo princípio de funcionalidade é o mesmo da cifra monoalfabética, mas de alguma forma induz a análise de frequência ao erro.

Cifra de substituição homofônica é uma cifra na qual existem várias substituições em potencial para cada letra do alfabeto, em potencial para cada letra do texto original. Por exemplo verificamos que a letra "e", é a letra mais frequente do alfabeto inglês, corresponde a 12 por cento da frequência nesse alfabeto, então utilizaríamos 12 caracteres diferentes para designar a letra "e"e supondo que em uma mensagem que gostaríamos de cifrar quando essa letra surgisse utilizaríamos ao acaso um dos 12 caracteres, dificultando uma possível análise de frequência. Assim aconteciam com todas as letras do alfabeto em questão, relacionando um número de símbolos com a sua frequência. Também era muito comum nesse sistema de cifragem que as letras fossem substituídas por números, tornando uma mensagem uma sequência numérica aparentemente caótica.

Dessa forma a cifra homofônica parece ser imune à análise de frequência e não deixa de ser uma forma de cifragem monoalfabética, uma vez que o alfabeto segue fixo durante toda a cifragem. Esse forma de cifragem garantia a segurança da mensagem, pois a técnica dos criptoanalistas de analisarem a frequência não era suficientemente forte para decodificar a mensagem.

Um exemplo de utilização dessa cifragem foi do a Grande Cifra de Luís XIV, que ocultara por cerca de dois séculos os segredos da corte francesa, dentre eles o mais intrigante, *o Homem da Máscara de Ferro.*

A Grande Cifra foi criada por *Antoine e Bonaventure Rossignol* no século XVII, pai e filho inicialmente eram criptoanalistas e auxiliaram o governo francês a decodificar documentos dos inimigos. Entretanto tão notável era a habilidade dos Rossignol à criptoanálise que os levaram a criar a sua própria cifra. A Grande Cifra era tão segura que desafiou todos os criptoanalistas inimigos da França, mas logo após o falecimento dos Rossignol a Grande Cifra entrou em desuso, pois os segredos dessa cifra foram perdidos com a morte do pai e filho.

Durante dois séculos os mais intrigantes segredos da França não foram revelados, somente em 1890, um historiador militar ao descobrir algumas cartas escritas com a Grande Cifra encaminhou esse documento ao Departamento Criptográfico do Exército Francês, onde o comandante Étienne Bazeries passou a estudar a sua decifragem.

Durante anos Bazeries não obteve sucesso, mas novamente ele tentou utilizar a análise de frequência para quebrar essa cifra, porém não poderia ser uma análise de frequência simples, analisando os números que apareciam nos documentos, conseguiu identificar um conjunto numérico que repetia inúmeras vezes, Bazeries percebeu então que os números representavam ora sílabas ora letras, e dessa forma iniciou o processo de decifragem da Grande Cifra.

Após duzentos anos, Bazeries foi a primeira pessoa a conhecer os segredos da França do século XVII, inclusive a identidade do Homem da Máscara de Ferro.

Novamente a guerra entre criptógrafos e criptoanalistas quebram mais uma forma de cifragem, a cifra homofônica. No século XVII cada potencia Européia montavam um centro de decifragem denominado **Câmara Negra**. Era um local onde as correspondencias interceptadas eram replicadas e decifradas por uma equipe de estenógrafos e criptoanalistas. Dessa forma a cifra homofônica também deixara de ser suficientemente segura, sendo neste momento a cifra polialfabética de Vigenère a mais segura.

No final do século XVIII um avanço tecnológico estimulou os criptógrafos a utilizarem as cifras polialfabéticas, o telégrafo. Esse novo e extraordinário meio de comunicação levou a necessidade de proteger os telegramas de serem decifrados.

A origem do telégrafo pode ser traçada em 1753, porém foi em 1839 que sua reputação foi disseminada quando popularizou o nascimento do segundo filho da rainha Vitória, o príncipe Alfred. A notícia foi telegrafada e apenas uma hora depois já estava estampada nos jornais, que ao anunciar a chegada do príncipe, dava crédito ao telégrafo eletromagnético.

Já nos Estados Unidos, Samuel Morse construíra um sistema telegráfico que cobria uma distância de 60 quilômetros, compreendendo o trecho entre Washington e Baltimore. O sistema de Morse produzia um sinal que conseguia fazer marcas curtas e longas no papel, pontos e traços, dando origem ao código Morse. Esse código foi largamente utilizado em toda a Europa, porém consiste apenas substituir as letras do alfabeto por pontos e traços. Para enviar uma mensagem era necessário que um operador transformasse a mensagem em código Morse para ser transmitida à um telegrafista. Dessa forma o conteúdo da mensagem era de conhecimento do telegrafista.

Para assegurar essa nova forma de comunicação os criptógrafos cifravam as mensagens

antes de serem enviadas, para tanto utilizavam o que era considerável até então o meio mais seguro de cifragem *le ciffre indéchiffrable*, a cifra de Vigenère.

Novamente os criptógrafos estavam levando vantagem na guerra contra os criptoanalistas. Mas os criptoanalistas ganham reforços com o notável Charles Babbage, que depois de muita dedicação, descobre uma forma de analisar o comprimento da chave e estabelecer qual foi o alfabeto cifrado utilizado, conseguindo assim decifrar a mensagem. Foi o momento em que a cifra de substituição polialfabética perdeu sua segurança, *le ciffre indéchiffrable* é quebrada.

No fim do século XIX, a criptografia vivia uma época crítica. A cifra mais segura havia sido quebrada, iniciava-se então uma nova jornada em busca de uma nova cifra, enquanto isso a evolução das telecomunicações era notória e também havia a necessidade militar e política de explorar essas comunicações de maneira segura.

Na virada do século, o físico italiano Guglielmo Marconi aperfeiçou ainda mais as telecomunicações, com suas experiências sobre as propriedades dos circuitos elétricos, induziu uma corrente em outro circuito isolado, a uma certa distância, ou seja, foi capaz de transmitir um sinal sem o uso de fios, o sinal de rádio. Marconi inventara o rádio, e com ele reforça ainda mais a necessidade de uma codificação segura.

2.7 A Criptografia como uma arma de guerra

Os militares ficaram fascinados com a invenção de Marconi, as vantagens táticas do rádio eram inúmeras porém estavam relutantes quanto a segurança da informação. Com o início da Grande Guerra e o advento do rádio a necessidade de uma cifra segura era imprescindível. Os criptógrafos inventaram inúmeras cifras, mas todas foram quebradas.

A cifra mais famosa na grande guerra foi a cifra ADFGVX que era extremamente complexa, sendo uma mistura de transposição e substituição. Em julho de 1918 a artilharia alemã se aproximava de Paris, e a única esperança dos aliados era quebrar a cifra ADFGVX e descobrir em que ponto os alemães iriam atacar. Mas os aliados tinham uma arma poderosa, o criptoanalista Georges Paivin que lutou arduamente para decifrar a cifra ADFGVX e obteve êxito.

Com a decifragem das informações alemãs que eram inúmeras, pois o rádio aumentou consideravelmente o tráfego de informações e, consequentemente, o número de interceptações, os aliados sabiam exatamente onde os alemães pretendiam iniciar o ataque e prepararam o contra ataque, resultando em uma retirada alemã depois de cinco dias de batalha.

Em setembro de 1914, um cruzador ligeiro alemão, o Magdeburg, naufragou no mar Bál-

tico. O corpo de um marinheiro alemão afogado foi recuperado pelos russos: grudados ao peito por braços rígidos pelo rigor mortis, estavam os livros de cifras e sinais da Marinha Alemã. No dia 6 de setembro, o adido militar russo procurou Winston Churchill, então Primeiro Lorde do Almirantado. O funcionário recebera uma mensagem de Petrogrado contando-lhe o que acontecera, e que o Almirantado russo, com a ajuda dos livros de cifras e sinais, conseguira decodificar partes de alguns códigos navais alemães. Os livros acabaram entregues a decodificadores britânicos na famosa Sala 40 de Whitehall, onde foram usados para decodificar rotineiramente comunicações secretas alemãs. Uma das comunicações mais importantes interceptadas e decodificadas na Sala 40 foi o telegrama de Zimmermann.

Arthur Zimmermann, um jovem ministro das Relações Exteriores, parecia anunciar uma nova era de diplomacia alemã inteligente. No entanto, seu telegrama interceptado e remetido à criptoanálise na Sala 40, revelava as verdadeiras intenções da ofensiva alemã. As informações contidas nesse telegrama revelavam um ataque da ofensiva alemã e obrigaram os Estados Unidos saírem da neutralidade. Foi através desse telegrama que houve uma mudança no cenários da Primeira Grande Guerra, os Estados Unidos passaram de expectadores para protagonistas da guerra.

Em conseqüência da publicação do caso Magdeburg, a Alemanha elevou o nível de seus códigos secretos no período entre guerras, investindo num complexo sistema mecânico que testaram até o limite os recursos de decodificação da Grã-Bretanha e dos Estados Unidos, e exigiram talentos científicos, matemáticos, tecnológicos e de engenharia além das delicadas artes do lápis e papel dos peritos empregados na Primeira Guerra Mundial. As autoridades militares da Alemanha se voltaram para uma invenção conhecida como "rotor de cifra", uma máquina de escrever que trabalhava com base num sistema de "substituição"mecânica.

2.7.1 A Enigma

Figura 13 - A Enigma

Fonte: Adaptado de www.gta.ufrj.com.br

A enigma parecia uma máquina de escrever de cerca de $30,5$ centímetros quadrados, $15,2$ centímetros de altura e pesando $3,6$ quilos. Fora desenvolvido por um engenheiro elétrico alemão, Arthur Scherbius, para uso no comércio, na diplomacia e potencialmente para uso militar. Foi denominada Enigma, palavra grega. Descrevendo a máquina para a Marinha Imperial alemã em 1918, Scherbius, então com trinta e nove anos e vivendo em Berlim, gabara-se de que ela "evitaria qualquer repetição da sequência de letras ainda que a mesma letra fosse batida milhões de vezes".

A solução de um telegrama é também impossível se uma máquina cair em mãos não autorizadas, pois exige um sistema de chaves pré-combinado". A criação de uma cifra com uma máquina de rotor do tipo que evoluiu para a Enigma envolve bater as teclas de uma máquina de escrever correspondentes às letras da mensagem, ou o "texto simples", e anotar o "texto cifrado", as sucessivas letras que se acendem numa tela de vidro. Quando cada letra é cifrada, a corrente elétrica passa pelo contato da placa de entrada dessa letra, entra no rotor no contato oposto a este, gira pelo rotor, sai numa posição diferente na outra face, passa para a placa de saída e vai para a lâmpada embaixo da letra de texto cifrado. O recebedor da mensagem em código tinha de preparar a máquina com as mesmas coordenadas do sistema de chaves para recuperar o texto simples original. O equipamento Enigma padrão usado pelas forças armadas alemãs incluía cinco rotores, dos quais três eram escolhidos na preparação da máquina para cada período (normalmente um dia), dando sessenta possíveis ordens de engrenagens.

Cada rotor era equipado com um anel ajustável com as vinte e seis letras do alfabeto nele inscritas. Havia, portanto, vinte e seis elevado ao cubo, ou seja, 17.576, diferentes configura-

ções desses anéis, dando pouco mais de 1 milhão de possíveis posições da "unidade embaralhadora"no núcleo da máquina. Mas a máquina também incluía um painel de plugues, que efetuava uma substituição antes da corrente entrar no embaralhador e a mesma substituição depois que ela a deixava para acender a letra cifrada.

A substituição produzida pelo próprio embaralhador era simétrica e usada na entrada e na saída, preservava as duas características críticas do componente embaralhador de codificação da Enigma: nenhuma letra podia ser cifrada como ela própria, e a codificação geral era recíproca: se W era cifrado para P, P era cifrado para W. O uso de 10 pares plugados introduzia um fator extra de cerca de 150 bilhões, levando o número total de diferentes formas de configurar a máquina a aproximadamente 159 trilhões. A configuração escolhida cada dia era distribuída para todos os usuários em cada rede particular, em geral como uma folha de chaves mensal.

Além disso, o ponto de partida para cada mensagem individual tinha de ser escolhido pelo originador, e comunicado ao recebedor, sem revelá-la ao inimigo. Essa informação era transmitida de várias formas por diferentes usuários e em diferentes fases do conflito. Durante a maior parte da guerra, o exército e a força aérea usaram um método simples, isto é, cifrar a posição de partida (digamos DQX) na máquina numa posição de partida (digamos RTG) também escolhida pelo operador. Se DQX era cifrado para KLB, os trigramas RTG KLB eram enviados como parte do preâmbulo da mensagem. O recebedor tinha apenas de configurar sua máquina para a posição RTG e bater KLB, revelando a posição de partida DQX da mensagem propriamente dita. Assim, se o inimigo soubesse a configuração da máquina para o período em questão, poderia decifrar qualquer mensagem nela enviada.Em 1929 Scherbius vendeu sua invenção ao exército e à marinha alemães, que iriam usar diferentes versões da Enigma.

Com a subida de Hitler ao poder em 1933, e sua rejeição do Tratado de Versalhes com as proibições de rearmamento alemão, a demanda de máquinas de código pelas forças armadas multiplicou-se. No fim, a Luftwaffe, a SS, a Abwehr (inteligência e contra-inteligência militares alemãs) e as ferrovias do Estado (a Reichsbahn) todas estavam usando maquinas Enigma, e o exército e a marinha coordenavam seus sistemas Enigma com vistas a maior segurança. O alto comando alemão acrescentou um sistema de segurança à prova de falhas com a ajuda de um Stichwort, uma palavra indicadora. Mesmo que o inimigo conseguisse obter uma máquina Enigma, e também as listas de chaves diárias, a transmissão do Stichwort para submarinos em operação orientava os operadores a abrir um envelope lacrado no qual uma tira de papel continha a palavra-chave. Os operadores seguiam então um complexo procedimento, acrescentando letras da palavra-chave à configuração especificada para a chave diária. Os alemães começaram a usar as máquinas Enigma em 1926, confundindo na mesma hora os decifradores de códigos

britânicos, franceses e americanos.

O único país que se recusou a aceitar que a nova codificação era indecifrável foi a Polônia. Acuado entre o gigante russo e uma Alemanha que se sentia roubada de território devolvido à Polônia após a Primeira Guerra Mundial, o governo polonês estava convencido de que não podia se dar o luxo de ignorar as intenções secretas da Alemanha. O Capitão Maksymilian Cieski era o encarregado do departamento de códigos polonês, o Biuro Szyfrów. Estava familiarizado com a Enigma comercial, o que se mostraria útil em longo prazo, mas a máquina empregada pelos militares alemães era diferente na fiação dos embaralhadores. O Biuro teve um golpe de sorte, porém, como resultado da espionagem de um alemão insatisfeito, Hans Thilo Schmidt, que passou cópias dos livros de código e configurações para o serviço secreto francês, que por sua vez os passou para seus aliados poloneses, e daí para o departamento de códigos polonês. A traição de Schmidt possibilitou aos poloneses projetarem uma máquina Enigma, mas os criptoanalistas tinham agora de decifrar as configurações.

2.7.2 Desvendando a enigma

A criptoanálise era uma tarefa tradicionalmente direcionada a classicistas e linguistas. Em vista da complexidade mecânica da Enigma, o departamento de códigos polonês decidiu voltar-se para os matemáticos, e entre seus primeiros recrutas, em 1929, estava Marian Rejewski, de 24 anos, ele se concentrou nos padrões da "chave da mensagem". Após um laborioso processo de verificação de cada uma das 105.456 "configurações de embaralhamento", que levou um ano, Rejewski finalmente começou a desvendar no mistério da cifra da Enigma. O ataque de Rejewski à Enigma é um dos maiores feitos da história da Criptografia.

Medo, matemática e espionagem foram os fatores preponderantes na motivação e sucesso dos poloneses para a quebra da Enigma. Porém com a guerra os alemães aperfeiçoaram a Enigma, pois Blitskreig de Hitler dependia de comunicações entre ar, blindados e infantaria. Os alemães aumentaram o número de cabos do painel de plugues de seis para dez, o que elevou o número de chaves, o que aumentou subitamente a segurança da Enigma.

O esforço polonês contra a Enigma não pode evitar que aquela nação se tornaria a primeira vítima da Segunda Guerra Mundial. Semanas antes do início da guerra o serviço secreto francês combinou um encontro dos criptoanalistas britânicos com Rejewski e sua equipe do departamento de códigos polonês. A história da quebra do código da Enigma durante a Segunda Guerra Mundial, e dos 12 mil criptoanalistas que acabaram trabalhando em Bletchley Park, na zona rural da Inglaterra, foi uma operação extraordináriamente centralizada, sobre a qual Churchill mantinha um olho atento, resolvendo admiravelmente problemas de redução de recursos

com um ressonante memorando em que ordenava AÇÃO HOJE.

A ferocidade de Hitler ambicionada por uma rápida guerra de agressão, as rivalidades expuseram muitas áreas de negligência na defesa, haviam sete organizações de decifração de códigos no Reich, ao todo seis mil pessoas trabalhando em criptoanálise, mas espalhadas pelas diferentes organizações. Os britânicos e americanos, que também investiam fortemente na criptografia, conseguiram desenvolver um sistema de codificação baseado no modelo Enigma, que era conhecida como Typex ou Type-X. As duas máquinas eram complexos sistemas de substituição e soma utilizando um sistema de cinco rotores.

A difusão das codificadoras chegou a tal ponto que tanques e aviões individuais carregavam uma "Enigma"à bordo. Excesso de tráfego, procedimentos operacionais inadequados, operadores precariamente treinados, e a crença arrogante alemã na superioridade de seus codigos: combinados com o presente inestimável dado pela Polônia, acabaram sendo uma benção dos céus para os decodificadores aliados. A quebra dos impenetráveis códigos alemães acabaria por envolver a Grã-Bretanha na construção do Colossus, o primeiro computador do mundo, e uma equipe gigantesca, incluindo a nata dos matemáticos britânicos, aproveitando a experiência adquirida na quebra da "Enigma"contra um alvo muito mais difícil: a Lorenz, uma máquina de teletipo de códigos binários e um sistema eletromecânico de embalhamento, usada nas comunicações do Alto Comando Alemão.

2.8 Linha do Tempo

- (480a.C) - Conflitos entre Grécia e Pérsia- Utilização da Estenografia, processo de ocultação da mensagem para garantir a transmissão segura.
- (58a.C) - Código de César- cifra de substituição monoalfabética. Utilizada para diversos fins, militares como o caso de César ou comerciais como os árabes. Quebrada pela análise de frequência.
- (1500) - Cifra de Substituição Polialfabética - Quadrado de Vigenère - utilização de aparatos de criptografar
- (1630)- Cifra de Substituição Homofônica - com a dificuldade de se implementar a cifra de substituição polialfabética a cifra de substituição homofônica é um aperfeiçoamento da cifra de substituição monoalfabética.
- (1700) - Industrialização da criptoanálise - enfraquecimento da cifra de substituição monoalfabética.

- (1839)- O nascimento do telégrafo propiciou rapidez na proteção das informações o que fortaleceu a utilização da cifra polialfabética.
- (1863) - Kasisk publica uma forma de quebrar a cifra polialfabética.
- (1918) - Março de 1918 - Cifra ADFGVX, com o rádio surgiu a facilidade de comunicação mas também a facilidade de interceptação, houve a necessidade de uma cifra mais segura. A cifra ADFGVX é um misto de cifra de transposição e substituição.
- (1918) - Junho de 1918 - A cifra ADFGVX é quebrada. A criptografia é uma arma de guerra, os criptoanalistas se multiplicam para vencer essa batalha. Várias outras cifras surgem, mas são todas fundamentadas nas cifras de séculos anteriores. Surge então o Santo Graal da da criptografia, o Bloco de Cifras, mas é inviabilizado pela barreira tecnológica.
- (1925) - A máquina Enigma é adotada na guerra. Nos anos seguintes máquinas similares a Enigma foram inventadas. A criptografia estava sendo mecanizada, foram criadas máquinas para codificar e também máquinas decodificadoras.
- (1943) - Máquina Colossus - projetada para quebrar a Cifra de Lorenz utilizada por Hitler, é um computador programável, precursor dos computadores digitais.
- (1976) - A era computacional já é uma realidade, ainda para poucos. A criptografia torna-se relevante em várias dimensões. Adota-se a DES (Data Encryption Standart). Um padrão americano de cifragem, o que também demandava a criação de um outro sistema de distribuição de chaves. Neste mesmo ano foi proposto por Diffie, Hellmam e Merkle o conceito de cifra assimétrica.
- (1977) - Criptografia de chave pública - Criptografia RSA
- (????) - Criptografia Quântica - Já é uma realidade ou apenas uma teoria?

3 MODELAGEM MATEMÁTICA E A CRIPTOGRAFIA

Segurança em redes, espionagem, quebra de códigos, a todo momento no noticiário nos deparamos com notícias a respeito de espionagem que envolvem segredos comerciais de grandes corporações, segredos e informações confidenciais de estado. Vários filmes de Hollywood que facinam o público com o desenrolar de estórias baseadas em códigos secretos. Todos estes tópicos são conceitos que aparecem de forma recorrente em criptografia.

Algo que disperta o interesse em pessoas de diferentes formações e gerações. Um típico exemplo relevante como a aplicação da matemática pode contrubir em seguranças em redes, em transações bancárias, dentre outras formas.

Alguns métodos criptográficos modernos são acessíveis a alunos do ensino fundamental e médio, como veremos ao longo desta monografia.

Chamamos atenção, que o desenvolvimento desta temática a nível de ensino médio, também poderia contribuir para o desenvolvimento de fundamentos básicos da computação, tais como o desenvolvimento de algorítmos, mesmo de forma simples, em plataformas computacionais voltadas a alunos de ensino médio. A elaboração destes algorítmos criptogáficos e protocolos, colaboraria para o aluno estabelecer a interface entre a ciência da computação e a matemática. Se levarmos a aspectos históricos, os alunos teriam a noção de que a própria ciência da computação, teve seu germe embrionário na matemática. Convém lembrar que o cientista que é considerado o pai da computação, foi um matemático britânico Alan Turing (1912-1954) que formalizou os conceitos de algoritmos e computação com a chamada máquina de Turing, que é considerado o primeiro modelo teórico proposto de um computador, o que levou aos aos modernos computadores eletrônicos dos dias de hoje.Também foi um dos grandes responsáveis pela quebra do código dos nazistas decifrando importantes mensagens enviadas pela máquina Enigma junto com a sua equipe no Bletchley Park.

Dada a crescente demanda por sistemas de comunicação mais rápidos, principalmente com o aumento do tráfego de informações, também aumenta a demanda pela segurança da informação. Basta observar a relevância de tudo isto na vida moderna, por meio, das transações bancárias realizadas de forma online, correspondências via correio eletrônico, acesso as mídias eletrônicas e a proteção de informações pessoais.

Esta demanda tecnológica destes últimos tempos, requer uma nova formação e uma nova

preparação de professores do ensino médio se comparados com um prazo curto de tempo de menos de vinte anos com novas habilidades.

Parte destas novas habilidades e competências, acreditamos que podem ser realizadas e abordadas na aplicação da criptografia em contexto de ensino fundamental e médio.

Um aprendizado objetivo dentre este tópico junto aos alunos do ensino fundamental e médio seria:

- Sensibilizar os alunos do ensino médio para questões voltadas para a segurança em redes, especialmente levar a seu conhecimento que o tráfico de informação na rede mundial de computadores é frequentemente monitorada e que não é segura.
- E saber que uma consequência direta da observação anterior é a necessidade do desenvolvimento de técnicas seguras de encriptação de mensagens, e o conhecimento de que precisamos identificar os participantes em um sistema de comunicação.

Chamamos a atenção que como parte de tópicos da criptografia podem ser explorados em diferentes níveis de ensino, seja, no ensino fundamental ou médio.

Aplicações da criptográfia clássica, as cifras de substituição como a de César e a de Vigènер que poderem serem realizadas já a nível de ensino fundamental, uma vez que envolvem conceitos de arranjos e combinatória.

Aplicações da criptográfia que envolvam a utilização de computadores, em particular, o uso de algorítmos e o sistema criptográfico RSA podem ser como exemplo tópicos a serem aborados no ensino médio.

Claro que alunos e mesmo alguns profissionais com formação em matemática, porém leigos na temática poderiam indagar como ciência, se a criptografia poderia ser considerada como parte da matemática. Para isto, basta que mostremos e verifiquemos que tal ciência baseia-se em métodos matemáticos tanto para codificar/encriptar mensagens quanto para decodificar/decifrar mensagens. Como vimos no capítulo histórico, no íncio da criptografia, apenas para nível de comparação a partir do código de César, o desenvolvimentos das cifras de substituição não eram realizada por matemáticos. Apenas a partir do século XX, com o advento das duas grandes guerras, que os departamentos de defesas de vários países começaram a utilizar matemáticos, tanto na criação dos sitemas criptográficos quanto nos criptoanalista.

Embora, desde o princípio, como vimos na parte histórica deste texto a quebra dos códigos sempre esteve de uma certa forma ligada a análise de frequência e de ciclos que se repetiam.

Principalmente, durante a segunda gerra mundial, a análise de frequência foi utilizada através de algoritmos matemáticos, como a quebra dos códigos dos japoneses pelos norte-americanos, e a quebra do códigos da máquina enigma dos alemães realizada pelos ingleses.

Se considerarmos os dias de hoje, o sistema criptográfico utilizado pelas grandes corporações econômicas é feito via o sistema criptográfico RSA. Predominantemente, é realizado com ferramentas matemática que pode ser desenvolvida no ensino médio. Em particular, parte do princípio do sistema criptográfico *RSA*, a encriptação, é dada pelo produto de dois números primos muito grandes da forma $n = pq$. Logo, a tarefa do criptanálista ao conferir o número n é procurar fatorá-lo, desde que descubra quem são os números p e q, a sua tarefa estará terminada.

A idéia por trás do problema é bem simples, mas a segurança do metódo está na barreira tecnológica para se realizar esta tarefa.

Logo, trata-se de uma motivação para estudar os números primos mais a fundo, e como seria interessante uma maneira prática de gerar números primos. Assim, teríamos que contribuir com os criptográfos na listagem de primos a seu dispor para realizar a encriptação.

Um dos primeiros questionamentos seria quantos números primos existem. Se for uma quantidade finita, um momento vai acabar, o que poderia comprometer o método. Daria para discutir e até provar, já que não é tão difícil que existem infinitos primos distribuídos na reta.

Surgiria outras questões como encontrá-los. Porém, para poder encontrá-los, seria interessante, como se dá sua distribuição na reta. Surgiria, uma outra questão, sua distribuição é uniforme na reta? Caso não seja é possível estimar do ponto de vista probalístico a distrubuição de primos na reta? Todos estas perguntas, poderiam ser motivações para discutir com alunos questões relacionados com a função de Euler, a distribuição dos números primos na reta, os testes de primalidade, entre outras.

Uma outra vantagem de se abordar o estudo da criptográfia no ensino médio, em particular, o sistema criptográfico RSA, é a possibilidade, de mostrar aos aluno que a matemática não é uma ciência acabada, mas sim, que existe ainda muita pesquisa a ser realizada. Ou melhor, é possível introduzir ao aluno de forma clara e acessível a sua formação que existem problemas em abertos em matemática. Em particular, problemas de teoria dos números poderiam ser incluídos, do tipo:

1. Os números primos gêmeos são aqueles números primos com diferença igual a 2, por exemplo, 3 e 5, 11 e 13. Podemos afirmar que existem infinitos primos gêmeos?

2. Existem números primos entre os inteiros n^2 e $(n+1)^2$?

3. Existem uma maneira eficiente de se fatorar números primos muito grandes?

A terceira questão, em um primeiro momento poderia ser discutida de forma experimental, utizando as propriedades do ensino médio, o que levaria ao aluno perceber que este método tem limitações, funcionando bem para números inteiros pequenos. Já para número grandes necessitaria buscar métodos computacionais. Este é o germe da idéia do sistema *RSA*. Considera-se uma função do tipo E dada por $E(x) = x^e \pmod{n}$, onde e e n são números naturais e n é um número muito grande. Esta função é invertível, porém, muito de difícil de ser realizada. Na prática, para que ela possa encontrar a sua inversa, necessitamos encontrar uma congruência dada na forma $c = x^e \pmod{n}$, mas para isto, precisa-se testar todos os valores inteiros de x variando entre $1, 2 \ldots, (n-1)$. Na prática, este método não é muito eficiente para problemas envolvendo números primos grandes módulo n. Os cálculos de x a partir de e e n é equivalente ao conhecimento dos fatores primos na decomposição n . Caso escolhamos um produto grande, primos obidos de forma secreta, a função não pode ser invertida de forma sem uma informação adicional. Tal fato é utilizado na contrução do sistema criptgráfico *RSA*.

A dificuldade e a falta de método eficiente de resolver o problema (3) representa a eficiência da segurança da função E.

Até há pouco mais de trinta anos a informação era encriptada da seguinte forma. A mensagem era codificada via uma função invertível E e a chave secreta K onde o texto era cifrado $C = E(M)$. A decodificação/decriptação da mensagem era realizado utilizando-se com a função inversa D tal que $D(M) = M$. A parâmetro K utilizado na construção de D e E devia ser enviado via um canal de segurança, envolvendo na maioria das vezes pessoas estranhas. Se imaginarmos os comércios online das dias de hoje, na rede mundial de computadores, não é um canal de comunicação seguro para que utilize procedimentos desta natureza.

A crescente utilização da computação nos dias de hoje fez com que aplicação da criptográfica torna-se crucial para o desenvolvimento.

Como vimos na parte histórica desta monografia até um pouco mais de meados do século XX, o desenvolvimento da criptográfia sempre esteve ligado a proteção de informação envolvendo questões de secredos militares ou segredos de estado.

Mas, hoje com a crescente demanda pelo tráfego de informações em sistemas que envolvem redes de comunicação com fio ou sem fio, representa um desafio cada vez maior, a segurança destes novos meios de informação precisam acompanhar esta evolução tecnológica desenvolvendo métodos matemáticos eficazes para a sua segurança.

4 ARITMÉTICA MODULAR

A relevância da Aritmética Modular na criptografia ocorre devido à sua característica de não possuir padrões em seus resultados, o que dificultaria a análise. Em outras palavras, na criptografia podemos definir o processo de encriptação como uma função e basta aplicarmos a função inversa para decodificar a mensagem. Dessa forma temos uma função de mão dupla, que é reversível.

Por exemplo, no caso da Cifra de César temos um deslocamento de 3 casas do alfabeto original. Para decodificar uma mensagem com essa cifra basta aplicar o processo inverso. No entanto, com a evolução da criptoanálise, tornou-se necessário uma maior segurança das informações. Com os computadores as mensagens codificadas eram facilmente decodificadas, assim sendo os matemáticos iniciaram uma busca por funções que satisfizessem essas necessidades, devendo ser funções de mão única, uma função fácil de fazer e difícil de desfazer.

A aritmética modular é um campo da matemática rico em funções de mão única. Por exemplo, se estamos trabalhando com uma função crescente na aritmética normal, quando aumentamos o valor de x o valor da função também aumenta, mas na aritmética modular não podemos realizar este tipo de relação o que dificulta reverter o processo sem conhecer a função original. Dessa forma abordaremos alguns fundamentos matemáticos para desenvolver esse tema.

4.1 Relações de Equivalência

A relação de equivalência entre elementos de um conjunto estabelece uma relação que satisfaz a mesma propriedade entre dois elementos de um conjunto. Uma relação de equivalência em um conjunto A, tal que $x, y, z \in A$, satisfaz as seguintes propriedades:

1. $x \sim x$
2. Se $x \sim y$ então $y \sim x$
3. Se $x \sim y$ e $y \sim z$ então $x \sim z$

A primeira propriedade se chama reflexiva e é a relação de um número com sí próprio. Essa propriedade nos diz que quando comparamos um número com ele mesmo as mesmas

propriedades são satisfeitas, mas devemos ter cautela. pois não é porque estamos comparando o mesmo número que esta propriedade será sempre satisfeita. Suponhamos que fosse verificar a relação de estritamente maior($>$), neste caso teríamos que esta propriedade não seria satisfeita.

A segunda propriedade é conhecida como simétrica. Nela podemos citar o mesmo exemplo da primeira como sendo uma relação que não satisfaz a propriedade. Podemos dizer que $14 > 10$, mas não podemos dizer que $10 > 14$, logo, a propriedade não é satisfeita uma relação de equivalência.

A terceira propriedade é conhecida como transitiva. Podemos observar que nela a relação citada acima é satisfeita, então um exemplo que podemos dar onde a relação não é satisfeita é a relação de $\neq$(diferente), pois podemos ter $15 \neq 17$ e $17 \neq 15$, mas $15 = 15$, mostrando que a propriedade não foi satisfeita.

As relações de equivalência são fundamentais para classificar os elementos quanto as suas propriedades, ou seja, elementos que possuem a mesma propriedade dentro de um conjunto formam um subconjunto de elementos que estão na mesma classe de equivalência. Consideremos um conjunto X, a relação de equivalência $\sim$ e $x \in X$. A classe de equivalência de x é o conjunto de elementos de X que equivalem a x por $\sim$. Chamaremos este conjunto de $\overline{x}$, é representado por:

$$\overline{x} = \{y \in X : y \sim x\}.$$

Existe uma propriedade das classes de equivalência tão importante que chega a ser considerada um princípio: *qualquer elemento de uma classe de equivalência é um representante da classe toda*, ou seja, necessitamos saber um único elemento da classe para que possamos construí-la toda.

Segundo o príncipio acima, temos que se y pertence a classe de x, suas classes serão iguais, ou seja, se $x \in X$ e $y \in \overline{x}$ então $\overline{x} = \overline{y}$.

Consideremos agora, as propriedades de X com a relação $\sim$:

1. X é a união de todas as classes de equivalência.
2. Duas classes de equivalência distintas não podem ter um elemento em comum.

A primeira propriedade pode ser provada pelo fato de que cada elemento pertence a sua classe de equivalência e a segunda decorre do princípio citado acima.

4.2 Inteiros Módulo *n*

Consideraremos um inteiro positivo n da qual chamaremos de módulo ou período, construiremos, então, uma relação de equivalência nos inteiros de tal forma que a cada valor n que somarmos todos os valores encontrados serão equivalentes entre sí seriam os números cuja diferença resultaria em um múltiplo de n, ou seja , consideremos dois inteiros a e b, estes serão congruentes entre sí caso $a-b$ for múltiplo de n. Usamos a notação a seguir para descrever esta relação:

$$a \equiv b \pmod{n}.$$

Esta relação é utilizada no cotidiano das pessoas, no entanto sem a sua referência matemática a aritmética modular. Uma das características da aritmética modular é descrever fenômenos cíclicos, dessa forma ela também é conhecida como aritmética do relógio. Sendo assim as pessoas realizam esse tipo de relação quando tratam da hora, por exemplo, o dia é composto de 24 horas, no entanto o relógio é uma circunferência subdividida em 12 partes, dessa forma tomemos o 12 como período ou módulo, podemos construir uma relação de equivalência. Por exemplo consideremos dois inteiros 3 e 15, estes serão congruentes entre si caso $15-3$ for multiplo de 12. Assim temos que:

$$15 \equiv 3 \pmod{12}.$$

Isso significa que 15 é congruente a 3 em módulo 12. Como módulo 12 está se referindo a horas, então significa dizer que 15 horas corresponde a 3 horas. A relação de equivalência deve satisfazer a três propriedades citadas anteriormente, portanto, devemos demonstrá-las. Tomemos novamente a sua forma generalizada:

$$a \equiv b \pmod{n}.$$

A primeira propriedade não é dificil de verificar, pois teremos:

$$a \equiv a \pmod{n}.$$

Esta propriedade não é dificil de provar, pois para que ela seja verdadeira, basta provarmos que $a-a$ seja múltiplo de n, mas como $a-a=0$, temos que a afirmação é verdadeira.

Para a segunda propriedade, teremos:

$$a \equiv b \pmod{n} \quad \textit{então,} \quad b \equiv a \pmod{n}$$

Disto temos que $a-b$ é múltiplo de n, mas como $b-a=-(a-b)$, temos que $b-a$ é múltiplo de n, portanto $b \equiv a \pmod{n}$.

Para a terceira propriedade teremos:

$$a \equiv b \pmod{n} \quad e \quad b \equiv c \pmod{n}.$$

Da primeira expressão temos que $a-b$ é múltiplo de n e da segunda expressão temos que $b-c$ é múltiplo de n, ao somarmos múltiplo de n teremos um novo múltiplo, teremos então:

$(a-b)+(b-c)=a-c$, que é igual a $\quad a \equiv c \pmod{n}$.

Dessa forma as três propriedades estão satisfeitas e, portanto, concluímos que a congruência módulo n é uma relação de equivalência.

Tomemos agora o conjunto $\mathbb{Z}$ pela relação de congruência módulo n, cuja notação é dada da forma $\mathbb{Z}_n$ e é denominado conjunto dos inteiros módulo n. Note que $\mathbb{Z}_n$ é um subconjunto de $\mathbb{Z}$. Encontremos agora seus elementos.

Seja $a \in \mathbb{Z}$, a classe de a é dada pelos $b \in \mathbb{Z}$ de tal forma que $b-a$ é múltiplo de n, ou seja $b-a=kn$, com $k \in \mathbb{Z}$, então podemos escrever este subconjunto de $\mathbb{Z}$ na forma:

$$\overline{a} = \{a+kn : k \in \mathbb{Z}\}.$$

É importante destacar uma classe específica. A classe $\overline{0}$ representa a classe dos números múltiplos de n. Em uma situação de extrema importância, consideremos $a \in \mathbb{Z}$ e o dividimos

por n, obtendo q e r inteiros da forma:

$$a = nq + r \quad e \quad 0 \leq r \leq n-1.$$

Disto temos que $a - r = nq$, ou seja $a - r$ é múltiplo de n, logo $a \equiv r \pmod{n}$. Deste cálculo podemos observar que os representantes de classes de $\mathbb{Z}_n$ variam de 0 a $n-1$.

Retomemos o funcionamento do relógio, percebemos que seu ponteiro sai de uma determinada posição x e, ao passar 12 horas, ele irá parar em uma posição y e que será a mesma posição em que x estava, ou seja, $y \sim x$, este fenômeno ocorrerá a cada 12 horas para qualquer posição do ponteiro, portanto, neste caso, temos o conjunto $\mathbb{Z}_{12}$, cujos valores inteiros do relógio vão de 1 até 12, mas como 12 é múltiplo de 12, o consideraremos como sendo da classe $\overline{0}$, portanto teremos que o relógio terá posição inicial no 0, e terá posição final no número 11, que é o nosso $n-1$. Tendo todos estes dados em mente, e mais o fato que o movimento relizado pelo ponteiro é uma circunferência, podemos concluir que o conjunto $\mathbb{Z}_n$ pode ser representada como uma circunferência que tem início no $\overline{0}$ e fim na classe $\overline{n-1}$.

4.3 Aritmética Modular

Para realizarmos a aritmética modular em $\mathbb{Z}_n$, imaginemos que possuímos um relógio de n horas com um ponteiro fixado em seu centro, de acordo com o que vimos anteriormente, teremos uma circunferência com números que pertencem a classe $\overline{0}$ até a classe $\overline{n-1}$.

Caso desejemos somar dois valores $\overline{a}$ e $\overline{b}$, de acordo com o procedimento adotado anteriormente, basta colocarmos o ponteiro em $\overline{a}$ e ao andarmos b posições encontraremos o resultado desejado. Consideremos o conjunto $\mathbb{Z}_{12}$, se formos somar $\overline{8}$ e $\overline{11}$ neste conjunto, temos então, que o ponteiro iniciará em $\overline{8}$ e teremos que andar $\overline{11}$, mas notamos que após andarmos duas casas, estaremos na classe $\overline{0}$ e, portanto, reiniciamos nossa contagem e o ponteiro irá parar na casa da classe $\overline{7}$, ou seja, temos que $\overline{8} + \overline{11} = \overline{7}$ em $\mathbb{Z}_{12}$.

Tendo como base a ilustração acima, podemos caracterizá-la em um caso mais geral, que será realizado da seguinte forma:

$$\overline{a} + \overline{b} = \overline{a+b}.$$

A esquerda temos algo que não sabemos realizar, a soma de classes, mas notamos que a di-

reita da igualdade está algo que realizamos diariamente, uma soma comum, mas que deveremos classificá-la em uma classe, o que não é diferente de tudo o que já realizamos.

Existe a possibilidade de que as classes não resultem no mesmo valor, neste caso temos que $\overline{a+b}$ estará resultando em um valor maior que n e portanto devemos subtrair n e desta forma teremos o mesmo resultado.

Algo importante que devemos destacar também é o fato de que não importa quais representantes das classes tomemos para realizar a operação que resultaremos sempre na mesma classe. Vamos provar esta afirmação.

Consideremos duas classes $\overline{a}$ e $\overline{b}$ e suponhamos $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Queremos verificar que $\overline{a+b} = \overline{a'+b'}$. Da igualdade $\overline{a} = \overline{a}'$, segue-se que $a - a'$ é múltiplo de n e o mesmo ocorre para a igualdade $\overline{b} = \overline{b'}$ e a soma de dois valores múltiplos de n resulta em um valor múltiplo de n. Portanto:

$$(a-a') + (b-b') = (a+b) - (a'+b')$$

e está feita a demonstração.

Para a multiplicação teremos uma prova bem similar,

$$\overline{a}.\overline{b} = \overline{ab}.$$

Suponhamos que temos $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$ e queremos mostrar que $\overline{ab} = \overline{a'b'}$. Como $\overline{a} = \overline{a'}$ temos $a - a'$, que é múltiplo de n, ou seja, podemos escrevê-lo da forma $a = a' + rn$ e com uma argumentação análoga de $\overline{a} = \overline{a'}$, obtemos de $\overline{b} = \overline{b'}$ que $b = b' + sn$. Realizando a multiplicação, teremos:

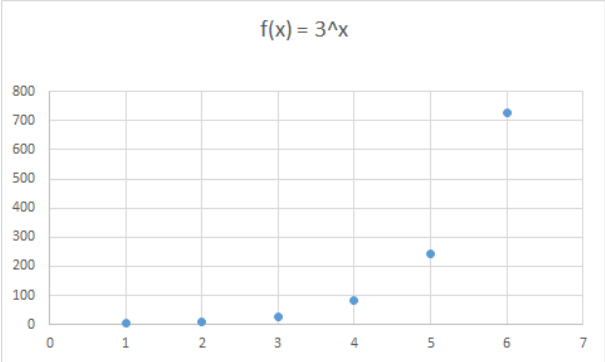
$$ab = (a'+rn)(b'+sn) = a'b' + (a's + rb' + srn)n.$$

Logo, $ab - a'b'$ é múltiplo de n o que mostra que a operação multiplicativa em $\mathbb{Z}_n$ está bem definida.

Na aritmética modular as funções não se comportam de modo sensato, e é essa a sua grande contribuição para a criptografia. Tomemos uma função por exemplo, $f(x) = 3^x$, temos que:

Tabela 3 - Análise do comportamento da função

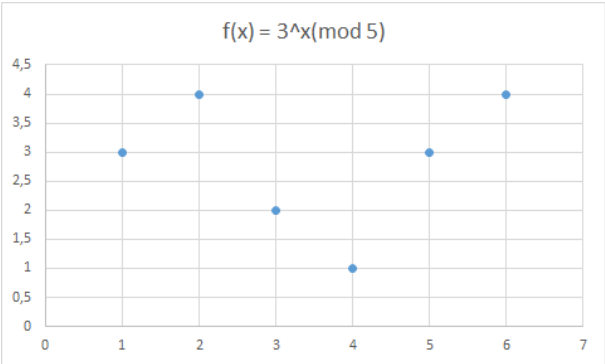
x	1	2	3	4	5	6
3^x	3	9	27	81	243	729



Observando a função descrita acima, notamos que conforme o valor de x aumenta a função também aumenta continuamente. Introduziremos agora uma função modular $f(x) = 3^x (mod\ 5)$.

Tabela 4 - Análise dao comportamento da função modular

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x (mod\ 5)$	3	4	2	1	3	4



Observando o comportamento da função modular, podemos concluir que não é possível estabelecer nenhuma relação, é apenas observável a ciclicidade dos resultados o que torna difícil estabelecer o seu correspondente. Essa dificuldade de reverter o processo é de fundamental importância para a criptografia.

4.4 Função φ de Euler

A função φ de Euler é uma forma generalizada do **Pequeno Teorema de Fermat**. Em Teoria dos Grupos a função φ de Euler é interpretada como a quantidade de elementos que possuem inverso multiplicativo em $\mathbb{Z}_n^*$.

Definição : Seja $n \geq 1$, $n \in N$. Então $\varphi(n)$ é a quantidade de inteiros a, $1 \leq a \leq n$, tais que $mdc(a,n) = 1$.

Dessa forma , se p é primo então:

- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

As sentenças acima se justificam pelo fato de que existem p^{k-1} inteiros positivos menores que p^k que são divisíveis por p. Ainda temos que a função φ é uma função multiplicativa, isto é, se $m,n \geq 1$ e $mdc(m,n) = 1$, então $\varphi(mn) = \varphi(m).\varphi(n)$. Dessa forma tem-se uma fórmula pra calcular os valores da função de Euler para números compostos.

Teorema 1. *Teorema de Euler: Seja n > 0, a, n ∈ Z. Se mdc(a,n) = 1, então* $a^{\varphi(n)} \equiv 1(mod\ n)$.

Demonstração: Seja $r = \varphi(n)$ e sejam $b_1, b_2, ..., b_r$, inteiros, dois a dois não côngruos módulo n, tais que $mdc(b_i, n) = 1$. para $i = 1, ..., r$. Têm-se então que $ab_1, ab_2, ...ab_r$, são ainda, dois a dois não côngruos módulo n e $mdc(ab_i, n) = 1$, para $i = 1, ..., r$. Dessa forma, os conjuntos $b_1(mod\ n), ..., b_r(mod\ n)$ e $ab_1(mod\ n), ..., ab_r(mod\ n)$ são iguais. Então:

- $a^r \prod_{i=1}^r b_i \equiv \prod_{i=1}^r ab_i \equiv \prod_{i=1}^r b_i (mod\ n)$

  Dessa forma,

- $(a^r - 1) \prod_{i=1}^r b_i \equiv 0(mod\ n)$

  Concluímos que $a^r \equiv 1(mod\ n)$

Note que no teorema de Fermat é necessário que p seja primo e não divida a para que $a^{p-1} \equiv 1(mod\ p)$. Já no Teorema de Euler basta que a e n sejam primos entre si para que $a^{\varphi(n)} \equiv 1(mod\ n)$, ainda se $n = p$ for primo, então $\varphi(p) = p - 1$.

5 PROPOSTA DO ENSINO DA CRIPTOGRAFIA NO ENSINO BÁSICO

5.1 Fundamentos Matemáticos para o desenvolvimento da criptografia

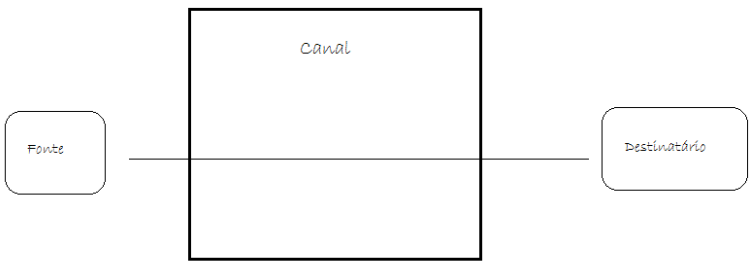
O objetivo desse trabalho é associar a criptografia com alguns tópicos do ensino da matemática. Para isto é necessário elencarmos alguns conceitos e teorias que precedem o desenvolvimento desse tema.

A criptografia é a arte de escrever em códigos de modo que apenas o destinatário consiga interpretar a mensagem ou os dados codificados. Então podemos dizer que a criptografia é um caso particular da Teoria dos Códigos que, além de ocultar a mensagem ou dados em códigos também tem fundamental importância a segurança da informação. Para este estudo discutiremos alguns fundamentos da Teoria dos Códigos.

5.2 Uma breve abordagem sobre Teoria dos Códigos

Como vimos ao longo do desenvolvimento histórico das técnicas da Criptografia, diferentes ferramentas matemáticas foram utilizadas. Porém o princípio básico é o de enviar informações de uma fonte a um destinatário.

Figura 14 - Fonte



Fonte:O próprio autor

A fonte pode ser caracterizada como um conjunto de informações. O canal é o meio fí-

sico em que é realizada a transmissão de informação. Mas no canal pode haver adversidades intrínsicas do canal denominadas ruído.

Nesse sentido a Teoria dos Códigos lança mão de procedimentos e ferramentas matemáticas que possam detectar e possivelmente corrigir erros que possam ocorrer na transmissão de informações.

Dessa forma há um mapeamento entre símbolos de informação da fonte nas palavras-códigos, e as palavras códigos são enviadas por meio do canal. A situação ideal (hipotéticamente o canal não introduziu erros) bastar realizar a decodificação no sistema de comunicação, assim o usuário obtém as informações transmitidas pela fonte.

A fonte é um conjunto finito onde as informações são elementos desse conjunto. O código também caracteriza um conjunto finito onde as palavras código são os elementos desse conjunto e a codificação que é o mapeamento realizado pelos elementos da fonte de informação nos códigos, palavras códigos, caracteriza uma função.

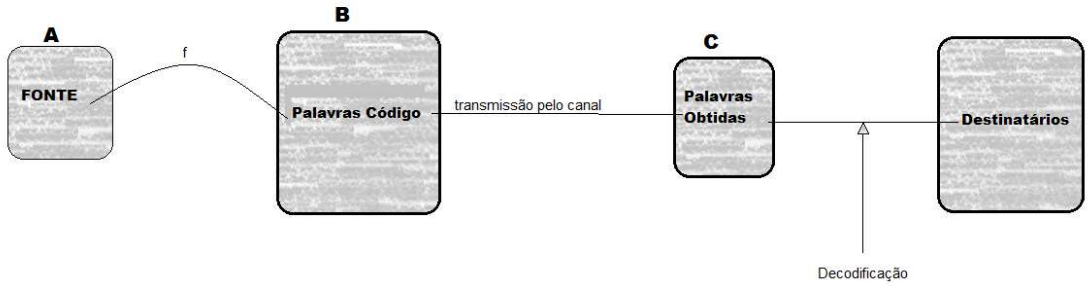
Sejam:

- **A** o conjunto que representa a fonte
- **B** o conjunto que representa o código
- **f** a codificação.

$$f : A \to B.$$

Cada palavra código é a imagem da informação, quando se refere ao caso ideal a decodificação em essência consiste em considerar a função inversa f^{-1}.

Figura 15 - Esquema



Fonte:O próprio autor

No caso ideal em que B=C, temos que:

$$A \xrightarrow{f} B \quad \text{e} \quad A \xleftarrow{f^{-1}} B$$

Repare que neste caso, discutimos conjuntos(finitos), função e uma função inversa, domínio e imagem da função. Este é um típico exemplo de modelagem matemática.

Na situação anterior é apenas discutido o caso ideal. Porém na prática isto não existe, na verdade o conjundo $B \neq C$

Para uma abordagem mais detalhada precisariamos estudar a Teoria de Códigos mais profundamente, que seria um bom tema para uma monografia.

Na Teoria dos Códigos, um código possui uma estrutura geométrica associada entre as palavras-código, considerando sempre a distância mínima. Assim, um código (n,k,d), tem:

n: comprimento da palavra código

k: dígitos da informação

d: a distância mínima

Um código (n,k,d) tem uma capacidade de correção de erros que depende da distância. Mas isto não é o objetivo do trabalho. O nosso objetivo é um sistema criptográfico , a cifra é um particular código e a chave é uma codificação.

Na criptografia interessa introduzir muita redundância e proteger a informação transmitida, onde novamente temos o conceito de função sendo utilizado.

Um código largamente utilizado na atualidade por aqueles que trabalham com tecnologia principalmente o desenvolvimento de software, é um código denominado ASCII que é a sigla de American Standard Code for Information Interchange, isto é, Código Padrão Americano para Troca de Informações que transforma caracteres alfabéticos ou não em números. Tomemos o código ASCII apenas para as letras maiúsculas.

Tabela 5 - Alfabeto em código ASCII

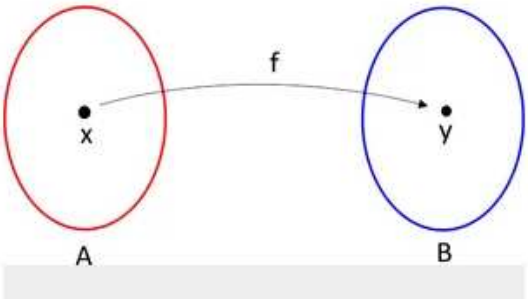
alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M
código ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77
alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
código ASCII	78	79	80	81	82	83	84	85	86	87	88	89	90

5.2.1 Função e Criptografia

Definição de Função

Dados dois conjuntos A e B não vazios, uma função f de A em B é uma relação que associa a cada elemento $x \in A$, um único elemento $y \in B$. Assim, uma função liga um elemento do domínio (conjunto A de valores de entrada) com um segundo conjunto, o contradomínio (conjunto B de valores de saída) de tal forma que a cada elemento do domínio está associado exatamente a um, e somente um, elemento do contradomínio. O conjunto dos elementos do contradomínio que são relacionados pela f a algum x do domínio é o conjunto imagem, denotado por Im(f).

Figura 16 - Representação dos conjuntos



Fonte:O próprio autor

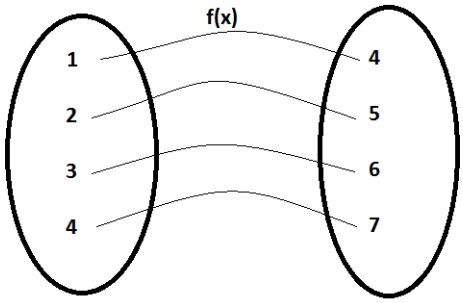
Sejam dois conjuntos $A = \{1,2,3,4\}$ e $B = \{4,5,6,7\}$ e f uma função que relaciona A e B

Tabela 6 - Alfabeto deslocado 3 casas

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

de modo que f é definido por $f(x) = x+3$. Assim temos:

Figura 17 - Função $f(x) = x+3$



Fonte:O próprio autor

Podemos utilizar os conceitos de função aplicado à criptografia para ressaltar a relevância dos dois temas. Estabelecendo uma aplicação prática do conceito e assim tornando o ensino desse tema mais interessante.

A criptografia pode ser considerada uma função bijetora, ou seja, todo elemento do domínio está relacionado com um elemento do contradomínio.

Então quando estudamos o código de César cuja relevância histórica já fora abordada, podemos concluir que o domínio e o contradomínio são compostos pelo alfabeto, e a função é a chave de deslocamento.

Sejam dois conjuntos $A = \{a,b,c,d,.....x,w,y,z\}$ e o conjunto $B = \{a,b,c,d,e,f,g,h,i,....\}$, tal que $x \in A$ e $f(x) \in B$, e f(x) seja definido pelo deslocamento de 3 casas.

5.2.2 Modelagem da Cifra de César

Associando a cifra de César ao código ASCII temos um sistema onde todos os caracteres do alfabeto tornam-se numéricos e podem ser facilmente processados computacionalmente. Mas

retomemos o objetivo inicial que é de identificar conceitos matemáticos fundamentais envolvidos nesses processos.

Seja A o conjunto finito cujos elementos são as representações numéricas do alfabeto.
Seja B um conjunto de mensagens a serem codificadas
Seja C um conjunto das mensagens codificadas
K = conjunto das chaves de codificação (1, 2, 3, 4,.....,25)
k_i é a chave de codificação

Logo,
$E : B \to C, f(x,k_1) = 65 + (x - 65 + k_1)(mod\ 26)$
$D : C \to B, g(x,k_2) = 65 + (x - 65 - k_2)(mod\ 26)$

Lembramos que a cifra de César é de chave simétrica, ou seja $k_1 = k_2$.
Segundo Signh(2002) "que César deslocava as letras em três casas, fica claro que, empregando-se qualquer deslocamento entre uma das 25 casas, é possível criar 25 códigos distintos". Para exemplificar vamos criptografar a palavra PROFMAT nesse sistema.

Tabela 7 - Codificando PROFMAT

		CODIFICAÇÃO		
Mensagem	Código ASCII	$65 + (x - 65 + k_1) mod 26$	Código Cifrado	Mensagem Cifrada
P	80	$65 + (80 - 65 + 3)(mod\ 26)$	83	S
R	82	$65 + (82 - 65 + 3)(mod\ 26)$	85	U
O	79	$65 + (79 - 65 + 3)(mod\ 26)$	82	R
F	70	$65 + (70 - 65 + 3)(mod\ 26)$	73	I
M	77	$65 + (77 - 65 + 3)(mod\ 26)$	80	P
A	65	$65 + (65 - 65 + 3)(mod\ 26)$	68	D
T	84	$65 + (84 - 65 + 3)(mod\ 26)$	87	W

Tabela 8 - Decodificando PROFMAT

		DECODIFICAÇÃO		
Mensagem Cif	Código Cif	$65 + (x - 65 - k_2) mod 26$	Código ASCII	Mensagem Original
S	83	65+(80 - 65 - 3)(mod 26)	80	P
U	85	65+(82 - 65 - 3)(mod 26)	82	R
R	82	65+(79 - 65 - 3)(mod 26)	79	O
I	73	65+(70 - 65 - 3)(mod 26)	70	F
P	80	65+(77 - 65 - 3)(mod 26)	77	M
D	68	65+(65 - 65 - 3)(mod 26)	65	A
W	87	65+(84 - 65 - 3)(mod 26)	84	T

5.2.3 Modelagem da Cifra de Vigenère

Utilizando o mesmo princípio da Cifra de César, Blaise Vigenère criou uma cifra que constituía em uma combinação de 26 deslocamentos do alfabeto original, no qual é necessário definir uma palavra chave codificar a mensagem. Vamos codificar a mensagem EDUCACAO*E*A*CHAVE utilizando como palavra chave PROFMAT. Primeiro vamos definir no quadro da cifra Vigenère quais deslocamento serão utilizados de acordo com a palavra chave.

Figura 18 - Quadrado de Vigenère PROFMAT

O quadrado de Vigenère

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

Fonte: Adaptado de o próprio autor

Modelando a Cifra de Vigenère com o código ASCII temos que:

Seja A o alfabeto em código ASCII.

Seja M o conjunto das mensagens a serem codificadas.

Seja C o conjunto de mensagens codificadas.

Seja K o conjunto das chaves de codificação e decodificação $(1,2,3,...,25)$.

$k_1, k_2, ...k_n$, são as chaves de codificação e decodificação.

Seja E a função de encriptação da mensagem de modo que:

$E : M^n \to C^n$

Seja D a função de decriptação da mensagem de modo que:

$D : C^n \to M^n$

Tabela 9 - Criptografando com a Cifra Vigenère - codificando

		CODIFICAÇÃO		
Mensagem	k^n	Sequência$65+(x-65+k_n)(mod\ 26)$	Código Cif.	Mensagem Cif.
E=69	P=15	65+(69 - 65 + 15)(mod 26)	84	T
D=68	R=17	65+(68 - 65 + 17)(mod 26)	85	U
U=85	O=14	65+(85 - 65 + 14)(mod 26)	73	I
C=67	F=05	65+(67 - 65 + 05)(mod 26)	72	H
A=65	M=12	65+(65 - 65 + 12)(mod 26)	77	M
C=67	A=26	65+(67 - 65 + 26)(mod 26)	67	C
A=65	T=19	65+(65 - 65 + 19)(mod 26)	84	T
O=79	P=15	65+(79 - 65 + 15)(mod 26)	68	D
E=69	R=17	65+(69 - 65 + 17)(mod 26)	86	V
A=65	O=14	65+(65 - 65 + 14)(mod 26)	79	O
C=67	F=05	65+(67 - 65 + 05)(mod 26)	72	H
H=72	M=12	65+(72 - 65 + 12)(mod 26)	84	T
A=65	A=26	65+(65 - 65 + 26)(mod 26)	65	A
V=86	T=19	65+(86 - 65 + 19)(mod 26)	79	O
E=69	P=15	65+(69 - 65 + 15)(mod 26)	84	T

Note que a letra A aparece diversas vezes na mensagem a ser codificada e em todas as suas codificações esta letra é representada por um código diferente. Isso ocorre porque apesar da correspondência da vogal A no código ASCII ser 65, a cada letra da mensagem está sendo utilizada uma encriptação diferente de acordo com a palavra chave estabelecida, tornando inaplicável a análise de frequência do alfabeto para desvendar a mensagem. Da mesma forma observamos que a letra T aparece diversas vezes na mensagem cifrada, entretanto sempre representando uma letra diferente na mensagem original, novamente isso ocorre devido a palavra chave.

5.3 Prática Experimental de Matemática

A Prática Experimental de Matemática surge como uma ferramenta para enriquecer o currículo da Matemática, tornado o aprendizado mais concreto, contextualizado e significativo. Dentro do tema criptografia podemos explorar diversos conceitos matemáticos relacionados à função, contagem, probabilidade entre outros. Algumas atividades relacionadas a esse tema foram implementadas com êxito em aulas de matemática do ensino Médio e Fundamental.

Inicialmente foram apresentados os conceitos básicos de criptografia, alguns aspectos históricos relevantes. Após toda a contextualização foram confeccionados dois aparatos de criptografar. Os alunos tiveram que codificar algumas mensagens, cada grupo com uma mensagem di-

Tabela 10 - Criptografando com a Cifra Vigenère - decodificando

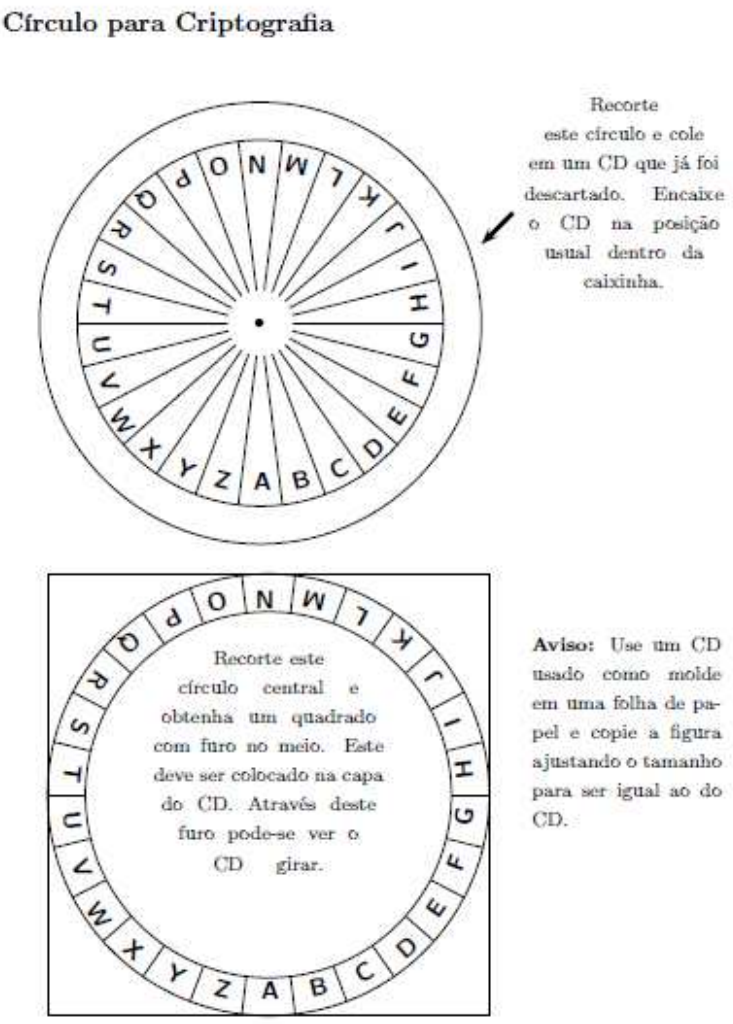
DECODIFICAÇÃO

Mens. Cif.	Código Cif.	Chave	k^n	$D(x) = 65 + (x - 65 - k_n)(mod\ 26)$	Mens.ASCII	Mens.
T	84	P	15	65+(84 - 65 - 15)(mod 26)	69	E
U	85	R	17	65+(85 - 65 - 17)(mod 26)	68	D
I	73	O	14	65+(73 - 65 - 14)(mod 26)	85	U
H	72	F	05	65+(72 - 65 - 05)(mod 26)	67	C
M	77	M	12	65+(77 - 65 - 12)(mod 26)	65	A
C	67	A	26	65+(67 - 65 - 26)(mod 26)	67	C
T	84	T	19	65+(84 - 65 - 19)(mod 26)	65	A
D	68	P	15	65+(68 - 65 - 15)(mod 26)	79	O
V	86	R	17	65+(86 - 65 - 17)(mod 26)	69	E
O	79	O	14	65+(79 - 65 - 14)(mod 26)	65	A
H	72	F	05	65+(72 - 65 - 05)(mod 26)	67	C
T	84	M	12	65+(84 - 65 - 12)(mod 26)	72	H
A	65	A	26	65+(65 - 65 - 26)(mod 26)	65	A
O	79	T	19	65+(79 - 65 - 19)(mod 26)	86	V
T	84	P	15	65+(86 - 65 - 15)(mod 26)	69	E

ferente. Realizado essa etapa foi explorado o princípio Multiplicativo da contagem, explorando e discutindo quantas maneiras diferentes poderiam codificar tais mensagens, ainda, definida a posição do aparato poderíamos concluir que se trata de uma função ou não.

Na etapa final, os alunos deveriam trocar as mensagens entre os grupos e tentar decodificar. Neste momento ficou muito forte o processo de codificação como uma função e para decodificar seria necessário encontrar qual seria a função inversa. Observando a frequência das letras em relação ao alfabeto, foi possível realizar a decodificação das mensagens com êxito.

Figura 19 - Disco de Criptografar



Fonte:Malaguti, Pedro Luiz

6 NÚMEROS PRIMOS E CRIPTOGRAFIA RSA

6.1 Números Primos

Desde os antigos gregos os números primos são estudados com um certo fascínio, a irregularidade em sua sequência é um dos principais objetos de estudos entre a comunidade científica. Os gregos já provaram a existência de infinitos números primos, porém determiná-los não é uma tarefa fácil. Até a era da informação atual eram tratados apenas como um aspecto da matemática, mas com a era da informação e principalmente o papel fundamental que os números primos exercem na criptografia, os números primos assumiram um dos papéis centrais no estudo e pesquisa matemática.

Não é fácil provar fatos adicionais sobre números primos. Sua sequência é razoavelmente suave, mas tem buracos e densos focos. Por exemplo, existe um número primo com um número dado de dígitos? A resposta a esta questão, importante em Criptografia, foi dada a meados do século XIX. Questões semelhantes ainda hoje estão em aberto. Com a era dos computadores em conjunto com o desenvolvimento de algoritmos, os matemáticos vêm procurando responder algumas indagações sobre os números primos. Por exemplo, como saber se um número inteiro n é primo?. Como determinar números primos com altos dígitos?

Se um número inteiro $n > 1$ não é primo, então pode ser escrito como produto de primos e tal representação é única (os gregos já provaram isto há mais de 2000 anos). A prova requer alguma sofisticação, como veremos mais em diante. O mais surpreendente que ainda hoje não existe uma forma eficiente para fatorar um número inteiro n. Usando supercomputadores e sistemas massivamente paralelos, o record atual é fatorar um número com 140 dígitos, e a dificuldade cresce exponencialmente com o número de dígitos. Assim, encontrar a decomposição prima de uma dado número com 400 dígitos, por qualquer um dos métodos conhecidos, hoje é ainda impossível.

Definição: Qualquer inteiro $p \geq 2$ é dito primo se seus únicos divisores positivos são 1 e p. Se p não é primo, então p é dito composto.

Teorema 2. *Se p é primo e $p|ab$, então $p|a$ ou $p|b$.*

Foi mencionado na introdução que todo número inteiro maior que 1, não primo, pode ser escrito como produto de primos. Pode-se afirmar que todo inteiro positivo pode ser escrito

como produto de primos: primos podem ser considerados como "produtos com um fator" e o interio 1 pode ser pensado como o "produto vazio". Assim, enunciamos e provamos o chamado Teorema Fundamental da Teoria da Aritmética.

Teorema 3. *(Teorema Fundamental da Aritmética.) Todo número inteiro, maior do* 1*, pode ser representado de maneira única, salvo a ordem dos fatores, como*

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k},$$

onde os p_i são primos distintos e e_i inteiros positivos.

Demonstração: Temos duas partes a provar, a existência de tal fatoração e a unicidade da mesma.

Seja $n > 1$. Podemos escrever $n = ab$, com $a, b \in \mathbb{Z}$, menores que n. Se um desses não for primo, escrevendo como o produto de dois inteiros menores que ele. Logo, se um destes não for primo, de novo escrevendo como produto de inteiros menores que ele e assim sucessivamente. Este processo finaliza em algum momento e desta forma teriamos escrito n na forma $n = p_1 p_2 \cdots p_k$, onde p_i é primo, para todo i. Isto garante a existência da fatoração de n.

Para mostrar a unicidade usamos um argumento indireto. Supondo a afirmação falsa e usando esta suposição, devemos obter uma contradição lógica. Portanto, assumimos que o inteiro n possui duas fatorações diferentes:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m,$$

onde p_i, q_j são primos positivos.

Podemos assumir, sem perda de generalidade, que p_1 é o menor primo ocorrendo em ambas fatorações. (De fato, se necessário, pode-se trocar o lado esquerdo e o lado direito de modo que o menor primo em qualquer das duas fatorações ocorre na esquerda e então mudar a ordem dos fatores no lado esquerdo de modo que o menor fator seja o primeiro). Também podemos assumir $m \geq k$.

Como p_1 é primo, então divide algum dos fatores q_i. Dado que não estamos interessados na ordem dos fatores, podemos assumir $q_i = q_1$. Mas como p_1 *e* q_1 são primos positivos, temos $p_1 = q_1$ e assim

$$n = p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m.$$

Seguindo este processo obtemos $p_2 = q_2,\ p_3 = q_3, \cdots, p_k = q_k$. Então, se $k \neq m$, temos $q_{k+1} q_{k+2} \cdots q_m = 1$, o que é uma contradição pois $q_{k+1} \nmid 1$. Portanto $k = m$.

Observar que o resultado não desconsidera a ocorrência de primos iguais. Assim, pode-se escrever

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

onde os números naturais n_i e os primos p_i são unicamente determinados.

Teorema 4. *Existem infinitos números primos.*

Demonstração: Precisamos mostrar que para inteiro positivo n, existe um número primo maior que n. Para isso considere o número $n! + 1$ e qualquer divisor primo p dele. Mostremos que $p > n$. Vamos supor que $p \leq n$ e devemos obter uma contradição. Se $p \leq n$, então $p|n!$ pois ele é um dos inteiros cujo produto é $n!$. Sabemos também que $p|(n! + 1)$ e, portanto, é um divisor da diferença $(n! + 1) - n! = 1$. Mas isso é impossível e assim $p > n$, o que mostra o resultado.

Teorema 5. *Sejam os números inteiros*

$$a = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \;\; e \;\; b = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k},$$

onde $e_i \geq 0$ *e* $f_i \geq 0$, *para* $i = 1, 2, \cdots, k$. *Então*

$$mdc(a,b) = p_1^{min(e_1,f_1)} p_2^{min(e_2,f_2)} \ldots p_k^{min(e_k,f_k)}$$

$$mmc(a,b) = p_1^{max(e_1,f_1)} p_2^{max(e_2,f_2)} \ldots p_k^{max(e_k,f_k)}$$

Lema 6.1. *Se* $a, b \in \mathbb{Z}$, *então* $max(a,b) + min(a,b) = a + b$.

Demonstração: Se $a = b$ então $max(a,b) = min(a,b) = a = b$. Logo $max(a,b) + min(a,b) = a + b$.

Se $a \neq b$, sem perda de generalidade, podemos considerar $a < b$. Logo $max(a,b) = b$ e $min(a,b) = a$. Portanto, $max(a,b) + min(a,b) = a + b$.

Teorema 6. *Se a e b são inteiros positivos então*

$$mmc(a,b) \cdot mdc(a,b) = ab.$$

Demonstração: Suponha $a = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ e $b = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$, onde cada $e_i \geq 0$ e $f_i \geq 0$. Segue que,

$$mdc(a,b) \cdot mmc(a,b) = \prod_{i=1}^{k} p_i^{min(a_i,b_i)} \prod_{i=1}^{k} p_i^{max(a_i,b_i)} = \prod_{i=1}^{k} p_i^{min(a_i,b_i)+max(a_i,b_i)}.$$

Pelo Lema 6.1, temos

$$\prod_{i=1}^{k} p_i^{min(a_i,b_i)+max(a_i,b_i)} = \prod_{i=1}^{k} p_i^{(a_i+b_i)} = ab,$$

o que prova o resultado.

Teorema 7. *Um número primo p qualquer, com $p \neq 2$, ou é da forma $4n+1$ ou da forma $4n+3$, para algum $n \in \mathbb{Z}$.*

Demonstração: Seja p um número primo. Se dividimos p por 4, pelo Algoritmo da Divisão, temos os possíveis restos $0, 1, 2$ ou 3. Assim, p pode ser da forma $4n$, $4n+1$, $4n+2$ ou $4n+3$, com $n \in \mathbb{Z}$. Se $p = 4n$ então $4|p$, o que contradiz a primalidade de p. Se $p = 4n+2 = 2(m+1)$ então que $2|p$, ou seja $p = 2$, o que contraria a hipótese. Assim, qualquer número primo p, com $p \neq 2$, é da forma $4n+1$ ou $4n+3$.

6.2 O "Pequeno" Teorema de Fermat

Os números primos são fundamentais, pois todo número inteiro é formado a partir deles. Mas os primos também têm outras e importantes propriedades. Uma dessas foi descoberta pelo matemático francês *Pierre de Fermat* (1601-1655), hoje chamado de Pequeno Teorema de Fermat. Para mostrar esse Teorema, precisamos do Lema 6.2 que enuncia uma outra propriedade de divisibilidade de primos.

Lema 6.2. *Se p é primo e $0 < k < p$, então $p| \begin{pmatrix} p \\ k \end{pmatrix}$.*

A prova do Lema 6.2 segue facilmente da definição do número $\begin{pmatrix} p \\ k \end{pmatrix}$.

Teorema 8. *Se p é primo e a um inteiro, então $p|(a^p - a)$.*

Prova: A prova segue aplicando indução sobre a.

P. de Fermat é mais famoso pelo seu "último" teorema, o qual afirma:

Se $n > 2$, então a equação $a^n + b^n = c^n$, não tem solução em $\mathbb{Z}$.

A hipótese de $n > 2$ é fundamental, pois para $n = 2$ temos alguns exemplos: $3^2 + 4^2 = 5^2$.

Pela história da matemática, sabe-se que *Fermat* afirmou que tinha feito a prova desse fato e escreveu às margens de uma tradução de Arithmetica de Diophante, ao lado do enunciado

deste problema : "*J'ai découvert une preuve tout à fait remarquable, mais la marge est trop petite pour l'écrire*"(Encontrei uma prova absolutamente notável, mas a margem é pequena demais para escrevê-la). Esse enunciado permaneceu como, talvez, o mais famoso problema não resolvido em matemática. Foi o matemático britânico *Andrew Wiles* (1995), com a ajuda do americano *R. Taylor*, que finalmente o mostrou.

Definição: Para $n \geq 1$, a função $\varphi(n)$ denota o números de inteiros no intervalo $[1,n]$, que são relativamente primos à n. Esta função φ é chamada de *Função Totiente de Euler*.

Propriedades:

(1) Se p é primo, então $\varphi(p) = p-1$. De fato, seja $S = \{1,2,\cdots,p-1\}$ o conjunto de todos os números menores que p. Dado $m \in S$, temos que $p \nmid m$, pois $m < p$. Além disso, p é primo e portanto $mdc(p,m) = 1$, para qualquer que seja $m \in S$. Como S contém $p-1$ elementos, segue que $\varphi(p) = p-1$.

(2) A função φ é multiplicativa, isto é, se $mdc(m,n) = 1$, então

$$\varphi(m,n) = \varphi(m)\varphi(n).$$

(3) Se $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, com p_i primos e $e_i \geq 0$, para todo i, então

$$\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_k}).$$

Assim, se n é um número composto que pode ser fatorado como o produto de dois números primos p e q então $\varphi(n) = (p-1)(q-1)$.

Teorema 9. *Para todo inteiro $n \geq 5$,*

$$\varphi(n) > \frac{n}{6\ln\ln n}.$$

Teorema 10. *Para qualquer inteiro positivo k, existem k inteiros consecutivos, todos compostos.*

Prova: *Consideramos a sequência de números inteiros*

$$(k+1)!+2,\ (k+1)!+3,\ \cdots,(k+1)!+k,\ (k+1)!+(k+1).$$

Observar que essa sequência está formada de k inteiros. Além disso, seja $m = (k+1)!+t$, $2 \leq t \leq k+1$. Então:

$$m = 2\cdot 3\cdots(t-1)\cdot t\cdot(t+1)\cdots(k+1)+t = t(2\cdot 3\cdots\widehat{t}\cdots(k+1)+1).$$

Logo, $m = tn$, para $n \in \mathbb{Z}$, e portanto, m é composto, para qualquer $2 \leq t \leq k+1$.

Examinemos a questão oposta, ou seja, encontrar dois primos muito próximos um do outro. Como todos os primos, exceto o 2, são ímpares, a diferença deles tem que ser, pelo menos, 2, exceto para 2 e 3. Dois primos cuja diferença é 2 são ditos *primos gêmeos*. Assim, $(3,5),(5,7),(11,13),(17,19)$ são primos gêmeos. Existem primos gêmeos com centenas de dígitos. Entretanto, não se sabe se existe uma quantidade infinita de primos gêmeos. Quase certamente existe, mas nenhuma prova foi encontrada, apesar dos esforços de muitos matemáticos durante mais de 2000 anos.

Uma questão importante sobre primos é quantos deles existem até um certo número dado *n*? Representemos o número de primos até *n* por $\pi(n)$. Esta função cresce suavemente e a sua inclinação decresce lentamente. Uma fórmula exata para $\pi(n)$ é certamente impossível de obter. Em 1896, um poderoso resultado, chamado de *Teorema do Número Primo* foi provado por *Hadamard e de la Vallée Poussin*. A prova do teorema abaixo é difícil. Já foi observado esse fato no século XVII, mas só foi provado mais de 100 anos depois.

Teorema 11. *(Teorema do Número Primo) Se $\pi(n)$ representa o número de primos entre $1,2,\cdots,n$, então*

$$\pi(n) \approx \frac{n}{ln(n)},$$

onde $ln(n)$ é o logaritmo natural de n.

Isto significa que o quociente $\pi(n)/\frac{n}{ln(n)}$ fica próximo de 1 se *n* for suficientemente grande.

Como uma ilustração do Teorema do Número Primo, vejamos quantos primos com 200 dígitos existem. Obtemos a resposta subtraindo o número de primos até 10^{199} do número de primos até 10^{200}. Pelo Teorema 11, esse número é cerca de

$$\frac{10^{200}}{200\ ln(10)} - \frac{10^{199}}{199\ ln(10)} \approx 1,95 \cdot 10^{197}.$$

Este número é muito grande. Comparando isto com o número total de inteiros positivos com 200 dígitos, que sabemos que é $10^{200} - 10^{199} = 9 \cdot 10^{199}$, obtemos

$$\frac{9 \cdot 10^{199}}{1,95 \cdot 10^{197}} \approx 460.$$

Portanto, entre os inteiros com 200 dígitos, um em cada 460 é primo.

Fica claro que o argumento acima não é preciso; é apenas uma aproximação, se *n* for muito grande. Quão grande deve ser *n* para o erro ser muito pequeno? Isso leva a questões ainda hoje não resolvidas.

6.2.1 A conjectura de Goldbach

A Conjectura de Goldbach

Os números primos sempre fascinaram o ser humano. A partir de sua definição simples podemos obter resultados belíssimos, como o Teorema Fundamental da Aritmética e a existência de infinitos números primos. No entanto, conhecemos muito pouco a respeito dos números primos. Por exemplo, os primos da forma p e $p+2$ são conhecidos como primos gêmeos. Assim, 3 e 5, 5 e 7, 11 e 13, 17 e 19 são exemplos de primos gêmeos. Uma questão que se coloca é a seguinte: Existem infinitos primos gêmeos? Não se conhece uma resposta para esta questão. Em 1919, Brun provou que a série formada pela soma dos recíprocos dos primos gêmeos converge, obtendo:

Teorema 12. *Teorema de Brun*

$$B = \sum(\frac{1}{p} + \frac{1}{p+2}) = (\frac{1}{3} + \frac{1}{5}) + (\frac{1}{5} + \frac{1}{7}) + (\frac{1}{11} + \frac{1}{13}) + ... = 1,902...$$

.

Uma outra especulação a respeito dos números primos nos leva à seguinte lista

$4 = 2+2; 6 = 3+3; 8 = 3+5; 10 = 5+5; 12 = 5+7; 14 = 7+7; 16 = 5+11, ...$.

Parece que todos os números inteiros pares maiores do que 2 podem ser escritos como sendo a soma de dois números primos. Esta observação foi feita em 1742 por Christian Goldbach numa carta a Euler.

Conjectura de Goldbach: Todo número inteiro par maior que 2 pode ser escrito como uma soma de dois números primos.

Várias tentativas para a sua demonstração têm sido feitas. Por exemplo, já se mostrou que ela é verdadeira para inteiros pares menores que 4.10^{14}. O caso geral continua em aberto.

Recentemente, em 2012 o matemático peruano Harald Andrés Helfgott, provou a conjectura "fraca"de Goldbach. De acordo com Helfgott, *todo número ímpar maior que* 5 *pode ser expresso como a soma de três números primos*, um importante resultado para a comunidade científica, mas o caso geral continua em aberto.

6.3 Distribuição dos números primos

Já demonstramos inicialmente que existem infinitos números primos. Mas um dos grandes interesses dos matemáticos é determinar quais são esses números primos. Por exemplo, existem quantos números primos até a ordem de 10 milhões de casas. Note que estamos tratando de números bem grandes, pois isso é fundamental na criptografia RSA, quando maior os números primos determinados, maior será a segurança de todo o criptossistema.

No entanto se observarmos a distribuição dos números primos, veremos que esta não tem nenhum padrão, ainda que a frequência de ocorrência dos números primos é cada vez menor, ou seja, quando maior o número primo, mais difícil será encontrar o próximo.

Eratóstenes foi um dos primeiros a determinar um teste de primalidade, criou uma tabela hoje denominada Crivo de Eratóstenes na qual é possível determinar os números primos extraindo os múltiplos dos números.

Figura 20 - Crivo de Erástotenes

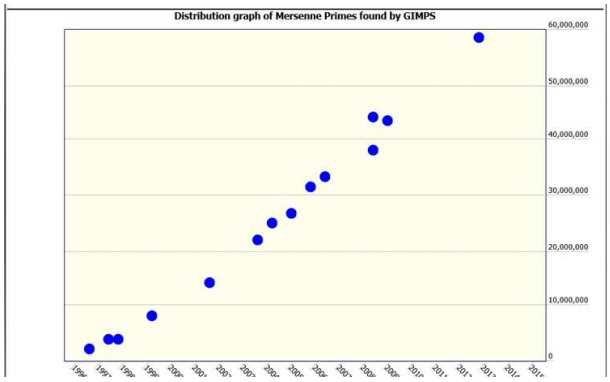
Fonte:Adaptado de http://e-reality-home.blogspot.com.br

O processo proposto por Eratóstenes é eficiente, porém muito lento e moroso. Realizar esse processo para números muito grandes é praticamente inviável. Além da determinação dos números primos grandes, outra questão é como será a frequência dos números primos. Para isto vamos formalizar o conceito de frequência de primos.

A título de curiosidade o maior número primo encontrado até os dias de hoje, é da casa de 17 milhões de dígitos. É um dos primos de Mersenne que foi descoberto em 2013 por

Curtis Cooper da University of Central Missouri. Para encontrar tal feito, o matemático Cooper conta com uma gigantesca rede de computadores, cerca de 360.000 processadores que operam a 150 trilhões de cálculos por segundo. Tanta demanda computacional encontrou o número $2^{(57.885.161)} - 1$.

Figura 21 - Distribuição do números primos



Fonte: Adaptado de Wikipedia

Denotemos $\pi(x)$ a quantidade de números primos menores ou iguais a x, portanto a probabilidade de que um elemento do conjunto $(1,...,x)$ seja primo é determinada por: $\frac{\pi(x)}{x}$.

Legendre e Gauss chegaram a conclusão de que este quociente está relacionado com $\frac{1}{lnx}$. Por volta de 1900, J Hadamard e Ch. de la Valleè-Poussin demonstraram independentemente o *Teorema dos Números Primos*.

- $$\lim_{x\to\infty} \frac{\pi(x)}{x}(\frac{1}{\ln x})^{-1} = 1$$

A distribuição dos números primos é ainda uma das questões mais discutidas na matemática, em relação à esse tema existem alguns problemas em aberto:

- Sempre existe um número primo entre n^2 e $(n+1)^2$?
- Para $n = 0,1,...,40$, tem-se que $n^2 - n + 41$ é primo. Existem infinitos números primos dessa forma?
- A sequência de Fibonacci contém infinitos números primos?
- A conjectura de Goldbach - Todo número natural pode ser escrito como a soma de dois números primos.

- A Hipótese de Riemann.

6.4 Sistema Criptográfico RSA

Finalmente chegamos ao capítulo de Criptografia RSA, onde aplicaremos tudo que foi visto até agora para criptografar e verificar a segurança deste sistema que estamos a estudar. Já sabemos que, para uma maior segurança do sistema de Criptografia RSA, devemos utilizar números primos grandes, porém, como desejamos apenas ilustrar seu procedimento e funcionalidade, utilizaremos números primos não tão grandes, facilitando a compreensão deste sistema.

6.5 Pré-codificação

Antes de utilizarmos o sistema de criptografia RSA devemos converter a mensagem a ser enviada para uma sequência de números. Para tal ato utilizaremos a tabela abaixo:

alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M
código ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77
alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
código ASCII	78	79	80	81	82	83	84	85	86	87	88	89	90

A frase "A EDUCAÇÃO É A CHAVE", por exemplo, ficaria desta forma:

$$65696885676567657969656772658669$$

6.6 Codificar e Decodificar

Para o processo de codificação necessitaremos de um valor n que seria o produto de dois primos p e q, e um valor e de tal forma que $mdc(\varphi(n), e) = 1$. Pela função $\varphi deEuler, temosque : \varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Chamaremos de (n, e) de chave de codificação e de b cada um dos blocos que devemos montar, quando codificada, cada um desses blocos resultará um um bloco novo que é como a mensagem será enviada.

O novo bloco será conhecido como $C(b)$ que será o resto da divisão de b^e por n. Para o processo de decodificação faremos um processo semelhante, porém no lugar de e usaremos o

inteiro d, que é a inversa de e módulo $\varphi(n)$ e o valor do novo bloco será denotado por $D(a)$ que será o resto da divisão de a^d por n, sendo a o bloco que estamos decodificando.

Consideremos os primos $p = 11$ e $q = 17$, e o inteiro $e = 13$, portanto teremos, $n = 187$, $\varphi(n) = 160$ e $d = 37$. Nosso objetivo será criptografar a frase "A EDUCACAO E A CHAVE"e decodificá-la para a forma normal. Utilizando a tabela da seção anterior para transformar os caracteres em números, obteremos a seguinte sequência:

$$65696885676567657969656772658669$$

Feito isto, devemos construir blocos para que possamos criptografá-lo. Observe que os valores de cada bloco deverão ser de tal forma que $b < n$, ou seja, $b < 187$ caso contrário teremos problemas para decodificar a mensagem.

$$65-69-68-85-67-65-67-65-79-69-65-67-72-65-86-69$$

Devemos, agora, criptografar esta sequência, para isto devemos calcular o resto da divisão de cada bloco elevado a $e = 13$ módulo $n = 187$.

$65^{13} \equiv 65^{10}.65^3 \equiv 144.109 \equiv 175(mod\ \ 187)$

$69^{13} \equiv 69^{10}.69^3 \equiv 1.137 \equiv 137(mod\ \ 187)$

$68^{13} \equiv 68^{10}.68^3 \equiv 34.85 \equiv 85(mod\ \ 187)$

$85^{13} \equiv 85^{10}.85^3 \equiv 34.17 \equiv 17(mod\ \ 187)$

$67^{13} \equiv 1^6.67 \equiv 1.67 \equiv 67(mod\ \ 187)$

$79^{13} \equiv 10^2.107 \equiv 41(mod\ \ 187)$

$72^{13} \equiv 72^{10}.72^3 \equiv 67.183 \equiv 106(mod\ \ 187)$

$86^{13} \equiv 1^2.86^3 \equiv 1.69 \equiv 69(mod\ \ 187)$

Logo, possuiremos a seguinte sequência de números da mensagem criptografada:

$$175-137-85-17-67-175-67-175-41-137-175-67-106-175-69-137$$

Com isto, a mensagem está criptografada e pronta para ser transmitida. Vejamos como decodificá-la

Para decodificar uma mensagem realizaremos o mesmo processo, porém o que nos interessa agora, é o resto da divisão de cada bloco elevado a $d = 37$ por $n = 187$. Note que no processo de codificação e decodificação não foram necessários conhecer quem seriam os dois números primos que deram origem a n.

$175^{37} \equiv 65(mod\ \ 187)$

$137^{37} \equiv 69(mod\ \ 187)$

$85^{37} \equiv 68(mod\ \ 187)$

$17^{37} \equiv 85(mod\ \ 187)$

$41^{37} \equiv 79(mod\ \ 187)$

$106^{37} \equiv 72(mod\ \ 187)$

$69^{37} \equiv 86(mod\ \ 187)$

$67^{37} \equiv 67(mod\ \ 187)$

Sendo assim, obteremos a seguinte sequência de números:

$$65-69-68-85-67-65-67-65-79-69-65-67-72-65-86-69$$

Retornamos a sequência anterior como o esperado e a mensagem está decodificada.

6.7 Funcionamento e Segurança

Temos que, para criptografar um mensagem, é necessário uma chave (n,e) denotada por $C(b)$, sendo b o bloco a ser codificado e uma chave (n,d) denotada por $D(b)$. Sendo assim, esperamos que o resultado de quando aplicamos estas duas ações seja $DC(b) = b$, ou ainda, que $\overline{b}^{ed} = \overline{b}$. Vejamos por que isso funciona.

Consideremos $n = pq$ e calculemos a forma reduzida de b^{ed} módulo p e q. Como ambos possuem o mesmo processo realizaremos este processo apenas para p. Consideremos, agora, o fato de d ser o inverso de e módulo $\varphi(n)$, portanto $ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$, com k inteiro. Sendo assim, teremos:

$$b^{ed} \equiv (b^{p-1})^{k(q-1)} b (mod \ \ p).$$

Mas, o teorema de Fermat nos diz que

$$b^{p-1} \equiv 1 (mod \ \ p).$$

Portanto,

$$b^{ed} \equiv b (mod \ \ p).$$

Logo, p divide $b^{ed} - b$ e por analogia q também o divide e n também o divide, está provado seu funcionamento.

Falaremos um pouco sobre a segurança fornecida pelo sistema de criptografia RSA.

A chave de codificação (n, e) é conhecida por chave pública, ou seja, qualquer um pode facilmente obtê-la, mas somente com estes dois dados, a obtenção do valor chave para a decodificação não pode ser facilmente encontrada, pois, este é o inverso de e módulo $\varphi(n)$ que só pode ser encontrado se fatorarmos n e encontrarmos p e q, ou, seja, resume-se a fatorar o valor n.

Para um melhor entendimento, suponhamos que haja um método para encontrar o valor de $\varphi(n)$ rapidamente a partir de n e e, ou seja, $n = pq$ e $\varphi(n) = (p-1)(q-1)$ são conhecidos e desejamos encontrar p e q, mas

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+1) + 1.$$

Disto, obteremos que $p + q = n - \varphi(n) + 1$, mas temos também que

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2.$$

Disto obteremos que $p - q = \sqrt{(p+q)^2 - 4n}$.

Observando as duas expressões encontradas, perceberemos que ambas são conhecidas e torna-se fácil, encontrar o valor de p e de q. Concluímos que não é muito útil encontrar uma maneira de encontrar $\varphi(n)$ sem fatorar n, pois com estes dois, chegamos a seus fatores.

7 CRIPTOGRAFIA QUÂNTICA

Os sistemas criptográficos atuais têm a sua segurança baseada no sistema RSA, que necessita da determinação de números primos grandes pois estes são difícilmente fatorados mesmo com toda a tecnologia que temos a nossa disposição. Entretanto a história nos mostra que sempre houve uma disputa entre os criptógrafos e os criptoanalistas, uma batalha silenciosa no campo da matemática. Alguns códigos, sistemas criptográficos perduraram por muitos séculos, porém em algum momento da história foram quebrados. Eis a questão, todo o nosso sistema de segurança eletrônica, tal como as transações bancárias, correspondências eletrônicas são baseadas na criptografia, essencialmente na RSA, será que estamos completamente em segurança? Será que o RSA pode ser quebrado?

A história nos responderia que mais cedo ou mais tarde o RSA se tornaria obsoleto. Mas como? Na atualidade já existem muitas pesquisas sobre o computador quântico e então a criptografia quântica. Baseados na física quântica, o computador quântico seria capaz de fatorar um número rapidamente, e assim descobrir quais são os seus dois números primos geradores e quebrar o sistema RSA. Existem muitas indagações na imprensa internacional de que alguns países já possuam esse computador quântico e que este possa ser utilizado para realizar espionagem.

A criptografia quântica já está sendo utilizada experimentalmente em alguns estabelecimentos comerciais tais como alguns bancos em Genebra na Suíça, porém possui muitas limitações e dificuldades de implementação. Uma das grandes vantagens da criptografia quântica é que ela permite detectar quando o sistema está sendo invadido e a transmissão cessa instantaneamente.

8 CONCLUSÃO

A história evidencia que a criptografia está presente durante séculos, milênios. O seu desenvolvimento ocorreu de acordo com a necessidade da sociedade, no entanto o seu aperfeiçoamento vêm de encontro ao desenvolvimento da matemática. Também é possível notar que ao longo dos anos os criptoanalistas conseguem quebrar os códigos por mais seguros que estes pareçam, e novamente surge a necessidade de inovar a forma de criptografar. Na contemporaneidade a criptografia está fortemente presente na vida das pessoas, é um atrativo para o ensino da matemática. Com este tema que perpassa por vários fundamentos da matemática em diferentes contextos e níveis de ensino, o torna muito enriquecedor para o currículo do ensino. O escopo deste trabalho foi propor uma nova perspectiva para o ensino de determinados temas na matemática, auxiliar no desenvolvimento das competências leitora e escritora através da história, colaborar com a interdisciplinariedade e principalmente tornar o aprendizado mais significativo. Foi possível evidenciar também que a matemática possui temas em aberto, temas para pesquisa, em constante desenvolvimento.

REFERÊNCIAS BIBLIOGRÁFICAS

S. C. Coutinho, *Números Inteiros e Criptografia RSA*, Série de Computação e Matemática, IMPA, Rio de Janeiro, 2003.

S. C. Coutinho,*Criptografia*, Programa de Iniciação Científica, OBMEP, Rio de Janeiro, 2008.

D. E. Knuth,*The art of computer programming*, vol.2, Seminumererical algorithms, segunda edição, Addison-Wesley Publishing Company, Reading, 1981.

A.M. Masuda e D. Panario, *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*, Coleção 26 Cóloquio Brasileiro de Matemática, Rio de Janeiro, 2007.

A. Hefez e M.L.T. Vilela, *Códigos Corretores de Erros*, Instituto Nacional de Matemática Pura e Aplicada - IMPA, Série de Computação e Matemática, Rio de Janeiro, 2002.

J.E.A.Rodrigues e E.D. Carvalho *Tópicos de Matemática Discreta*, Apostila ERMAC - SBMAC /UNESP Bauru, 2008.

N. Koblitz *A Course in number theory and criptography* Graduate Texts in Mathematics, Sringer-Verlag, New York, 1987.

Pedro Luiz Malaguti, *Atividades de contagem com criptografia*,Programa de Iniciação Científica, OBMEP, Rio de Janeiro.

Singh, Simon *O Livro dos Códigos*, Editora Record,2004