PROFMAT **Departamento de Matemática**
Universidade Federal do Paraná
81531-990, Curitiba, PR
Brazil

Criptografia e Matemática

por

Fernanda Ricardo Schankoski

Preprint PROFMAT 3 (2015) 20 de Março, 2015

Disponível via INTERNET:
http://www.mat.ufpr.br

Criptografia e Matemática

Fernanda Ricardo Schankoski
Curitiba, PR
Brazil
e-mail: nandi.rs@gmail.com

Resumo

O maior desafio atualmente, nas escolas, do professor de matemática é despertar o interesse, o gosto no aluno por essa disciplina e consequentemente fazê-lo compreender que, sim, é possível ele aprender e utilizar no seu cotidiano muitos dos conteúdos trabalhados em sala de aula. É dentro desse contexto que desenvolvemos esse trabalho, com o objetivo de ampliar o conhecimento de nossos colegas professores e interessados no assunto Criptografia, dando-lhes mais possibilidades e ideias para a contextualização de conteúdos de matemática na sala de aula. Para isso descrevemos uma breve história sobre a criptografia, os principais códigos, cifras e a criptografia utilizada pelo homem até a atualidade, relatamos seu destaque em momentos históricos e a sua evolução paralela a comunicação, assim fica fácil compreender o papel da matemática no desenvolvimento de novos métodos para criptografar mensagens, dados, informações e também, consequentemente, de decriptá-las. Destacamos, na sequência, a aritmética modular, principal ferramenta utilizada hoje para criptografar de forma segura e eficaz no método RSA, o qual também situamos historicamente e descrevemos sua implementação. Diante disso sugerimos várias atividades, para serem aplicadas com alunos a partir do 6º ano até a 3ª série do ensino médio, que englobam diversos conteúdos de matemática, análise combinatória, matrizes, funções, divisão, e vamos além, sugerindo algumas atividades de aritmética modular e RSA.
Palavras-chave: Criptografia; Criptoanálise; Matemática.

Sumário

Conteúdo

Lista de Tabelas

Introdução

A criptografia tem sua participação no curso da história da humanidade e hoje está presente no nosso cotidiano, são senhas, compras pela internet, cartões, caixas eletrônicos, e tudo isso precisa ser mantido em segredo, e nós nem sabemos como isso acontece, simplesmente acreditamos que é confiável.

Além disso, o tema desperta curiosidade nas pessoas, em particular nos alunos, que tão pouco compreendem que a matemática está aplicada no simples fato de manter sua senha de redes sociais segura. Levar esse assunto para as aulas trará novas aplicações para o estudo de matrizes, análise combinatória e funções e ainda agregará a aritmética modular ao conhecimento e formação matemática dos alunos do ensino médio.

O estudo abrange três tópicos importantes, que juntos estimulam, explicam e indicam possibilidades que o professor de matemática pode adotar em suas aulas, para tanto, cada tópico apresenta atividades para sala de aula.

Primeiramente abordamos os tipos de criptografia usados no passado, quais contribuíram em muitos momentos da história, como funcionavam e para que eram utilizados. Esses primeiros métodos de criptografia podem ser aplicados em sala de aula em diversos níveis, através de atividades envolvendo os conteúdos de análise combinatória, funções, matrizes entre outros.

A criptografia é o estudo que desenvolve métodos para ocultar o conteúdo de uma mensagem. Sua evolução caminhou em paralelo às descobertas dos meios de comunicação e as necessidades das pessoas manterem em segredo suas conversas e dados, cada vez mais suscetíveis em cair em mãos erradas.

Conforme a criptografia avançava, junto a ela também nascia e se desenvolvia a criptoanálise, métodos de decifrar as mensagens, e isso impulsionou os vários tipos de criptografia, que vão desde os códigos, que são a substituição de palavras por outras palavras, e as cifras monoalfabéticas e polialfabéticas, que são a troca de uma letra por outra, ordenadamente ou não, até chegar à aritmética modular, que é o sistema mais usado e seguro atualmente, que também usa a substituição alfabética assim como as cifras, mas com um algoritmo e chave muito mais seguros.

A partir de então a matemática tornou-se imprescindível para o sigilo de mensagens, senhas, transações financeiras e etc. E é essa a matemática abordada no segundo tópico, a teoria dos números pela aritmética modular. Para compreensão da aritmética modular elementar apresentamos alguns resultados, exemplos e também atividades possíveis de serem desenvolvidas com os alunos.

Finalizando, temos o terceiro tópico que explica como criptografar e decriptar mensagens usando o método RSA, ou seja, temos a implementação do RSA. Método esse que nasceu junto à invenção do computador e resiste até hoje, pois além de viável, ainda é seguro. Como nas seções anteriores há sugestões de atividades para aprofundamento de alunos mais interessados no tema.

1 Criptografia

O homem, desde a antiguidade, sempre teve a necessidade de se comunicar através de mensagens e ainda as utiliza, mas as formas de envio e recebimento sofreram alterações, adaptando-se aos meios de comunicação que surgiram e evoluindo com eles.

Fez-se necessário então a utilização das escritas secretas, principalmente pelo comércio, as guerras e a espionagem que sempre existiram. O propósito era que as mensagens fossem compreendidas apenas pelo destinatário, ou seja, não poderiam ser descobertas ou lidas por inimigos ou rivais, seu conteúdo só poderia ser revelado a quem era de interesse.

Os primeiros relatos sobre tais escritas secretas são do século V a.C. e aparecem nos nove livros *As Histórias, de Heródoto*, historiador grego. Consistia na verdade em *esteganografia*.

Esteganografia é uma comunicação secreta, onde se esconde a existência da mensagem, que só é revelada ao destinatário final, a palavra deriva do grego *steganos*, que significa coberto, e *graphein*, que significa escrever. O termo esteganografia ficou conhecido em 1499 em um livro de 3 volumes do monge Johannes Trithemius, que aparentemente era sobre magia, espíritos, religião, porém, mais tarde, descobriu-se que o livro relatava sobre esteganografia e criptografia, detalhando vários métodos para enviar uma mensagem.

Os livros de Heródoto descrevem que as mensagens enviadas aos gregos, de como e quando Xerxes, o rei da Pérsia, iria atacá-los, eram escritas em pedaços de madeira e cobertas com cera. Outro episódio destes mesmos livros relata sobre um jovem que raspa a cabeça para escrever uma mensagem em seu couro cabeludo, que é levada em segurança ao destinatário coberta pelo cabelo já crescido e é revelada raspando novamente a cabeça.

Com o tempo e após Heródoto, várias formas de esteganografia foram usadas no mundo. Os chineses antigos, por exemplo, escreviam mensagens em seda fina, faziam uma bolinha, cobriam com cera e a comiam. Já no século XVI, um cientista italiano, descreveu como esconder uma mensagem dentro de um ovo cozido, escrevendo na casca com uma solução só vista quando se tira a casca. Outras técnicas com tintas especiais, que quando secas ficavam invisíveis e depois de submetidas ao calor revelavam o que havia sido escrito, foram utilizadas.

Houve muitos outros casos e outras técnicas que permitiam esconder informações, dentro de outros textos, em jornais, imagens e músicas. A longevidade da esteganografia mostra que ela oferece certa segurança, porém é vulnerável a uma vigilância rígida.

Buscando ultrapassar os limites da vigilância, a Criptografia surgiu, pois diferentemente da esteganografia, a Criptografia não tem por objetivo esconder a mensagem, mas sim esconder seu significado.

Houaiss *in* da Cruz [6] explica a lexicografia da palavra Criptografia, o termo deriva do latim moderno *cryptographia*, cripto, do grego *kryptós*, oculto, secreto,

obscuro, ininteligível, e grafia, do grego *graphía*, com o sentido de escrita, do verbo grego *gráphó*, escrever. Segundo ele, criptografia significa,

> "conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; [...] em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções."

E segundo Singh [26],

> "O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado – um processo conhecido como encriptação. Para tornar a mensagem incompreensível, o texto é misturado de acordo com um protocolo específico, que já foi estabelecido previamente por ambos transmissor e receptor."

Este protocolo acordado entre o transmissor e o receptor chama-se Chave, que serve para escrever a mensagem secreta e posteriormente voltar à mensagem original.

O Portal ICP Brasil (Infraestrutura de Chaves Públicas) *in* da Cruz [6] estabelece criptografia como:

> "Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo. [...] Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem."

Desde então esconder a mensagem não foi mais necessário, o envio dessas, seja por telegramas, via rádio, ou hoje, por e-mails pode ser interceptado, pois o conteúdo não fará sentido para o intermediário.

O que foi feito muitas vezes, era uma combinação da esteganografia com a criptografia, dessa forma, caso fosse descoberta uma mensagem camuflada, ainda existia outro obstáculo: lê-la. Um exemplo é o microponto, utilizado muito na 2ª Guerra Mundial pelos alemães, que consiste na redução fotográfica da mensagem até transformá-la num ponto final para ser inserido no texto de uma carta inofensiva. Porém, ele foi descoberto em 1941 pelo F.B.I.(Unidade de Polícia do Departamento de Justiça dos Estados Unidos) e desde então antes de reduzida, a mensagem era criptografada.

Nessas épocas de guerra, a ameaça da interceptação incentivou ainda mais o desenvolvimento e aprimoramento da criptografia através de códigos e cifras, que são técnicas para mascarar a mensagem de modo que só o destinatário possa ler

o seu conteúdo. Aliás, quando uma mensagem é enviada, há duas preocupações; a de transmitir a mensagem de modo que fontes não autorizadas não tenham acesso ao conteúdo desta mensagem e a de transmitir com segurança e clareza a mensagem, ou seja, garantir que a mensagem vai ser recebida corretamente, não sofrerá danificação. Como Criptografia é o ramo que tem como objetivo a primeira preocupação, manter uma mensagem em sigilo, a segunda preocupação, cabe à Teoria de Códigos, a qual não abordaremos.

Ao mesmo tempo em que as nações junto aos criptografistas criavam códigos e cifras cada vez mais elaboradas para garantir a segurança de suas informações e comunicações, os decifradores e decodificadores inimigos, chamados criptoanalistas, tentavam quebrar esses códigos e cifras para roubar seus segredos. Esses conjuntos de métodos e técnicas para decifrar ou decodificar uma mensagem é conhecido como Criptoanálise, esta juntamente com a Criptografia constitui a área de conhecimento Criptologia.

Em suma, Criptografia é a ciência de escrever em cifras ou em códigos, tornando a mensagem incompreensível, permitindo apenas ao destinatário desejado decifrar ou decodificar a mensagem com clareza, utilizando para isso, a Chave.

Código e cifra são maneiras diferentes de criptografar uma mensagem, segundo Singh [26]:

> "Um Código envolve a substituição de uma palavra ou frase por uma outra palavra, um número ou um símbolo e Cifra é uma técnica que age num nível mais fundamental, onde as letras, no lugar das palavras são substituídas."

Embora ambos, criptografar e codificar, utilizam o método da substituição, então se pode usar simultaneamente as duas formas, o que torna aparentemente a mensagem mais segura, mas é um engano, pois a parte cifrada pode ser decifrada usando análise de frequência, que veremos mais a frente, e a parte codificada é decodificada deduzindo-se a partir do contexto.

Para entender melhor, a Criptografia é dividida em dois ramos, conhecidos como transposição e substituição, e a substituição por sua vez é subdividida em outros dois ramos, código e cifra. Sendo que a cifra é historicamente a mais usada.

Observa-se, primeiramente, que não se utilizava matemática para cifrar ou codificar uma mensagem, mas com cálculos matemáticos, principalmente análise combinatória, é possível obter quantos são os resultados possíveis para algumas cifras e códigos utilizados, analisando assim a segurança, vulnerabilidade e conveniência de adotá-los.

A criptografia de transposição foi usada poucas vezes ao longo da história, isso se deve ao fato de que para mensagens curtas, ou para palavras de ordens de comando esse método é extremamente inseguro, visto que as letras das mensagens são rearranjadas, gerando um anagrama. Veja:

amor

AMOR, AMRO, AOMR, AORM, AROM, ARMO, MARO, MAOR, MOAR, MORA, MRAO, MROA, OAMR, OARM, ORMA, ORAM, OMRA, OMAR, RAMO, RAOM, ROAM, ROMA, RMAO, RMOA

$$P_4 = 4! = 4 \times 3 \times 2 \times 1 = 24 \tag{1}$$

Observe que existem somente 24 anagramas para palavra amor, sendo que um deles é a própria palavra.

Embora, mensagens longas e textos, torne essa criptografia muito segura, haverá uma imensa dificuldade, tornando-se praticamente impossível que o destinatário obtenha a mensagem original, se não houver uma comunicação prévia com o remetente. Como se segue:

matemática é minha matéria preferida

TEAFMNPAID T IEEMH ARAITER ARMCIAEAM

$$P_{32}^{4,7,3,5,4,3} = \frac{32!}{4!7!3!5!4!3!} = 2,63130836933693 \times 10^{35} \tag{2}$$

Essa frase contém 32 letras que formam mais de 20.000.000.000.000.000.000.000.000 arranjos distintos, como podemos observar na permutação acima. No exemplo dado, as letras foram transpostas aleatoriamente, e nesse caso diz Singh [26],

> "A transposição efetivamente gera um anagrama incrivelmente difícil e, se as letras forem misturadas ao acaso, sem rima ou fundamento, a decodificação do anagrama se tornará impossível, tanto para o destinatário quanto para o interceptor inimigo."

Para reverter esse problema, há o sistema de transposição chamado de *cerca de ferrovia* que consiste em escrever uma mensagem de modo que as letras alternadas fiquem separadas nas linhas de cima e de baixo, formando uma sequência de letras na linha superior seguida pela inferior, criando a mensagem cifrada final. O destinatário reverte o processo reposicionando a mensagem cifrada nas linhas recuperando a mensagem original. Observe usando a mesma frase:

```
M   T   M   T   C   E   I   H   M   T   R   A   R   F   R   D
  A   E   A   I   A   M   N   A   A   E   I   P   E   E   I   A

Cifra: M T M T C E I H M T R A R F R D A E A I A M N A A E I P E E I A
```

Nesse sistema podemos escolher usar o mesmo processo com três, quatro ou mais linhas ou também podemos trocar cada par de letras, ou cada trio em uma mesma sequência, e assim por diante.

O primeiro aparelho criptográfico usava a Cifra de Transposição, conhecido como *Citale espartano*, um instrumento militar do século V a.C., que consistia em um bastão de madeira em volta do qual era enrolada uma tira de couro ou pergaminho. O remetente escrevia a mensagem ao longo do comprimento do citale e depois desenrolava a fita e as letras eram misturadas. Para decifrar a mensagem era necessário enrolá-la em um citale de mesmo diâmetro.

Figura 1: Citale

Logo, o método da transposição consiste apenas em rearranjar as letras de uma mensagem, ou seja, as letras mantêm sua identidade, mas mudam de posição. Uma das primeiras descrições de cifra por substituição aparece no texto *Kama-sutra*, escrito no século IV a.C., que recomenda que as mulheres deveriam estudar 64 artes, entre elas, a *mlecchita-vikalpa* que é a arte da escrita secreta.

Esse método de criptografar percorreu toda história, sua utilização foi evidente em guerras, foi objeto de estudo de criptoanalistas e criptografistas do mundo todo, e foi percussor do que temos atualmente no processo de escritas secretas e computacional.

Segundo Singh [26] a cifra de substituição é chamada desta maneira " ...porque cada letra no texto é substituída por uma letra diferente, complementando assim a cifra de transposição."

Como já descrito, a criptografia por código é uma substituição de palavras ou frases, por outras palavras, símbolos, números, sendo assim, para codificar uma mensagem deve-se ter um dicionário chave para que o remetente escreva o texto, e quando chegar ao destinatário, o mesmo deve ter o dicionário chave idêntico para decodificar a mensagem corretamente.

Por exemplo:

```
ataque: LEÃO
fuja: AVE
inimigo:TUBARÃO
Frase: ataque do inimigo fuja
Código: LEÃO TUBARÃO AVE
```

É uma forma de criptografar segura, se não fosse o fato de que cada possível destinatário deveria possuir um dicionário chave, e esse poderia cair em mãos erradas e em posse da chave a decodificação seria fácil, tornando-o um método inviável, pois além do inimigo conseguir decodificar qualquer mensagem que havia sido escrita, teria que ser reformulado um novo dicionário com outros códigos.

O primeiro documento que usou uma cifra de substituição para propósitos militares foi no século I a.C. nas Guerras da Gália de Júlio César. César descreve como mandou uma mensagem para Cícero: substituiu as letras do alfabeto romano por letras gregas. Como Júlio César usava com muita frequência a escrita secreta, existe uma Cifra de Substituição chamada Cifra de César em sua homenagem.

A cifra de César funciona simplesmente substituindo cada letra na mensagem por outra que está três casas á frente no alfabeto, como na tabela abaixo:

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

Tabela 1: Cifra de César

Pode-se também deslocar não apenas três casas, mas cinco, sete ou qualquer outro número entre uma e 25 casas, para a letra A escolhemos uma das outras 25 letras do alfabeto e consequentemente as letras B,C, ..., Z seguem a sequência, obtendo 25 Cifras de César distintas.

Sem se limitar a mover as casas ordenadamente haverá mais de 400.000.000.000.000.000.000.000.000 de cifras diferentes e consequentemente chaves diferentes terão de ser testadas, tornando inviável a verificação de todas as possibilidades. Essa verificação pelo inimigo é conhecida como ataque pela força bruta. De fato,

$$P_{26} = 26! = 4,03291461126605 \times 10^{26} \tag{3}$$

Deslocando ordenadamente as letras do alfabeto ou não, cada cifra será codificada e decifrada de modo único, sendo o método geral de codificação o Algoritmo e os detalhes para decifrá-la, a Chave.

O importante deste método é o conhecimento da Chave apenas pelo destinatário final, caso contrário, qualquer inimigo conseguirá ler a mensagem. Note que nos moldes da Cifra de César teremos apenas 25 tipos diferentes de Chaves, logo se um inimigo interceptar uma mensagem escrita nesses moldes, ele só precisa checar 25 possibilidades.

Como relata Singh [26]:

> "A importância da chave, em oposição ao algoritmo, é um princípio constante da criptografia, como foi definido de modo definitivo em 1883 pelo linguista holandês Auguste Kerckhoff Von Nieuwenhof, em seu livro La Cryptographie Militarie. Este é o Princípio de Kerckhoff: "A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave."

Embora a segurança da Chave da Cifra de César seja frágil, evita confusão no compartilhamento pelo remetente e destinatário. Já as outras formas de substituição podem não ser decifradas pelo destinatário de forma correta devido à complexidade da Chave. Com esse dilema, no lugar de escolher ao acaso o alfabeto para criar uma cifra, o emissário deve escolher primeiro uma palavra chave ou frase chave, depois deve remover qualquer espaço ou letra repetida, sendo este resultado o início do alfabeto cifrado e o resto é meramente uma mudança que começa onde a frase cifrada termina, omitindo-se as letras que já existem na frase chave.

Por exemplo, se escolhermos a frase-chave: CRIPTOGRAFIA É A CHAVE, teremos o seguinte alfabeto cifrado:

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

Tabela 2: Exemplo Cifra de César com substituição de frase chave

Podemos também substituir cada letra do alfabeto por um símbolo distinto, por exemplo, a por +; b por @ e assim por diante, tornando ainda mais complexo o algoritmo e a chave.

Assim, nas cifras de substituição as letras da mensagem original são tratadas individualmente ou em grupos de comprimento constante, são substituídas por outras letras, figuras, símbolos ou uma combinação destes de acordo com um sistema predefinido e uma chave. Resumindo, as letras mudam sua identidade e mantêm suas posições.

Quando para a substituição utiliza-se apenas um alfabeto, como exemplo a Cifra de César, a substituição é chamada de *monoalfabética* e caso contrário, utilize mais de um alfabeto é chamada de *polialfabética*.

Segundo Singh [26], "monoalfabética é o nome dado a qualquer cifra de substituição na qual o alfabeto cifrado pode consistir em símbolos, letras assim como uma mistura de letras e ou símbolos."

A substituição monoalfabética divide-se em monogâmicas, poligâmicas e tomogâmicas. Na monogâmica cada caractere da mensagem original é substituído

por outro, o comprimento da mensagem original é igual ao da cifrada e a frequência da ocorrência das letras também é o mesmo. Já as poligâmicas têm a diferença que se substitui grupos de caracteres da mensagem original por um ou mais caracteres, geralmente mudando o comprimento da mensagem depois de cifrada. No sistema tomogâmicos cada letra é substituída por duas ou mais letras, símbolos ou números, consequentemente, o criptograma será maior que a mensagem original.

A Cifra de Substituição Monoalfabética foi muito utilizada durante o primeiro milênio graças a sua força e simplicidade, porém a riqueza da cultura islâmica desenvolveu uma técnica que quebrou a chave de qualquer Criptografia de Substituição Monoalfabética, a conhecida análise de frequência, qual se fundamenta no fato de algumas palavras ou letras serem mais comuns do que outras em um determinado idioma. Essa técnica foi descrita nas obras de um importante cientista do século IX conhecido como *al-Kindi*, que consiste em verificar a frequência das palavras e letras de uma mensagem comparando-a com um texto diferente, suficientemente longo e na mesma língua. Verificando qual a letra mais utilizada naquela língua, qual a segunda mais utilizada e assim por diante, conseguindo a chave para decifrar a mensagem. De modo geral, quanto mais longo o texto, maior a probabilidade de apresentar a frequência padrão do idioma.

Atualmente, existe análise da frequência de várias línguas facilmente disponíveis. E também se pode analisar os digramas e trigramas mais frequentes da língua que se quer decifrar e por fim, desvenda-se a mensagem secreta.

O site aldeianumaboa [1] tabulou a Frequência das Letras na Língua Portuguesa, depois de analisadas 157.764 palavras com 725.511 letras, transformando vogais acentuadas em normais e cedilha em c é a seguinte:

Alfabeto	Porcentagem	Alfabeto	Porcentagem
a	14,63	n	5,05
b	1,04	o	10,73
c	3,88	p	2,52
d	4,99	q	1,20
e	12,57	r	6,53
f	1,02	s	7,81
g	1,30	t	4,34
h	1,28	u	4,63
i	6,18	v	1,67
j	0,40	w	0,01
k	0,02	x	0,21
l	2,78	y	0,01
m	4,74	z	0,47

Tabela 3: Frequência de letras na Língua Portuguesa

Portanto, se desejarmos enviar uma mensagem secreta com segurança, a Criptografia de substituição monoalfabética não é recomendada por ser facilmente decifrada. Mas, há outros métodos utilizados que dificultam o texto ser decifrado, por exemplo, não utilizar a letra de maior frequência da língua utilizada, qual foi feito pelo romancista Georges Perec quando escreveu *La Disparition* e este mesmo livro foi traduzido para o inglês por Gilbert Adair, qual manteve a ausência da letra "e", neste caso a mais frequente na língua inglesa.

Depois da descoberta da técnica de análise de frequência e da sua fraqueza houve a necessidade da criação de uma cifra mais segura. Uma das mudanças mais simples para a cifra de substituição foi a inclusão de nulos, ou seja, letras, símbolos que não eram equivalentes às letras verdadeiras da mensagem. Por exemplo, podemos substituir as 26 letras do alfabeto por números de 1 a 100, sobrando assim, 74 números que não representariam letra alguma. Estes poderiam ser distribuídos pela mensagem criptografada em várias frequências. Outra saída encontrada para aumentar a segurança de uma cifra, foi escrever uma mensagem com a ortografia errada e depois cifrá-la.

Com o desenvolvimento da criptoanálise, a existência de cifras mais seguras se tornara uma necessidade para vencer os criptoanalistas, mas isto surgiu de fato apenas no século XVI, quando o diplomata francês Blaise de Vigenère, em sua obra *Traicté dés Chiffres* publicado em 1586, concluiu e aperfeiçoou o trabalho de Leon Alberti, arquiteto italiano considerado pai da cifra polialfabética, que consistia o uso de dois ou mais alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas da época. Criou uma nova cifra, chamada de *Le Chiffre Indechifrable* que significa A Cifra Indecifrável, conhecida também como Cifra de Vigenère em homenagem a seu criador, onde é usado 26 alfabetos cifrados distintos.

	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

Tabela 4: Quadrado de Vigenère

Observa-se na tabela 4, 26 alfabetos cifrados conforme a Cifra de César, sendo um dos alfabetos o alfabeto original, logo o remetente pode agora, por exemplo, cifrar a primeira letra de sua mensagem de acordo com o alfabeto 5, a segunda letra de acordo com o alfabeto 14 e assim por diante, tendo 26 alfabetos cifrados distintos a sua disposição.

Para decifrar a mensagem, o destinatário precisa saber que linha do quadrado de Vigenère foi usada para cifrar cada letra e como a mesma letra pode ser escrita de até 26 formas diferentes, de nada adiantará os criptoanalistas usarem a técnica da frequência das letras. O único problema deste modo de Criptografia é que se faz necessário que o destinatário não confunda a linha utilizada em cada letra, e a solução é usar uma palavra-chave, por exemplo, DECIFRAR. A palavra-chave indica qual linha do quadrado de Vigenère usar. Na primeira letra usa-se a linha do D, correspondente a linha número 04, na segunda letra a linha do E, correspondente a linha 05, e assim por diante até usar a linha do R, que é a linha do 18, na oitava letra. Na nona letra, repete-se o processo, usando a linha D novamente e assim sucessivamente até chegar ao fim da mensagem.

Por usar não somente um alfabeto para cifrar a mensagem, mais sim vários, dependendo da palavra chave, a criptografia usando o quadrado de Vigenère é polialfabética.

Apesar deste tipo de Cifra ser segura, foi negligenciada durante os 2 séculos seguintes após sua descoberta por ser considerada muito complexa.

> "Em consequência disso, os criptógrafos buscaram uma cifra intermediária, mais difícil de quebrar do que a cifra monoalfabética direta, mas que fosse mais simples de usar do que a cifra polialfabética." (Singh [26])

Foi onde criou-se a Cifra de Substituição Homofônica, na qual cada letra é substituída por uma variedade de símbolos proporcional à sua frequência. Por exemplo, a letra e na língua portuguesa poderá ser substituída por 12 símbolos distintos, pois sua frequência é de 12,57% (vide tabela 3), cada vez que a letra e for aparecer no texto cifrado, será escolhido ao acaso qual dos 12 símbolos usar, e assim ocorrendo com as demais letras, de modo que no final do texto, cada símbolo representará 1% do texto cifrado, despistando a técnica da análise da frequência.

Este método foi mais utilizado do que a Cifra de Vigenère, por ser mais simples de ser usado e por representar certo grau de segurança para a época. Porém, os criptoanalistas também conseguiram quebrá-lo, estudando as letras que apresentam um único símbolo para representá-la e que fazem parte de dígrafos ou trígrafos comumente usados na língua, deixando evidente que a Cifra de Vigenère oferecia maior segurança.

Porém, em 1854, Charles Babbage, matemático britânico já tinha decriptado a Cifra de Vigenère analisando em que frequência as letras se repetiam e descobrindo a palavra-chave usada, mas ele não publicou sua descoberta. Em 1863, Friedrich Kasiski publicou a técnica e então a Cifra de Vigenère não era mais segura oficialmente.

A partir daí, houve uma série de Criptografias que eram ou de Tranposição ou de Substituição ou ainda, uma combinação das duas, mas os Criptoanalistas não demoravam a decriptá-las.

Samuel Morse, americano, em 1838, inventou o telégrafo eletromagnético e concomitantemente o código Morse, onde as letras do alfabeto são substituídas por pontos e traços, e após, criou um receptor acústico, de modo que o destinatário ouvisse as letras através de bips.

Em 1894, com a descoberta do rádio, um importante meio de comunicação que serviu na época para enviar mensagens militares através do código Morse, e sem fios interligando remetente e destinatário, ficou mais fácil a interceptação das mensagens e consequentemente concedeu várias vitórias para os criptoanalistas na Primeira Guerra Mundial.

A cifra ADFGVX, muito famosa na Primeira Guerra Mundial e que inclui os dois métodos de criptografar, transposição e substituição, foi decifrada em 3 meses

de utilização. Seu processo de criptografia consistia em construir um quadro com as 6 letras ADFGVX na horizontal e na vertical e escrever aleatoriamente as 26 letras do alfabeto e mais os 10 dígitos. A escolha das letras ADFGVX, deve-se ao fato de que, as mesmas em código Morse são muito diferentes.

/	A	D	F	G	V	X
A	k	1	g	y	5	f
D	l	a	4	h	2	m
F	s	3	z	q	7	t
G	v	j	b	9	i	e
V	r	8	p	w	0	u
X	c	x	6	o	d	n

Tabela 5: Exemplo de disposição da Cifra ADFGVX

A substituição se dá, por exemplo, para cifrar a palavra CRIPTOGRAFIA temos AX AV VG FV XF GX FA AV DD XA VG DD. E para a transposição precisamos de uma palavra chave, como VOCE, então reescrevemos o texto cifrado num quadro junto à palavra chave (tabela 6), e arrumamos a palavra chave em ordem alfabética, transpondo as colunas (tabela 7). Sendo a mensagem final AVXAFVGVGXFXAVAFXADDDDGV e esta seria transmitida via rádio usando o código Morse.

V	O	C	E
A	X	A	V
V	G	F	V
X	F	G	X
F	A	A	V
D	D	X	A
V	G	D	D

Tabela 6: Organização da Cifra ADFGVX com palavra chave

C	E	O	V
A	V	X	A
F	V	G	V
G	X	F	X
A	V	A	F
X	A	D	D
D	D	G	V

Tabela 7: Transposição da Cifra ADFGVX

Ficou evidente a necessidade de uma criptografia mais forte e então só no fim da Primeira Guerra Mundial, cientistas da América descobriram que se usassem uma frase-chave tão grande quanto o tamanho da mensagem que precisava ser enviada, a técnica de decifrar desenvolvida por Babbage e Kasiski não iria funcionar e assim começaram a desenvolver métodos e máquinas, com a tecnologia que dispunham na época, para aperfeiçoar cada vez mais as frases-chaves, até que fossem letras aleatórias, distribuídas em blocos de papel.

No século XV foi inventada a primeira máquina criptográfica por Alberti, que reproduzia um deslocamento simples de César, através de dois discos que continham o alfabeto gravado e podiam ser girados, um deles continha o alfabeto original e o outro o alfabeto cifrado. Podendo ainda esta máquina gerar uma cifra polialfabética, bastava girar o segundo disco durante a mensagem. Em 1918, Arthur Scherbius patenteou uma máquina elétrica e mecânica com rotores, qual pode ser considerada uma versão elétrica da máquina de Alberti, chamada de Enigma, que servia tanto para criptografar como para decriptografar, e foi amplamente usada pelas forças militares alemãs. No projeto de Scherbius a máquina continha três discos que eram os misturadores, as letras do texto original sofriam uma substituição, através da rotação desses três discos, quais continham as 26 letras do alfabeto, fornecendo assim, $26 \times 26 \times 26 = 17576$ ajustes diferentes de misturadores. Agregando essa orientação a outras variáveis da máquina, havia no total 10.000.000.000.000.000 chaves. Para decifrar a mensagem o destinatário teria que ter uma cópia do livro contendo os ajustes iniciais e outra máquina enigma.

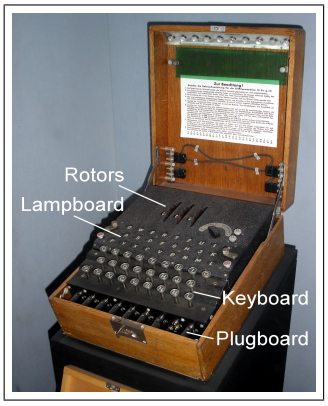


Figura 2: Enigma

Em 1931, o *Biuro Szyfrów*, departamento de códigos do Serviço Secreto da Polônia, depois de conseguir uma cópia do projeto da Máquina Enigma, por um traidor alemão, decide contratar matemáticos para decriptografá-la. Entre eles, Marian Rejewski, que dedicou-se muito na quebra da Enigma, depois das suas descobertas, as comunicações da Alemanha ficaram acessíveis. Os Poloneses usaram por vários anos as técnicas de Rejewski, até que os alemães fizeram alterações na transmissão de suas mensagens, em contrapartida, Rejewski, consegue construir outra máquina, chamada de Bomba e decriptografa a Enigma sem os alemães saberem. Singh [26] diz que, "O sucesso polonês na quebra da Enigma pode ser atribuído a três fatores: medo, matemática e espionagem."

Porém, os alemães foram aperfeiçoando a Enigma usando uma combinação maior de rotores e ligações elétricas e em 1939, a Bomba de Rejewski estava ultrapassada e então, os poloneses passaram tudo o que sabiam aos ingleses e franceses antes de serem invadidos pela Alemanha. Em *Bletchey Park*, sede da Escola de Cifras e Códigos do governo na Inglaterra, com mais recursos e cientistas disponíveis, eles puderam então decriptografar novamente a Enigma. Numa combinação de matemáticos, cientistas, linguistas, especialistas da cultura clássica, mestres de xadrez e viciados em palavras cruzadas, destaca-se o matemático Alan Turing, que teve papel fundamental na base da Ciência da Computação e durante a II Guerra na quebra dos códigos da Enigma, criando uma máquina, conhecida por Bomba também, devido a semelhança da máquina de Rejewski, após aperfeiçoamentos a nova máquina conseguia encontrar a chave de uma Enigma em uma hora.

Depois da Bomba de Turing, vieram muitas outras máquinas mais aperfeiçoadas. A mais importante delas foi a Lorenz SZ40, responsável pela comunicação entre Hitler e seus generais, semelhante a Enigma, porém, mais evoluída, o que deu muito trabalho para ser decifrada em *Bletchey Park*. Até que o matemático Max Newman projetou como mecanizar a criptoanalise da Lorenz, com base nas já ultrapassadas Bombas. A máquina foi chamada de Colossus, ela tinha 1500 válvulas eletrônicas e era programável, fato esse que faz da Colossus o pri-

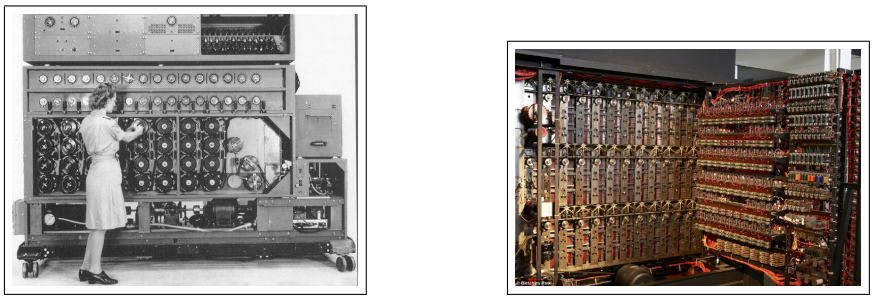


Figura 3: Bomba de Rejewski e Bomba de Turing

meiro computador. Como a máquina e seus projetos foram destruídos após a II Guerra, durante décadas considerou-se que a ENIAC (*Electronic Numerical Integrador And Calculator*) fosse precursora do computador moderno.

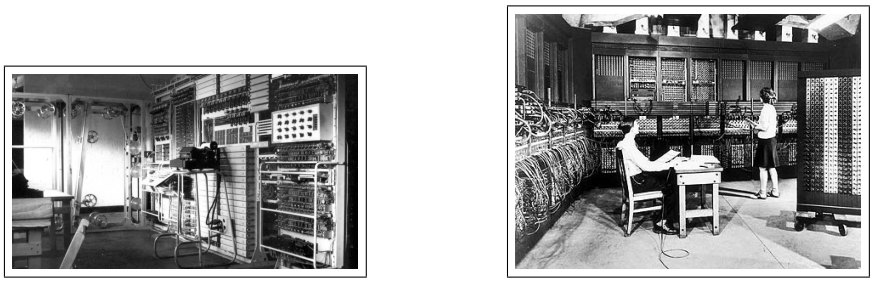


Figura 4: Colossus e ENIAC

Paralelamente à Inglaterra, os Estados Unidos também possuíam seus Criptoanalistas. Todos ficaram anônimos depois da Guerra, mas foram essenciais contra as Forças Japonesas na Segunda Guerra.

Após um ataque do Japão, em 1941, surgiu a ideia de colocar o povo *Navajo* para criptografar as mensagens de guerra dos Estados Unidos, considerando que a linguagem *Navajo* era extremamente complexa, pois não possuía escrita e sua pronúncia era complicada. O comando naval recrutou 200 índios, ficando conhecidos por *Code Talkers*, e foram incorporados aos fuzileiros. Em 1942 foi criado o código *Navajo* e um dicionário com associações do dialeto Navajo aos termos militares.

Exemplos:

besh-lo (peixe de ferro) = submarino

dah-he-tih-hi (beija-flor) = avião de caça

Apesar de os japoneses serem especialistas em decifrar códigos em inglês e em muitas línguas europeias, seus homens jamais haviam conseguido quebrar aquele estranho código usado pelos Fuzileiros, o código Navajo. E a última mensagem enviada em código Navajo foi realizada em 1945.

Então foi criada em 1952 a NSA (*National Security Agency*), e apenas revelada em 1982, é a Agência Nacional de Segurança dos Estados Unidos que garante a proteção das Comunicações dos Estados Unidos e a Criptologia é uma de suas funções. É a organização que mais emprega matemáticos no mundo. Além disso, possui os mais poderosos computadores já fabricados.

Hard [12] acreditava que, *"Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers."*

Na verdade a Criptografia teve uma grande importância nos acontecimentos históricos, principalmente nas guerras, de acordo com Sir Harry Hinsley *in* Singh [26]:"a guerra, em vez de acabar em 1945, teria terminado em 1948, se a Escola de Códigos e Cifras do Governo não fosse capaz de ler as cifras Enigma..."

Com a criação do computador, os criptógrafos iniciaram a busca por cifras mais difíceis e complexas, e também, desenvolveram técnicas para quebrar as cifras, podendo pesquisar chaves com uma maior velocidade. Como diz Singh [26], "... o computador pode simular uma máquina de cifragem hipotética de imensa complexidade."

A utilização de computadores ao invés das máquinas mecânicas tem três principais diferenças, um computador pode ser programado para simular centenas de misturadores, com vários sentidos e ordem, é muito mais veloz e o computador mistura números ao invés de letras do alfabeto.

O computador trabalha com números binários, ou seja, um sistema de numeração posicional de base 2, ao invés da conhecida base decimal, onde os números são representados por sequências formadas por apenas dois dígitos: 0 ou 1, essas são chamadas de dígitos binários, *bits (binary digits*, em inglês).

Por exemplo, o número decimal 116 é representado no sistema binário como $01110100 = 0 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 + 1 \times 2^4 + 1 \times 2^5 + 1 \times 2^6 + 0 \times 2^7$.

Bit é a menor unidade de informação que pode ser armazenada ou transmitida, podendo assumir dois valores: 0 ou 1. O computador é projetado para armazenar instruções em múltiplos de *bit*.

A ASCII, *American Standard Code for Information Interchange*, destina que cada letra do alfabeto e cada símbolo corresponde um número binário de 7 dígitos, dando ao todo um conjunto de 128 caracteres que podem ser usados na digitação. Por exemplo e conforme a tabela 8, a letra A corresponde ao *bit* 1000001, C ao 1000011, F ao 1000110, I ao 1001001 e R ao *bit* 1010010, escrevendo CIFRA temos a palavra cifrada em *bits* como 1000011 1001001 1000110 1010010 1000001.

A	1000001	H	1001000	O	1001111	V	1010110
B	1000010	I	1001001	P	1010000	W	1010111
C	1000011	J	1001010	Q	1010001	X	1011000
D	1000100	K	1001011	R	1010010	Y	1011001
E	1000101	L	1001100	S	1010011	Z	1011010
F	1000110	M	1001101	T	1010111		
G	1000111	N	1001110	U	1010101		

Tabela 8: ASCII

Vamos destacar dois exemplos simples de cifragem por computador. Um deles é por transposição, que consiste em trocar os dígitos da mensagem, troca-se o primeiro e o segundo dígito, o terceiro e o quarto, e assim por diante. Criptografando a palavra CIFRA desta forma, teríamos:

```
Palavra original: 1000011 1001001 1000110 1010010 1000001
Palavra cifrada:  0100101 1000110 0100111 0100001 0100001
```

Ainda podemos criptografar a palavra CIFRA através de uma cifra de substituição, do seguinte modo, escolhemos uma chave com a mesma quantidade de letras, como JOIAS, que em *bits* via ASCII é 1001010 1001111 1001001 1000001 1010011, então, na junção da mensagem com a palavra-chave, se os dígitos são os mesmos na mensagem criptografada temos 0 e se os dígitos são diferentes temos 1. Com o exemplo dado, obtemos a mensagem criptografada assim:

1000011100100110001101010010100001
1001010100111110010011000011010011
0001001000011000011110010011001010 → mensagem criptografada

E atualmente, como 1 *byte* tem 8 *bits*, ou seja, temos 256 caracteres, a cada letra do alfabeto ou símbolo corresponde um número binário de 8 dígitos, apesar de ter tido tamanho variável. Usando o mesmo exemplo da cifra de substituição, CIFRA ficaria assim com os 8 dígitos: 01000011 01001001 01000110 01010010 01000001, e a palavra-chave JOIAS: 01001010 01001111 01001001 01000001 01010011, fazendo o mesmo processo descrito em 7 dígitos, temos:

0100001101001001010001100101001001000001
0100101001001111010010010100000101010011
0000100100000110000011110001001100010010 → mensagem criptografada

Contudo, os computadores eram restritos ao governo e aos militares. Com a popularização dos computadores, primeiramente houve a preocupação em uma padronização, de forma que empresas, pessoas pudessem se comunicar usando

um mesmo sistema de cifragem. Em 1970, Horst Feistel desenvolveu um dos algoritmos de cifragem mais usados, conhecido como Lucifer, no qual o emissor e o receptor só precisavam escolher um número para decidir qual chave seria usada. Uma versão de 56 *bits* da cifra Lucifer foi oficialmente adotada e batizada como Padrão de Cifragem de dados (DES–*Data Encryption Standard).* A DES garantia a segurança das mensagens, encorajando as empresas a utilizarem a criptografia, havia apenas um problema, a distribuição de chaves.

Na década de 1960, a ARPA, Agência de Projetos Avançados de Pesquisa, financiado pelo Departamento de Defesa dos Estados Unidos, tinha como um de seus projetos encontrar uma forma de conectar os computadores através de grandes distâncias, em 1969 nasce a ARPANet, qual em 1982 deu origem à internet.

Com a internet onde as mensagens são enviadas pela linha telefônica fez-se necessário uma Criptografia muito mais complexa e difícil de ser quebrada. Mesmo que a mensagem não seja um segredo de Estado, pode ser o número do cartão de crédito em uma compra pela internet, a segurança dos dados é um problema de vital importância.

A distribuição de chaves, que emissor e receptor conhecesse, se tornou um dos problemas da Criptografia, pois com toda essa popularização eram agora milhares de pessoas que necessitavam de chaves para, principalmente, atividades financeiras. Era, por exemplo, bastante complicado e oneroso para um banco distribuir e entregar as chaves a todos os seus clientes.

Whitefield Diffie, Martin Hellman e Ralph Merkle estavam dispostos a resolver este problema, suas pesquisas concentravam-se em funções matemáticas. Uma definição para função é:

> "Sejam A e B dois conjuntos. Chamamos de função do conjunto A no conjunto B a uma regra que a cada elemento de A associa um único elemento de B, e denotamos simbolicamente por $f : A \to B$, $a \mapsto f(a)$, onde para cada $a \in A$ está associado um único $b = f(a) \in B$, através da regra que define f."

Essas são regras que associam um número a outro número, muitas funções são inversíveis (funções de mão dupla), ou seja, podemos aplicar uma regra a um número e conseguimos encontrar outra regra que desfaça a operação empregada, obtendo assim, o número inicial. Mas o foco das pesquisas eram as funções que possuíam regras difíceis de serem desfeitas.

Então, Diffie, Hellman e Merkle propuseram uma Cifra, para troca de chaves de uma forma segura, onde a mensagem secreta era codificada e decodificada por duas chaves diferentes, a do remetente e a do destinatário, sem que precisassem trocá-las entre si. O sistema Diffie–Hellman–Merkle consistia na ideia que tanto o emissor como o receptor aplicassem uma função genérica, difícil de ser revertida, em um número escolhido em segredo, trocassem os resultados, que não comprometeriam a comunicação se fossem descobertos por alguém, novamente ambos

aplicariam a mesma função utilizando o número que era segredo ao resultado recebido e encontrariam assim um mesmo número, que seria a chave.

Em 1975, Diffie pensou em um outro tipo de cifra, esta consistia em o emissor criar seu próprio par de chaves: uma chave de cifragem e uma de decifragem. Através de um computador isso aconteceria da seguinte forma: uma pessoa escolheria um número que seria sua chave de cifragem e um outro número que seria sua chave de decifragem, este seria mantido em segredo, chamado de chave particular. A chave de cifragem é divulgada, para que todos tenham acesso, esta é chamada de chave pública. Se alguém quiser mandar uma mensagem a esta pessoa, ele utiliza a chave pública para cifrar a sua mensagem, envia à pessoa de seu interesse, qual, com sua chave particular, irá decifrar a mensagem recebida.

Esse foi o fim da chave simétrica, utilizada em todas as outras técnicas de cifragem, onde ambos usam a mesma chave, e o processo da decifragem era apenas o oposto da cifragem. A partir de então, entrou em vigor a chave assimétrica, qual utiliza a chave pública e chave particular, neste tipo de cifra uma pessoa pode cifrar uma mensagem, mas não pode decifrar. A vantagem desse sistema é que não há troca de chaves.

O sistema estava longe de ser algo simples, pois para ser incorporado num sistema criptográfico operacional necessitava de uma função matemática difícil de ser revertida. Após exaustivas pesquisas e tentativas, eles encontraram uma saída na Aritmética Modular, desenvolvendo então, o método RSA, utilizado até hoje. Ambos serão apresentados com mais detalhes nos capítulos seguintes.

1.1 Aplicações Sala de Aula

Bem sabemos que ensinar matemática fazendo cálculos desprovidos de utilidade e contextualização gera muitas vezes problemas na relação professor-aluno, além de dificuldades em aprender o conteúdo, seja no ensino fundamental ou médio. Uma solução seria o profesor apresentar aos alunos a origem da criptografia, sua evolução e presença no cotidiano.

Nas Diretrizes Curriculares de Educação do Paraná (DCE's) [7] consta que:

> "Essa argumentação chama a atenção para a importância da práxis no processo pedagógico, o que contribui para que o conhecimento ganhe significado para o aluno, de forma que aquilo que lhe parece sem sentido seja problematizado e aprendido."

Nos Parâmetros Curriculares Nacionais (PCNs) das séries iniciais [20] temos que:

> "—A Matemática é componente importante na construção da cidadania na medida em que a sociedade se utiliza cada vez mais de conhecimentos científicos e recursos tecnológicos dos quais os cidadãos devem se apropriar.

—A Matemática precisa estar ao alcance de todos e a democratização do seu ensino deve ser prioritária do trabalho docente.

—A atividade matemática escolar não é "olhar para coisas prontas e definitivas" mas a construção e a apropriação de um conhecimento pelo aluno, que se servirá dele para compreender e transformar sua realidade.

—No ensino da Matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações(esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo a comunicação tem grande importância e deve ser estimulada levando-se o aluno a "falar" e a "escrever" sobre matemática... ."

Também os PCNs para o ensino médio [19] reforçam:

"—Desenvolver a capacidade de utilizar a Matemática na interpretação e interveção social.

—Aplicar conhecimentos e métodos matemáticos em situações reais, em especial em outras áreas do conhecimento.

—Relacionar etapas da história da Matemática com a evolução da humanidade.

—Utilizar adequadamente calculadoras e computador reconhecendo suas limitações e Potencialidades... ."

E ainda A Lei de Diretrizes e bases da Educação Nacional [15] coloca que o ensino médio apresenta as seguintes finalidades:

- " a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação e aperfeiçoamento posteriores;
- a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina... ."

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

As atividades expostas abaixo podem ser aplicadas nos diversos níveis de ensino de matemática, cabe ao professor observar em que nível seus alunos estão para seleção dessas atividades. Cada problema está resolvido e detalhado, e estão disponíveis para cópia nos anexos.

Esses exercícios estão organizados em nível 1 e 2, sendo o primeiro aplicados ao ensino fundamental e o segundo ao ensino médio, observe que a divisão em

níveis é preferencialmente e não obrigatoriamente, muitos exercícios do nível 1 podem ser feitos por alunos do ensino médio e vice – versa, mas alguns do nível 2 envolvem conteúdos específicos do ensino médio e, é claro, o grau de dificuldade é maior.

Os problemas abaixo são de criptografia e criptoanálise por permutação, por permutação em blocos, e pelo sistema cerca de ferrovia, todos usam o método de transposição e cifras. Embora o conteúdo específico de permutação, possibilidades e contagem esteja inserido no currículo do ensino médio, podemos iniciá-lo no ensino fundamental, com o objetivo de estimular o raciocínio lógico, interpretação e ainda trabalhar possibilidades e contagem, cujo os alunos já trazem na sua bagagem tais preceitos.

Nível 1

1) Alice cifrou a palavra PAZ usando permutação das letras e mandou através de um bilhete para sua colega Fernanda. De quantas, e quais as maneiras Fernanda pode ter recebido esse bilhete?

Maneiras = anagramas: PAZ, PZA, AZP, APZ, ZAP, ZPA.
Quantidade: 6 maneiras de receber a mensagem($P_3 = 3! = 3 \cdot 2 \cdot 1 = 6$).

2) Você e seus amigos tem um grupo no WhatsApp. Robson enviou ao grupo SARERPSU! Propondo que pagaria uma pizza para quem decifrasse. Decifre a mensagem.

Chave: Separar em blocos de 2 letras, permutar 1º e 4º bloco e permutar 2º e 3º bloco.
Processo:SA RE RP SU $\longrightarrow$ blocos de 2 letras
SU RP RE SA $\longrightarrow$ permutação
Mensagem: SURPRESA!

3) No intervalo da aula, Ana recebeu no celular a seguinte mensagem: ECOVE DNILA, que está criptografada. Decripte-a para Ana.

Chave: Separar em blocos de 5 letras, permutar 1ª e 4ª letra e permutar 2ª e 3ª letra em cada bloco.
Processo:ECOVE DNILA $\longrightarrow$ blocos de 5 letras
VOCEE LINDA $\longrightarrow$ permutação
Mensagem:VOCÊ É LINDA.

4) Carlos quer convidar para o seu time de futebol um aluno artilheiro de outra turma, mas ninguém pode saber. Como são muito amigos eles já têm acordado

um método de criptografia por ferrovia em duas linhas. Como ficará cifrada a pergunta: QUER SER DO MEU TIME NO TORNEIO DA ESCOLA?

Processo:

```
Q  U  E  R  S  E  R  D  O  M  E  U  T  I  M  E  N

  O  T  O  R  N  E  I  O  D  A  E  S  C  O  L  A  ?
```

Mensagem: QOUTEORRSNEERIDOODMAEEUSTCIOMLEAN?.

Nível 2

1) João precisa mandar para Aline a mensagem: ME ENCONTRE NA ESCOLA. Os dois têm conhecimento da chave: blocos de 3 letras, permutação entre 1º e 2º bloco, 3º e 4º bloco e assim por diante até terminarem os blocos, e permutação entre a 1ª e 3ª letra de cada bloco. Como Aline receberá a mensagem?

Chave: separar em blocos de 3 letras, permutar 1ª e 3ª letra, permutar 1º e 2º, 3º e 4º, 5º e 6º blocos.
Processo:MEE NCO NTR ENA ESC OLA⟶blocos de 3 letras
NCO MEE ENA NTR OLA ESC⟶permutação dos blocos
OCN EEM ANE RTN ALO CSE⟶permutação das letras
Mensagem: OCNEEMANERTNALOCSE

2) Considere: TAME TAMI EACL AGEL

a) O que está escrito nessa mensagem?

Processo: TAME TAMI EACL AGEL
MATE MATI CAEL EGAL ⟶ permutação entre 1ª e 3ª letra em cada bloco
Mensagem: MATEMÁTICA É LEGAL.

b) Qual a chave de permutação?

Chave: Separar a frase em blocos de 4 letras e permutar em cada bloco a 1ª e 3ª letra, mantendo a posição das outras letras.

c) Quantas permutações são possíveis em cada bloco?

Solução: $P_4 = 4! = 24$.

d) Se cada bloco usar uma permutação diferente dos demais, de quantas formas poderei escrever a mensagem?

Solução:
1º bloco = 24 maneiras
2º bloco = 23 maneiras
3º bloco = 22 maneiras
4º bloco = 21 maneiras
24.23.22.21 = 255024 formas de escrever a mensagem.

3) Quantos anagramas a palavra ESCOLA tem se:

a) S for a primeira letra?

Solução: $P_5 = 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ anagramas.

b) S for a primeira e C a última letra?

Solução:$P_4 = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ anagramas.

c) S for a primeira, C a última letra e as letras OL permanecerem juntas nessa ordem?

Solução:$P_3 = 3! = 3 \cdot 2 \cdot 1 = 6$ anagramas.

4) Decifre o ditado popular usando a cerca de ferrovia e diga quantas linhas você precisa usar:
AIESDOGCEEROEUSISMSCCLAIOOHORNMEPMHIAOAELPBOCAARS EMREOM
Processo: Como o ditado tem 55 letras, o mais coerente é divisão em 5 linhas com 11 letras cada.

```
A   O   R   I   C   O   M   I   L   A   M

  I   G   O   S   L   H   E   A   P   A   R

    E   C   E   M   A   O   P   O   B   R   E

      S   E   U   S   I   R   M   A   O   S   O

        D   E   S   C   O   N   H   E   C   E   M
```

Mensagem: AO RICO, MIL AMIGOS LHE APARECEM, AO POBRE, SEUS IRMÃOS O DESCONHECEM.

Os próximos exercícios abordam a Cifra de César, alguns com palavra-chave e outros não, para criptografar e decifrar utilizaram-se o deslocamento de três letras, igual a usada por Júlio César, e outros deslocamentos. Lembrando que essa cifra de substituição é bastante simples, se nos basearmos nos padrões de hoje, mas ela foi bastante utilizada e é a ideia do disco decodificador, utilizados nas máquinas de criptografar que surgiram. Esse método desenvolve, assim como os outros, a observação, o raciocínio e a identificação de um padrão, de uma regra para a substituição.

Para o deslocamento de três letras deve-se utilizar a tabela 1, para outros deslocamentos ou para quando há chave deve-se montar uma tabela com o alfabeto original e o cifrado.

Nível 1

1) Júlio César, Imperador Romano, costumava utilizar a criptografia para se comunicar com seus exércitos. Decifre a mensagem que Júlio enviou, ao seu oficial Cícero, utilizando a Cifra de César: DMXGDHVWDDFDPLQKR.

Processo: Observar na tabela 1, qual apresenta o deslocamento de César, e substituir as letras da mensagem cifrada pelas letras do alfabeto original.

Mensagem: AJUDA ESTÁ A CAMINHO.

2) Dudu gostou muito da Cifra de César e resolveu usá-la para mandar um recado ao seu amigo Daniel. Como Daniel receberá a seguinte mensagem?

DANI VAMOS JOGAR VIDEO GAME HOJE A TARDE?

Processo: Observar na tabela 1, qual apresenta o deslocamento de César, e substituir as letras da mensagem pelas letras do alfabeto cifrado.

Mensagem: GDQLYDPRVMRJDUYLGHRJDPHKRMHDWDUGH?

Nível 2

1) Edgar Allan Poe, autor do conhecido poema O Corvo, tinha um grande interesse por códigos e cifras, em seu conto mais famoso O Escaravelho de Ouro, o protagonistas tem que decifrar uma mensagem. Agora, decripte uma de suas frases, onde a chave é o título do seu conto mais famoso.

"CARHYZOBZAIHCOIBOWOMGOISZXZSGHSOZGHJXHSOCOEAWATO.
ZIAKKYHSZDKHTAZVZIJZ."

Chave: O Escaravelho de Ouro

Processo: Deve-se remover os espaços entre as palavras do título do conto e as letras repetidas: OESCARVLHDU, esse será o início do alfabeto cifrado e o resto continua onde a frase cifrada termina, omitindo as letras que já aparecem na frase chave e seguindo a ordem do alfabeto original. Montando uma tabela com o alfabeto original e na linha abaixo o cifrado obtemos:

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

Mensagem: "DEFINO A POESIA DAS PALAVRAS COMO CRIAÇÃO RÍTMICA DA BELEZA. O SEU ÚNICO JUIZ É O GOSTO. "

2) Descubra o título de uma das obras de Dalton Trevisan, escritor curitibano, sabendo que na cifragem foi utilizado algum dos 26 deslocamentos possíveis.
TBQJHRPSTRJGXIXQPETGSXSP

Processo: Quando não se sabe qual é a quantidade de letras deslocadas, deve-se fazer por tentativa, excluindo os casos pouco prováveis na língua portuguesa, por exemplo, é pouco provável que o título inicie com K, Y, W, a não ser que seja alguma palavra estrangeira ou nome próprio, mas, é menos provável, então inicia-se as tentativas pelas letras de maior ocorrência no nosso idioma, e também, observa-se as sílabas ou pares de letras formados, por exemplo, se na tentativa, você achar que uma das letras é Q, então a próxima terá que ser U, pensando no nosso idioma. Após tentativas, deve-se concluir que o deslocamento utilizado foi de 15 casas e monta-se a tabela do alfabeto original e o cifrado:

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

Título: EM BUSCA DE CURITIBA PERDIDA.

A seguir, trataremos nos exercícios a criptografia e a criptoanálise utilizando-se da cifra de Vigenère, uma cifra polialfabética de substituição. Esse sistema de criptografar mostra para o aluno como seguir coordenadas, encontrando e substituindo letras, pois é com base nessas coordenadas que ele conseguirá cifrar

e decifrar textos. Em todas as atividades usaremos a tabela 4 - Quadro de Vigenère.

Nível 1

1) Com a palavra-chave CÓDIGO, cifre o verso abaixo de Memória (Carlos Drummond de Andrade) pelo quadro de Vigenère.

"Mas as coisas findas
muito mais que lindas,
essas ficarão."

Chave: CÓDIGO, que em números é 03-15-04-09-07-15, de acordo com a ordem no alfabeto.

Processo: Completar a tabela abaixo seguindo coordenadas na tabela 4.

3M	15A	4S	9A	7S	15C	3O	15I	4S	9A	7S	15F	3I	15N	4D	9A
P	P	W	J	Z	R	R	X	W	J	Z	U	L	C	H	J
7S	15M	3U	15I	4T	9O	7M	15A	3I	15S	4Q	9U	7E	15L	3I	15N
Z	B	X	X	X	X	T	P	L	H	U	D	L	A	L	C
4D	9A	7S	15E	3S	15S	4A	9S	7F	15I	3C	15A	4R	9A	7O	
H	J	Z	T	V	H	E	B	M	X	F	P	V	J	V	

Verso cifrado: PPW JZ RRXWJZ ULCHJZ
RXXXX TPLH UDL ALCHJZ,
TVHEB MXFPVJV.

Nível 2

1) A frase VPKMJOCGPJYIAVZRPJ está cifrada de acordo com o quadro de Vigenère. Em posse da código-chave L3P11, que está no texto abaixo, decifre-a:

Texto:

"E assim, aos poucos, ela se esquece dos socos, pontapés, golpes baixos que a vida lhe deu, lhe dará. A moça - que não era Capitu, mas também tem olhos de ressaca - levanta e segue em frente. Não por ser forte, e sim pelo contrário: por saber que é fraca o bastante para não conseguir ter ódio no seu coração, na

sua alma, na sua essência. E ama, sabendo que vai chorar muitas vezes ainda. Afinal, foi chorando que ela, você e todos os outros, vieram ao mundo."

Dom casmurro (Machado de Assis)

Chave: L3 linha 3 e P11 palavra 11, no texto achamos a palavra-chave:
FORTE = 06-15-18-20-05, de acordo com a ordem alfabética.
Processo: Verifica-se em cada linha da chave a letra original, correspondente a cada letra cifrada.
Linha 06: V$\longrightarrow$P
Linha 15: P$\longrightarrow$A
Linha 18: K$\longrightarrow$S
Linha 20: M$\longrightarrow$S
Linha 05: J$\longrightarrow$E
Linha 06: O$\longrightarrow$I
Linha 15: C$\longrightarrow$N
Linha 18: G$\longrightarrow$O
Linha 20: P$\longrightarrow$V
Linha 05: J$\longrightarrow$E
Linha 06: Y$\longrightarrow$S
Linha 15: I$\longrightarrow$T
Linha 18: A$\longrightarrow$I
Linha 20: V$\longrightarrow$B
Linha 05: Z$\longrightarrow$U
Linha 06: R$\longrightarrow$L
Linha 15: P$\longrightarrow$A
Linha 18: J$\longrightarrow$R
Frase: PASSEI NO VESTIBULAR.

Posteriormente temos alguns exercícios referentes a cifra ADFGVX, qual envolve tanto a substituição, quanto a transposição. Utilizaremos a tabela 5 para as substituições, claro, poderia ser qualquer outra tabela dispondo as letras e os algarismos de forma aleatória.

Nível 1

1) Na Primeira Guerra uma cifra muito famosa foi a conhecida ADFGVX. Se coloque no lugar de um soldado e cifre a mensagem PERIGO para seus amigos soldados, utilizando essa cifra.

a) Faça a substituição através da tabela 5.

Processo: Basta trocar as letras da palavra original pelo par de letras que está na mesma coluna e na mesma linha.

PERIGO = FV XG AV VG FA GX

Palavra: FVXGAVVGFAGX

b) Faça a transposição através da palavra-chave VIDA.

Processo: reescreva a palavra cifrada num quadro junto à palavra chave, depois coloca-se a palavra chave em ordem alfabética e copia as linhas.

V	I	D	A
F	V	X	G
A	V	V	G
F	A	G	X

A	D	I	V
G	X	V	F
G	V	V	A
X	G	A	F

Palavra: GXVFGVVAXGAF

Nível 2

1) Cifre a palavra PASSÁRGADA utilizando o método ADFGVX e a palavra-chave RUA.

Processo: Primeiramente deve-se fazer a substituição utilizando o quadro sugerido acima, trocando as letras da palavra original pelo par de letras que estão na mesma coluna e na mesma linha.

PASSARGADA = FV DD AF AF DD AV FA DD VX DD

Em seguida, reescreva a palavra cifrada num quadro junto à palavra-chave, depois coloca-se a palavra chave em ordem alfabética e copia-se as linhas.

R	U	A
F	V	D
D	A	F
A	F	D
D	A	V
F	A	D
D	V	X
D	D	

A	R	U
D	F	V
F	D	A
D	A	F
V	D	A
D	F	A
X	D	V
	D	D

Palavra: DFVFDADAFVDADFAXDVDD.

Os próximos exercícios são referentes ao sistema binário. Como já foi relatado, os computadores trabalham internamente com esse sistema de numeração, onde a base é 2, e todas as quantidades são representadas utilizando apenas dois dígitos, 0 e 1. As combinações desses dígitos levam o computador a criar várias informações : letras, palavras, cálculos, etc. O interessante em apresentar e trabalhar números binários com os alunos, é o fato deles terem um pouco de contato com a linguagem computacional e mais uma vez ter conhecimento de outra aplicação da matemática. E além de trabalhar a criptografia nesse sistema, ele reforça a divisão, resto, numeração decimal, entre outros conceitos que podem ser revistos.

Na resolução dos exercícios será utilizada a tabela 8 de números binários em ASCII para letras maiúsculas.

Nível 1

1) Cifre a palavra LIVRO através de uma cifra de substituição, use a palavra TIGRE como chave, da seguinte forma: escreva ambas em bits via ASCII, então,

na junção da mensagem com a palavra-chave, se os dígitos forem iguais escreva na mensagem criptografada 0 e se os dígitos forem diferentes escreva 1.

Processo: escreva ambas as palavras em bits utilizando a tabela 8:
LIVRO = 1001100 1001001 1010110 1010010 1001111
TIGRE = 1010111 1000101 1000111 1010010 1000101
Após, observe nas palavras escritas com os algarismos 0 e 1, e em ordem, quando as letras forem iguais coloque 0 na mensagem cifrada e quando diferentes coloque 1.
Mensagem: 00110110001100001000100000000001010.

Nível 2

1) Cifre o nome FERMAT através de uma transposição, trocando os dígitos da palavra, o primeiro com o segundo, o terceiro com o quarto, e assim por diante.

Processo: escreva a palavra em bits utilizando a tabela:
FERMAT = 100011010001011010010100110110000011010111
Após, faça a transposição dos algarismos.
Palavra Cifrada 010011100010100101101000111001000011101011.

O conteúdo funções está sempre presente na matemática, mesmo nos anos iniciais trabalhamos funções, claro, não com essa nomenclatura e nem com conceitos iguais quando trabalhada no ensino médio, mas determinadas regras e associações são funções, assim acaba ficando simples trabalhar a criptografia através de funções a partir do 6º ano até a 3ª série. Para realizar a criptografia através de funções, associamos cada letra, número, símbolo a um número e codificamos cada um desses caracteres através de uma função $f(x)$. Para decifrar a mensagem criptografada é necessário substituir o valor fornecido por $f(x)$ em $f^{-1}(x)$, que é a função inversa de $f(x)$. Novamente, quando não trabalhada no ensino médio, não será necessariamente trabalhado os conceitos de função inversa, mas mesmo assim, pode-se trabalhar com a regra inversa da criptografia.

Para os exercícios, vamos utilizar a seguinte associação numérica ao alfabeto, novamente temos aqui um exemplo, mas essa tabela pode ser montada com outros valores para as letras e ainda pode ser acrescentado algarismos e outros símbolos:

a	b	c	d	e	f	g	h	i	j	k	l	m
1	2	3	4	5	6	7	8	9	10	11	12	13
n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 9: Substituição de letras por números em Funções

Observe que se no processo de criptografar encontrarmos números maiores que 26, reiniciamos a contagem do alfabeto. Por exemplo, se encontrarmos o valor 28, então temos: 26 é a letra z, 27 é a letra a, 28 é a letra b. Ou seja, z+2 =b, a substituição será pela letra b.

Também podemos optar por trabalhar as mensagens cifradas numericamente, e no processo de decifrar encontraremos as letras correspondentes. Apresentaremos atividades das duas formas.

Nível 1

1) Lari encontrou um bilhete embaixo da sua carteira: BJNOJHPDOJYZPJXZ, como sua professora de matemática havia trabalhado em sala criptografia, desconfiou que aquelas letras poderiam estar escondendo alguma mensagem, curiosa levou para casa e tentou decifrá-lo, já descobriu que foi utilizado a seguinte regra para criptografar: valor da letra -5. Com essa informação decifre a mensagem.

Substituição por números: 2, 10, 14, 15, 10, 8, 16, 4, 15, 10, 25, 26, 16, 10,24, 26

Processo: Vamos, novamente, atribuir ao valor da letra da mensagem original a variável x e ao valor da letra cifrada y, assim, podemos reescrever a regra utilizada para criptografar na linguagem matemática: $y = x - 5$. Mas como o objetivo é decifrar deve-se encontrar a regra inversa a esta, ou seja, a operação que desfaz o que foi feito por essa regra, ou seja, desfaz a codificação, que é: $x = y + 5$. (Aqui o professor pode deixar que os alunos substituam os primeiros números na regra de criptografar e isolem o x, para posteriormente mostrar que poderiam ter encontrado a regra inversa para depois substituir os valores).

Deve-se aplicar os números da mensagem criptografa na regra inversa, calcular e associar na tabela a letra correspondente para encontrar a mensagem original. (Observe que não é preciso fazer mais de uma vez os números repetidos, pois o resultado será o mesmo):

2: $x = 2 + 5 = 7$

10: $x = 10 + 5 = 15$

14: $x = 14 + 5 = 19$
15: $x = 15 + 5 = 20$
8: $x = 8 + 5 = 13$
16: $x = 16 + 5 = 21$
4: $x = 4 + 5 = 9$
25: $x = 25 + 5 = 30$ que corresponde ao 4
26: $x = 26 + 5 = 31$ que corresponde ao 5
17: $x = 17 + 5 = 22$
24: $x = 24 + 5 = 29$ que corresponde ao 3
7, 15, 19, 20, 15, 13, 21, 9, 20, 15, 4, 5, 22, 15, 3, 5.
Mensagem: GOSTO MUITO DE VOCÊ.

2) A professora Kelly propôs aos alunos para escolherem um trecho de uma música que gostam e cifrarem para colocar no mural da sala de aula como desafio da semana. Guilherme escolheu o seguinte trecho da música do Legião Urbana: "É PRECISO AMAR AS PESSOAS COMO SE NÃO HOUVESSE AMANHÃ" e resolveu cifrá-lo aplicando os seguintes cálculos: subtrair 3 e multiplicar por 5. Como ficará sua mensagem após cifrada?

Processo: Vamos atribuir ao valor da letra original a variável x e ao da letra cifrada y, assim, obtemos: $y = 5 \cdot (x - 3)$. Deve-se olhar na tabela os valores das letras da mensagem original e calcular na regra:
E: $y = 5 \cdot (5 - 3) = 10$
P: $y = 5 \cdot (16 - 3) = 65$
R: $y = 5 \cdot (18 - 3) = 75$
C: $y = 5 \cdot (3 - 3) = 0$
I: $y = 5 \cdot (9 - 3) = 30$
S: $y = 5 \cdot (19 - 3) = 80$
O: $y = 5 \cdot (15 - 3) = 60$
A: $y = 5 \cdot (1 - 3) = -10$
M: $y = 5 \cdot (13 - 3) = 50$
N: $y = 5 \cdot (14 - 3) = 55$
H: $y = 5 \cdot (8 - 3) = 25$
U: $y = 5 \cdot (21 - 3) = 90$
V: $y = 5 \cdot (22 - 3) = 95$
Criptografando a mensagem original:

É	PRECISO	AMAR	AS	PESSOAS
10	65,75,10,0,30,80,60	-10,50,-10,75	-10,80	65,10,80,80,60,-10,80

COMO	SE	NÃO	HOUVESSE	AMANHÃ
0,60,50,0	80,10	55,-10,60	25,60,90,95,10,80,80,10	-10,50,-10,55,25,-10

Mensagem: $10, 65, 75, 10, 030, 80, 60, -10, 50, -10, 75, -10, 80, 65, 10, 80, 80, 60, -10, 80, 0, 60, 50, 0, 80, 10, 55, -10, 60, 25, 60, 90, 95, 10, 80, 80, 10, -10, 50, -10, 55, 25, -10.$

Nível 2

1) O professor Rodrigo toda sexta passa um desafio aos seus alunos referente a algum conteúdo que ele trabalhou durante a semana. Nessa semana ele explicou funções e também como curiosidade explicou criptografia, então no desafio resolveu dar um exercício envolvendo ambos os assuntos. Ele apresentou a função que utilizou para criptografar uma frase de Einstein e pediu aos seus alunos para de terminarem a função inversa e a mensagem original.

Função cifradora: $y = 3 \cdot x - 16$ e

Mensagem cifrada: $29, 47, 26, 11, -7, 29, 20, 47, 5, -13, 38, 29, 26, -4, -1, 29, 41, 47, -7, -1, 41, 41, 29, 50, -1, 23, -13, 26, 44, -1, 41, -4, 29, 44, 38, -13, -10, 20, 8, 29, -1, 26, 29, -4, 11, -1, 11, 29, 26, -13, 38, 11, 29.$

Processo: Para determinar a função inversa basta isolar x e como este exercício tem como público alvo alunos do ensino médio pode-se trabalhar os conceitos de função inversa e as notações:

$f^{-1}(x) = \frac{x+16}{3}$

Agora para obter a mensagem original basta substituir em f^{-1} os valores da mensagem cifrada, utilizando ainda a tabela 9 de alfabeto:

$f^{-1}(29) = \frac{29+16}{3} = 15$
$f^{-1}(47) = \frac{47+16}{3} = 21$
$f^{-1}(26) = \frac{26+16}{3} = 14$
$f^{-1}(11) = \frac{11+16}{3} = 9$
$f^{-1}(-7) = \frac{-7+16}{3} = 3$
$f^{-1}(20) = \frac{20+16}{3} = 12$
$f^{-1}(5) = \frac{5+16}{3} = 7$
$f^{-1}(-13) = \frac{-13+16}{3} = 1$
$f^{-1}(38) = \frac{38+16}{3} = 18$
$f^{-1}(-4) = \frac{-4+16}{3} = 4$
$f^{-1}(-1) = \frac{-1+16}{3} = 5$
$f^{-1}(41) = \frac{41+16}{3} = 19$
$f^{-1}(50) = \frac{50+16}{3} = 22$
$f^{-1}(23) = \frac{23+16}{3} = 13$
$f^{-1}(44) = \frac{44+16}{3} = 20$

$f^{-1}(-10) = \frac{-10+16}{3} = 2$
$f^{-1}(8) = \frac{8+16}{3} = 8$

Trocando os valores da mensagem criptografada pelos valores encontrados temos:

15,21,14,9,3,15,12,21,7,1,18,15,14,4,5,15,19,21,3,5,19,19,15,22,5,13,1,14,20,5,
19,4,15,20,18,1,2,1,12,8,15,5,14,15,4,9,3,9,15,14,1,18,9,15.

Para finalizar basta trocar esses valores pelas suas respectivas letras da tabela 9.

Mensagem: "O ÚNICO LUGAR ONDE O SUCESSO VEM ANTES DO TRABALHO É NO DICIONÁRIO."

2) Cifre a palavra CIDADE através da função exponencial $y = 2^x - 3$.

Processo: Deve-se olhar na tabela 9 os valores das letras da palavra original e substituir no lugar do x e calcular cada y correspondente:

C: $x = 3$, $y = 2^3 - 3 = 5$
I: $x = 9$, $y = 2^9 - 3 = 509$
D: $x = 4$, $y = 2^4 - 3 = 13$
A: $x = 1$, $y = 2^1 - 3 = -1$
E: $x = 5$, $y = 2^5 - 3 = 29$

Criptografando a palavra original:

C	I	D	A	D	E
5	509	13	-1	13	29

Cifra: $5, 509, 13, -1, 13, 29$.

3) Cifre a palavra ELEFANTE através da função polinomial cifradora:
$f(x) = x^3 - x^2 - 2x + 5$.

Processo: Deve-se olhar na tabela os valores das letras da palavra original e substituí-los em f(x) :

E:$f(5) = 95$
L:$f(12) = 1565$
F:$f(6) = 173$
A:$f(1) = 3$
N:$f(14) = 2525$
T:$f(20) = 7565$

Criptografando a palavra original:

E L E F A N T E
95 1565 95 173 3 2525 7565 95

Cifra: 95,1565,95,173,3,2525,7565,95.

Finalmente os problemas a seguir são de criptografia por matrizes, e usa o método de substituição e cifras. Serão aplicados somente ao ensino médio, visto que é conteúdo da 2ª série. Os exercícios usam como ferramenta a multiplicação de matrizes e podem ser aplicados para revisar, reforçar, praticar ou introduzir o assunto de matriz inversa.

A tabela abaixo faz a substituição das letras pelos números correspondentes para que se possam fazer os cálculos.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 10: Substituição de letras por números em Matrizes/Aritmética Modular

Assim como em funções, se no processo de criptografar encontrarmos números maiores que 25, reiniciamos a contagem do alfabeto. Por exemplo, se encontrarmos o valor 28, então temos: 25 é a letra z, 26 é a letra a, 27 é a letra b, 28 é a letra c. Ou seja, z+3 =c, a substituição será pela letra c.

E também podemos optar por trabalhar as mensagens cifradas numericamente, e no processo de decifrar encontraremos as letras correspondentes. Optaremos por trabalhar as mensagens numericamente.

Nível 2

1) Criptografe a frase no $\mathbb{R}^2$, através do processo $B \cdot M = C$ onde a matriz chave é $B = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$, M a matriz original com as letras dispostas ordenadamente nas colunas e C será a mensagem cifrada.

Frase: INFORMAÇÕES, SEGREDOS, MATRIZES E CRIPTOGRAFIA.

Quantidade de letras: Como temos na frase 40 letras, que é múltiplo de 2, não precisamos acrescentar nenhum letra.

Substituição: 8, 13, 5, 14, 17, 12, 0, 2, 14, 4, 18, 18, 4, 6, 17, 4, 3, 14, 18, 12, 0, 19, 17, 8, 25, 4, 18, 4, 2, 17, 8, 15, 19, 14, 6, 17, 0, 5, 8, 0.

Processo: Matriz chave multiplica cada vetor $\mathbb{R}^2$, porém para simplificar podemos usar uma matriz de ordem 2×4, ou seja, com 8 elementos cada, pois 40 também é divisível por 8.

$$\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 8 & 5 & 17 & 0 \\ 13 & 14 & 12 & 2 \end{pmatrix} = \begin{pmatrix} 68 & 66 & 82 & 8 \\ 73 & 75 & 77 & 10 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 14 & 18 & 4 & 17 \\ 4 & 18 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 44 & 108 & 32 & 50 \\ 34 & 108 & 34 & 37 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 3 & 18 & 0 & 17 \\ 14 & 12 & 19 & 8 \end{pmatrix} = \begin{pmatrix} 62 & 84 & 76 & 66 \\ 73 & 78 & 95 & 57 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 25 & 18 & 2 & 8 \\ 4 & 4 & 17 & 15 \end{pmatrix} = \begin{pmatrix} 66 & 52 & 72 & 76 \\ 45 & 38 & 87 & 83 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 19 & 6 & 0 & 8 \\ 14 & 17 & 5 & 0 \end{pmatrix} = \begin{pmatrix} 94 & 80 & 20 & 16 \\ 89 & 91 & 25 & 8 \end{pmatrix}$$

Cifragem: 68, 73, 66, 75, 82, 77, 8, 10, 44, 34, 108, 108, 32, 34, 50, 37, 62, 73, 84, 78, 76, 95, 66, 57, 66, 45, 52, 38, 72, 87, 76, 83, 94, 89, 80, 91, 20, 25, 16, 8.

2) Sabendo que a matriz chave $A = \begin{pmatrix} 3 & 4 \\ 1 & 0 \end{pmatrix}$ foi usada para cifrar a partir do método $A \cdot M = C$ (M matriz original, com letras ordenadas em colunas e C matriz cifrada), determine a inversa de A e decifre a seguinte mensagem descobrindo qual é a importância da criptografia: 148, 20, 128, 8, 8, 0, 36, 8, 12, 0, 28, 4, 85, 23, 118, 6, 66, 22, 47, 13, 100, 0.

Inversa da chave: $A \cdot A^{-1} = I_2$

$$\begin{pmatrix} 3 & 4 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 3a+4c & 3b+4d \\ a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$a = 0 \qquad e \qquad b = 1$$
$$4c = 1 \longrightarrow c = \tfrac{1}{4}$$
$$3 + 4d = 0 \longrightarrow d = -\tfrac{3}{4}$$
$$A^{-1} = \begin{pmatrix} 0 & 1 \\ \frac{1}{4} & -\frac{3}{4} \end{pmatrix}$$

Processo: A matriz inversa multiplica cada vetor cifrado, obtendo os valores das letras originais:

$$\begin{pmatrix} 0 & 1 \\ \frac{1}{4} & -\frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} 148 & 128 & 8 \\ 20 & 8 & 0 \end{pmatrix} = \begin{pmatrix} 20 & 8 & 0 \\ 22 & 26 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ \frac{1}{4} & -\frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} 36 & 12 & 28 \\ 8 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 8 & 0 & 4 \\ 3 & 3 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ \frac{1}{4} & -\frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} 85 & 118 & 66 \\ 23 & 6 & 22 \end{pmatrix} = \begin{pmatrix} 23 & 6 & 22 \\ 4 & 25 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ \frac{1}{4} & -\frac{3}{4} \end{pmatrix} \cdot \begin{pmatrix} 47 & 100 \\ 13 & 0 \end{pmatrix} = \begin{pmatrix} 13 & 0 \\ 2 & 25 \end{pmatrix}$$

Mensagem: 20, 22, 8, 26, 0, 2, 8, 3, 0, 3, 4, 4, 23, 4, 6, 25, 22, 0, 13, 2, 0, 25.
Substituindo: PRIVACIDADEESEGURANÇAZ $\longrightarrow$ excluímos a letra Z.
Importância da criptografia: PRIVACIDADE E SEGURANÇA.

3) Em uma prova de matemática o professor solicitou em uma das questões que o aluno desenhasse e explicasse um sólido, cujo nome foi cifrado pela multiplicação de matrizes pelo processo $M \cdot A = E$, onde M é a matriz que contém o nome do sólido ordenado na linhas, A é a matriz chave e E a matriz cifrada. Descubra qual é o sólido, dadas $A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$ e $E = \begin{pmatrix} 40 & -18 \\ 13 & -4 \\ 17 & 0 \end{pmatrix}$.

Processo: Primeiramente determine a matriz inversa de A e após multiplique a matriz E por A^{-1}, obtendo assim M:

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ 2a-c & 2b-d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$a = 1 \quad e \quad 2a - c = 0 \longrightarrow c = 2$$
$$b = 0 \quad e \quad 2b - d = 0 \longrightarrow d = -1$$
$$A^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$$

Observe que nesse caso a inversa é a própria matriz.
Multiplicando a matriz E pela matriz A^{-1} obtemos a matriz M:

$$\begin{pmatrix} 40 & -18 \\ 13 & -4 \\ 17 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 5 & 4 \\ 17 & 0 \end{pmatrix}$$

Agora basta copiar as linhas da matriz 4, 18, 5, 4, 17, 0 e substituir na tabela do alfabeto cifrado.
Palavra: ESFERA.

2 Aritmética Modular

Iniciaremos esse capítulo com o seguinte trecho[4]:

> "Os processos pelos quais informações enviadas eletronicamente são codificadas depende, de maneira crucial, do uso da matemática. O mais curioso é que até os anos 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que destituída de utilidade prática."

Uma das ferramentas mais importantes na Teoria dos Números, área que estuda as propriedades dos números inteiros, é a Aritmética Modular (ou Aritmética do Relógio como é conhecida), que consiste em um conjunto de números que representam os restos de uma divisão inteira por outro número inteiro pré-determinado, chamado de módulo. Foi Gauss quem observou uma relação existente entre números distintos que possuíam o mesmo resto quando divididos por outro número dado, introduzindo então uma notação específica para este fato e denominando-a de congruência.

> "The German mathematician Carl Friedrich Gauss, considered to be one of the greatest mathematicians of all time, developed the language of congruences in the early nineteenth century. When doing certain computations, integers may be replaced by their remainders when divided by a specific integer, using the language of congruences." (ROSEN [22])

Há inúmeras aplicações envolvendo congruência, criptografia, códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, calendários e diversos fenômenos periódicos. E estes podem ser facilmente trabalhados em sala de aula.

Para, posterior compreensão do método de criptografia RSA, abordado no capítulo 3, apresentaremos alguns resultados básicos e propriedades da aritmética modular.

Há várias formas de apresentar a definição de congruência, uma delas [25]:

> "Dizem que Dois números inteiros a, b são congruentes módulo m se e somente se $m|(a-b)$, ou $m|(b-a)$. ... Quando $m|(a-b)$, dizemos que a é congruente com b módulo m. ... Quando a, b forem congruentes módulo m, escreveremos $a \equiv b \mod m$."

No livro de Coutinho [4] encontra-se a definição apresentada da seguinte forma:

> "se n é o módulo e a e b são números inteiros, então diremos que a é congruente a b módulo n se $a-b$ é múltiplo de n".

Outra forma de descrever a definição [23]:

"Se os inteiros a e b dão o mesmo resto quando divididos pelo inteiro k $(k > 0)$ então podemos dizer que a e b são côngruos, módulo k e podemos representar: $a \equiv b \mod k$ ".

Assim, entendemos que a e b, números inteiros, são congruentes módulo m, ou seja, $a \equiv b \mod m$ quando m divide $a - b$, notação: $m|(a - b)$, isto é, $(a - b) = k \cdot m$, onde k é um número inteiro.

Exemplos:

1)$74 \equiv 50 \mod 6$, pois, segundo as definições, temos:
6 divide $(74 - 50) = 24$, isto é, $6|(74 - 50)$, ou
$(74 - 50) = 24$ é múltiplo de 6, pois, $24 = 6 \cdot 4$, ou ainda,
$74 = 12 \cdot 6 + 2$ e $50 = 8 \cdot 6 + 2$, ambos os números deixam resto 2 quando divididos por 6.

2)Apresentaremos um exemplo aplicado ao relógio, na distribuição em doze horas, teremos que $14 \equiv 2 \mod 12$, pois $12|(14 - 12)$. Estendendo o raciocínio teríamos $2 \equiv 14 \equiv 26 \equiv 38 \equiv ... \equiv \mod 12$.

A congruência modular satisfaz algumas propriedades importantes, para seu entendimento e relevantes para sua aplicação no RSA, que serão apresentadas sem demonstração, pois o interesse está na utilização destas e nos seus resultados. Considere m número inteiro positivo e os números a, b, c e d, inteiros.
A congruência é uma relação de equivalência, isto é, satisfaz as propriedades: reflexiva, simétrica e transitiva:

1)$a \equiv a \mod m$

2)se $a \equiv b \mod m$ então $b \equiv a \mod m$

3)se $a \equiv b \mod m$ e $b \equiv c \mod m$ então $a \equiv c \mod m$

Podemos fazer uma relação da congruência com o Algoritmo da Divisão de Euclides: sejam n, d naturais e $d > 0$, então, existem únicos q, r naturais, tais que: $n = q \cdot d + r$, onde $0 \leq r < d$. Assim, $n - r = q \cdot d$ que é equivalente à: $n \equiv r \mod d$, logo, todo número natural é congruente módulo d ao resto da sua divisão por d. E dizemos que r é o resíduo de n módulo d. O conjunto de todos os resíduos de um dado número d, possui d elementos, $0, 1, 2, ..., d - 1$.

Exemplo: O conjunto dos resíduos do número 5 é {0, 1, 2, 3, 4}, que são os possíveis restos de uma divisão por 5.

Um teorema que se faz necessário apresentar é:

Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então:

1)$a + c \equiv b + d \mod m$

2)$a \cdot c \equiv b \cdot d \mod m$, em particular, $a^k \equiv b^k \mod m$, para $k \geq 0$

Existem vários teoremas importantes que facilitam a resolução de congruências, um resultado muito importante e útil é o teorema de Fermat, aplicado principalmente no cálculo de restos de potências.

Teorema de Fermat: Se p é um primo e a é um inteiro que não é divisível por p, então: $a^{p-1} \equiv 1 \mod m$.

A Aritmética Modular foi usada na Criptografia por ser uma função fácil de ser calculada, mas difícil de ser revertida. Veremos que o método RSA parte da escolha de dois números primos, onde seus produtos geram um terceiro número. Mas o que teria de difícil em reverter uma função envolvendo números primos? O fato é que, sabemos através do Teorema Fundamental da Aritmética que [24]: "todo inteiro maior que 1 pode ser representado de maneira única (a menos de ordem) como um produto de fatores primos", a dificuldade está no fato que, não temos algoritmos práticos, rápidos para fatoração de números. Assim, iremos observar que fatorar um número suficientemente grande em dois números primos torna a cifra RSA inquebrável.

2.1 Atividades Sala de Aula

Pensando no ensino fundamental observamos que os alunos têm dificuldades na operação de divisão pelo algoritmo de Euclides, por isso, as atividades apresentadas trabalham com os termos: divisores, dividendos, quocientes e inclusive os restos, reforçando este algoritmo e fixando melhor assim o aprendizado.

No ensino médio as atividades com aritmética modular e sua aplicação em criptografia ajudarão os alunos a desenvolver estratégias na resolução de problemas que envolvem a base da teoria dos números além de estender os conhecimentos para contextos diferenciados.

E mais uma vez, conhecendo a aritmética modular, o aluno verá que a matemática está presente em outras situações de seu cotidiano, em calendários, relógios e problemas em geral envolvendo repetições periódicas.

Assim como no capítulo 1, trabalharemos com dois níveis, sendo o nível 1 para o Ensino Fundamental e o nível 2 para o Ensino Médio. Em ambos, os primeiros exercícios são para compreensão da aritmética modular, e os demais são suas aplicações em criptografia. Nas aplicações usaremos a tabela 10 para substituição dos números pelas letras, e novamente, no processo de criptografar quando os números forem maior que 26 reiniciaremos a contagem do alfabeto.

Nível 1

1) O relógio está marcando 8:00, e ainda é de manhã, minha mãe me avisou que daqui a 9 horas tenho consulta médica.

a) Para que horas está agendada a consulta?

Solução: $8 + 9 = 17$ horas.

b) Se estivéssemos trabalhando com um relógio que conta de 12 em 12 horas ao invés das 24 horas o habitual no Brasil, que horário é a consulta?

Solução: 5 horas da tarde.

c) O algoritmo da divisão é **dividendo = quociente x divisor + resto**, se o divisor é 12, o dividendo 17, e o quociente 1, qual é o resto? Qual a relação com os resultados anteriores?

Algoritmo: $17 = 1 \cdot 12 +$ resto $\longrightarrow$ resto $= 5$.
Relação: 17 é o horário da consulta no período de 24 horas, dividindo por 12, restam 5, que é o horário correspondente à 17, só que num período de 12 horas.

2) Joana faz aniversário dia 1 de janeiro e sua mãe dia 17 de abril. Sabendo que seu aniversário caiu em uma quarta em 2014, em que dia da semana caiu o aniversário de sua mãe nesse mesmo ano? (não vale olhar no calendário, é claro!).

Processo: monte uma tabela com os dias da semana do 1 ao 7:
1 - quarta, 2 - quinta, 3 - sexta, 4 - sábado, 5 - domingo, 6 - segunda, 7 - terça.
Determine quantos dias há entre 01/01 e 17/04:
Janeiro: 31 dias
Fevereiro: 28 dias
Março: 31 dias
Abril: 17 dias
Total = 107 dias.
Dividindo 107 por 7 tem-se: $107 = 7 \cdot 15 + 2$ (ou seja, $107 \equiv 2 \mod 7$).
Logo, o 107º dia foi o mesmo dia da semana do 2º dia.
Dia da semana: quinta-feira.

3) A informação que devemos conhecer para trabalhar problemas periódicos através da aritmética modular é o ..... do fenômeno. Esse valor será o ..... da divisão. E a aritmética modular faz uma relação entre os números que apresentam o mesmo ..... quando divididos por um mesmo número não nulo.

Solução: PERÍODO, DIVISOR, RESTO.

4) Cifre NÚMERO, sendo o quociente 2, o divisor é 26 e o resto é o valor de cada letra da palavra, e o dividendo é a cifra.

Substituição: 13 - 20 - 12 - 4 - 17 - 14
Processo:
dividendo $= 2 \cdot 26 + 13 \longrightarrow$ dividendo $= 65$
dividendo $= 2 \cdot 26 + 20 \longrightarrow$ dividendo $= 72$
dividendo $= 2 \cdot 26 + 12 \longrightarrow$ dividendo $= 64$
dividendo $= 2 \cdot 26 + 4 \longrightarrow$ dividendo $= 56$
dividendo $= 2 \cdot 26 + 17 \longrightarrow$ dividendo $= 69$
dividendo $= 2 \cdot 26 + 14 \longrightarrow$ dividendo $= 66$
Mensagem Cifrada: 65 - 72 - 64 - 56 - 69 - 66.

Nível 2

1) Resolva as congruências:

a) $93 \equiv x \mod 5$

Resolução: $93 \equiv 3 \mod 5$

b) $(26 + 32) \equiv x \mod 7$

Resolução: $26 \equiv 5 \mod 7$ e $32 \equiv 4 \mod 7 \longrightarrow (26 + 32) \equiv 9 \mod 7$ e

$9 \equiv 2 \mod 7 \longrightarrow (26 + 32) \equiv 2 \mod 7$

c) $(8 \cdot 43) \equiv x \mod 8$

Resolução: $8 \equiv 0 \mod 8$ e $43 \equiv 3 \mod 8 \longrightarrow (8 \cdot 43) \equiv 0 \mod 8$

d) $7^{26} \equiv x \mod 12$

Resolução: $7^{26} = 7^2 \cdot 7^{24} \longrightarrow 7^2 = 49 \equiv 1 \mod 12$ e $7^{24} = (7^2)^{12} \equiv 1^{12} \mod 12$

$\longrightarrow 7^{26} \equiv 1.1^{12} \mod 12 \equiv 1 \mod 12$

e) $56^{13} \equiv x \mod 13$

Resolução: $56^{13} = 56^{12} \cdot 56$ como $56 \equiv 4 \mod 13$ e por Fermat $56^{12} \equiv 1 \mod 13$

$\longrightarrow 56^{13} \equiv 4 \mod 13$

f) $x \equiv 2 \mod 30$

Resolução: $x = 32$ pois $32 = 30 \cdot 1 + 2$, para $q = 1$

Mas $q = 0, 1, 2, 3, \ldots$ temos $x = 2, 32, 62, 92, \ldots$

2) No CPF, o décimo dígito(que é o primeiro dígito verificador) é o resultado de uma congruência módulo 11, de um número obtido por uma operação dos primeiros nove dígitos. Devemos multiplicá-los, nessa ordem, pelos valores 1, 2, 3, 4, 5, 6, 7, 8, 9 e somar os produtos obtidos. O décimo dígito, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \mod 11$. Note que tal número será o próprio resto da divisão por 11 da soma obtida. Suponha que o CPF de uma pessoa é formado pelos os seguintes nove primeiros dígitos: 245.103.201, determine através do processo acima o décimo dígito:

Processo: Efetuando as multiplicações dos dígitos pelas bases citadas acima e soma S dos produtos:

$S = 2 \cdot 1 + 4 \cdot 2 + 5 \cdot 3 + 1 \cdot 4 + 0 \cdot 5 + 3 \cdot 6 + 2 \cdot 70 \cdot 8 + 1 \cdot 9 = 70$

Para determinar a_{10}:

$70 - a_{10} \equiv 0 \mod 11$

Dividindo 70 por 11 tem-se: $70 = 11 \cdot 6 + 4$, logo, $a_{10} = 4$, pois $70 - 4 = 66 = 6 \cdot 11$.

Solução: primeiro dígito de controle será o algarismo 4.

(Curiosidade: A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9).

Observe que , caso o resto da divisão for 10, isto é, $S - 10 \equiv 0 \mod 11$, usa-se o dígito 0.

Para cifrar usamos de maneira geral $C \equiv a \cdot P + k \ mod\ 26$

Para decifrar usamos $P \equiv \overline{a} \cdot (C - k) \ mod\ 26$,

P – número da letra original

C – número da letra cifrada

a – número inteiro tal que $(a,26)=1$

k – número inteiro positivo

$\overline{a}$ - inverso de a, ou seja, $\overline{a} \cdot a \equiv 1 \ mod\ 26$

Quadro 1 - Método para criptografar por aritmética modular

3) Criptografe TECNOLOGIA, para $a = 1$ e $k = 3$.

Substituição por números: 19, 4, 2, 13, 14, 11, 14, 6, 8, 0.
Transportando as letras: $C \equiv a \cdot P + k \mod 26$
$C \equiv 1 \cdot 19 + 3 \mod 26 \longrightarrow C \equiv 22 \mod 26 \longrightarrow 22 \equiv 22 \mod 26$
$C \equiv 1 \cdot 4 + 3 \mod 26 \longrightarrow C \equiv 7 \mod 26 \longrightarrow 7 \equiv 7 \mod 26$
$C \equiv 1 \cdot 13 + 3 \mod 26 \longrightarrow C \equiv 16 \mod 26 \longrightarrow 16 \equiv 16 \mod 26$
$C \equiv 1 \cdot 14 + 3 \mod 26 \longrightarrow C \equiv 17 \mod 26 \longrightarrow 17 \equiv 17 \mod 26$
$C \equiv 1 \cdot 11 + 3 \mod 26 \longrightarrow C \equiv 14 \mod 26 \longrightarrow 14 \equiv 14 \mod 26$
$C \equiv 1 \cdot 6 + 3 \mod 26 \longrightarrow C \equiv 9 \mod 26 \longrightarrow 9 \equiv 9 \mod 26$
$C \equiv 1 \cdot 8 + 3 \mod 26 \longrightarrow C \equiv 11 \mod 26 \longrightarrow 11 \equiv 11 \mod 26$
$C \equiv 1 \cdot 0 + 3 \mod 26 \longrightarrow C \equiv 3 \mod 26 \longrightarrow 3 \equiv 3 \mod 26$
Números Cifrados: 22, 7, 5, 16, 17, 9, 11, 3.
Palavra criptografada: X H F Q R O R J L D
Observação: Note que esse método é análogo a Cifra de César.

4) Verifique se é possível usar $a = 7$ e use $k = 10$. Depois cifre a palavra SECRETO com esses valores.
Verificando o valor a: $a = 7$ pois $(7, 26) = 1$
Substituindo as letras por números: 18, 4, 2, 17, 4, 19, 14.
Transportando as letras: $C \equiv a \mod P + k \mod 26$
$C \equiv 7 \cdot 18 + 10 \mod 26 \longrightarrow C \equiv 136 \mod 26 \longrightarrow 136 \equiv 6 \mod 26$
$C \equiv 7 \cdot 4 + 10 \mod 26 \longrightarrow C \equiv 38 \mod 26 \longrightarrow 38 \equiv 12 \mod 26$
$C \equiv 7 \cdot 2 + 10 \mod 26 \longrightarrow C \equiv 24 \mod 26 \longrightarrow 24 \equiv 24 \mod 26$

$C \equiv 7 \cdot 17 + 10 \mod 26 \longrightarrow C \equiv 129 \mod 26 \longrightarrow 129 \equiv 25 \mod 26$
$C \equiv 7 \cdot 19 + 10 \mod 26 \longrightarrow C \equiv 143 \mod 26 \longrightarrow 143 \equiv 13 \mod 26$
$C \equiv 7 \cdot 14 + 10 \mod 26 \longrightarrow C \equiv 108 \mod 26 \longrightarrow 108 \equiv 4 \mod 26$
Números cifrados: 6, 12, 24, 25, 12, 13, 4
Palavra criptografada: G M Y Z M N E
Observação:
Calculando $\overline{a}$ inverso de a:
$\overline{a} \cdot a \equiv 1 \mod 26 \longrightarrow \overline{a} \cdot 7 \equiv 1 \mod 26 \longrightarrow \overline{a} = 15$, pois $15 \cdot 7 = 105 \equiv 1 \mod 26$
A chave para criptografar é $a = 7$ e $k = 10$.
A chave para decriptar é: $\overline{a}= 15$ e $k = 10$.
Fazendo: $P \equiv \overline{a} \cdot (C - k) \mod 26$ para, por exemplo, $C = 25$
$P \equiv 15 \cdot (25 - 10) \mod 26 \longrightarrow P \equiv 225 \mod 26 \longrightarrow 225 \equiv 17 \mod 26$.
Voltamos ao $P = 17$.

3 Método e Implementação RSA

Whitefield Diffie publicou, em 1975, um resumo de suas ideias e assim muitos cientistas passaram a estudar e pesquisar tal função apropriada para o sistema de chave assimétrica.

Segundo Singh [26], "A ideia de Diffie funcionaria na teoria, mas não na prática.", o que levou outros pesquisadores a tentar fazer da cifra assimétrica realidade.

Reunindo-se para isso, os cientistas da computação Ronald L. Rivest e Adi Shamir, e o matemático Leonard Adleman, em 1977 terminaram o trabalho baseado nas funções modulares de mão única (funções praticamente impossíveis de serem revertidas). Esse sistema de criptografia ficou conhecido como RSA, iniciais dos sobrenomes dos três pesquisadores e é chamado de criptografia de chave pública, veremos seus detalhes no próximo capítulo. Após anos, constatou-se que o método RSA já havia sido descoberto em Bletcheley Park, mas como todos os arquivos foram incendiados após o fim da guerra então a fama ficou para Rivest, Shamir e Adleman.

Rosen [22] explica o sistema RSA e sua segurança:

> "relies on the disparity in computer time required to find large primes and to factor large integers. In particular, to produce an enciphering key requires that two large primes be found and then multiplied; this can be done in minutes on a computer. When these large primes are known, the deciphering key can be quickly found. To find the deciphering key from the enciphering key requires that a large integer, namely the product of the large primes, be factored. This may take billions of years."

Phil Zimmermann que estudou física e computação, desenvolveu o projeto PGP (*Pretty Good Privacy*), no qual, em 1980, montou um software misturador, com o objetivo de acelerar a velocidade da cifra RSA, de acordo com ele in Singh [26]: "Agora é possível, com a criptografia moderna, criar cifras que estão fora do alcance de todas as formas conhecidas de criptoanálise. E eu acho que vai continuar assim."

Até o momento Phil está certo, entre os sistemas de criptografia o mais popular é o RSA, além de, atualmente, ser também o mais utilizado, é a conhecida criptografia de chave pública. Método esse usado por vários programas de navegação da Internet.

Iremos descrever os conceitos básicos do método RSA, contando que o leitor tenha conhecimento dos conceitos elementares da teoria dos números que é a matemática necessária para entender o método, no entanto diremos o suficiente para explicar porque o RSA é difícil de ser decifrado. Assim diz Coutinho [4]:

> "A maior parte do que precisamos será encontrado nos métodos da teoria dos números desenvolvidos pelos gregos antigos e pelos matemáticos Fermat, Gauss e Euler, entre os séculos XVII e XIX. Se os fundamentos da teoria já têm quase 20 anos, muitas das aplicações que nos interessam têm menos de 20 anos."

Quando pensamos em cifrar uma mensagem, refletimos pelo capítulo 1, que o podemos fazer usando somente letras ou substituindo essas letras por números. No sistema RSA usamos a substituição por números, e esta é a primeira coisa a se fazer.

Usam-se números de dois dígitos, para que não ocorra ambiguidade, pois se fizéssemos a letra A como 1 e a letra I como 9, a palavra AI fica 19 que pode ser confundida com a letra S, então elabora-se uma tabela para a substituição que deve ser conhecida por todos envolvidos:

a	b	c	d	e	f	g	h	i	j	k	l	m
10	11	12	13	14	15	16	17	18	19	20	21	22
n	o	p	q	r	s	t	u	v	w	x	y	z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 11: Substituição de letras por números em RSA

Para completar o sistema RSA de criptografia também devemos saber como escrever as cifras e depois decifrá-las, para isso se faz necessário, a chave pública e a chave privada.

Escolhem-se dois números primos distintos p e q, considere $n = p \cdot q$, sendo n inteiro.

Depois calcula-se a função de Euler $\phi(n) = (p-1).(q-1)$, que é a quantidade de números coprimos com n e escolhe-se um número inteiro e, chamado de potência de encifração, tal que $mdc(e, \phi(n)) = 1$.

O par (e, n) é a chave pública.

Outro par, (d, n), é a chave privada, d é um número inteiro chamado potência de decifração, onde, $e \cdot d \equiv 1 \mod \phi(n)$, com $1 \leq d < \phi(n)$.

Para achar o valor de d , conhecidos $\phi(n)$ e e, aplica-se o algoritmo de Euclides estendido.

Implementando o RSA, usamos a aritmética modular, onde C representa o texto cifrado e D o texto original.

O texto original depois de convertido em números onde os espaços entre as palavras são completados pelo número 99, é separado em blocos, esses blocos são $D_1, D_2, D_3, ..., D_r$ e cada bloco deve ser menor que o número $n = p \cdot q$, e não deverá começar com 0 para evitar problemas na decodificação. Para cifrar cada um dos blocos fazemos:

$$C \equiv D^e \mod n \tag{4}$$

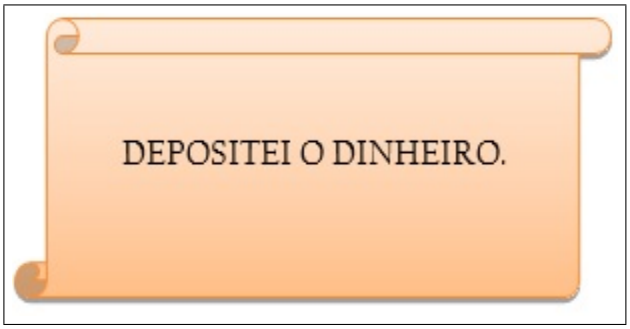
Depois de cifrados geram os blocos $C_1, C_2, C_3, ..., C_r$. Observe que para esse processo usa-se somente a chave pública.

Transmitida a mensagem, agora é hora de decifrar, para tal usa-se a chave privada, conhecida somente pela pessoa que recebe a mensagem, fazendo com cada um dos blocos cifrados:

$$D \equiv C^d \mod n \tag{5}$$

Vejamos um exemplo:

Lucy precisa enviar para Alexandre a seguinte mensagem:



A mensagem não deve ser vista por mais ninguém, pois se trata de uma compra que ela está realizando. Lucy fará os seguintes passos:

1) Procura a chave pública de Alexandre (5, 247);

2) Substitui as letras da mensagem conforme tabela 11:

13142524281829141899249913182317141827 24

3) Separa em blocos de números menores que n= 247

131 - 42 - 52 - 42 - 81 - 82 - 9 - 141 - 89 - 92 - 4 - 99 - 13 - 182 - 3 - 171 - 41 - 82 - 72 - 4

4) Executa $C \equiv D^e \mod n$:

$C \equiv 131^5 \mod 247 \longrightarrow 131^5 = 131 \cdot 131^2 \cdot 131^2 \equiv 131 \cdot 118 \cdot 118 \equiv 196 \mod 247$

$C \equiv 42^5 \mod 247 \longrightarrow 42^5 = 42^3 \cdot 42^2 \equiv 235 \cdot 35 \equiv 74 \mod 247$

$C \equiv 52^5 \mod 247 \longrightarrow 52^5 = 52^3 \cdot 52^2 \equiv 65 \cdot 234 \equiv 143 \mod 247$

$C \equiv 81^5 \mod 247 \longrightarrow 81^5 = 81^3 \cdot 81^2 \equiv 144 \cdot 139 \equiv 9 \mod 247$

$C \equiv 82^5 \mod 247 \longrightarrow 82^5 = 82^3 \cdot 82^2 \equiv 64 \cdot 55 \equiv 62 \mod 247$

$C \equiv 9^5 \mod 247 \longrightarrow 9^5 = 59049 \equiv 16 \mod 247$

$C \equiv 141^5 \mod 247 \longrightarrow 141^5 \equiv -80^5 = -80^3 \cdot 80^2 \equiv -216 \cdot 255 \equiv -188 \equiv 59 \mod 247$

$C \equiv 89^5 \mod 247 \longrightarrow 89^5 = 89^3 \cdot 89^2 \equiv 31 \cdot 17 \equiv 33 \mod 247$

$C \equiv 92^5 \mod 247 \longrightarrow 92^5 = 92^3 \cdot 92^2 \equiv 144 \cdot 66 \equiv 118 \mod 247$

$C \equiv 4^5 \mod 247 \longrightarrow 4^5 = 1024 \equiv 36 \mod 247$

$C \equiv 99^5 \mod 247 \longrightarrow 99^5 = 99^3 \cdot 99^2 \equiv 83 \cdot 168 \equiv 112 \mod 247$

$C \equiv 13^5 \mod 247 \longrightarrow 13^5 = 371293 \equiv 52 \mod 247$

$C \equiv 182^5 \mod 247 \longrightarrow 182^5 = -39^5 \equiv -80^3 \cdot 80^2 \equiv -39 \cdot 39 \equiv -39 \equiv 208 \mod 247$

$C \equiv 3^5 \mod 247 \longrightarrow 3^5 = 243 \equiv 243 \mod 247$

$C \equiv 171^5 \mod 247 \longrightarrow 171^5 = -50^5 = -50^3 \cdot 50^2 \equiv -18 \cdot 30 \equiv -46 \equiv 201 \mod 247$

$C \equiv 41^5 \mod 247 \longrightarrow 41^5 = 41^3 \cdot 41^2 \equiv 8199 \equiv 110 \mod 247$

$C \equiv 72^5 \mod 247 \longrightarrow 72^5 = 72^3 \cdot 72^2 \equiv 31244 \equiv 154 \mod 247$

Envia a mensagem cifrada conforme resultados do passo 4:

196 - 74 - 143 - 74 - 9 - 62 - 16 - 59 - 33 - 118 - 36 - 112 - 52 - 208 - 243 - 201 - 110 - 62 - 154 -36

Recebendo a mensagem, Alexandre em posse dos números primos escolhidos por ele, $p = 13$ e $q = 19$, sabendo que $\phi(n) = 216$ e $e = 5$ primeiro primo onde mdc(5, 216) = 1, calcula o valor de d :

$e \cdot d \equiv 1 \mod 216$
$5 \cdot d \equiv 1 \mod 216$
$216 = 5 \cdot 43 + 1 \longrightarrow 1 = 216 + (-43) \cdot 5$

Como o inverso de 5 módulo 216 é -43, e precisamos de d positivo, $d = 216 - 43 = 173$.

Agora é só decifrar a mensagem por $D \equiv C^d \mod n$, e para o 1º bloco que é 196 fica assim:

$D \equiv 196^{173} \mod 247$

$196^{173}=$

3633292352000246607155222636242868093386051894578991537403560451171508780383631464826708799200197373959903240073543636740836847605153193717968423266554093103344579746077290452487262412042708830135895727668018371694498222612027202173615178745559721598174855203655467717238791875499993824340067095016823088440144685914476075577986005986676170296755259315202541409212591884796153534733149591553703936

Só a potência gera um número de 397 casas decimais. Escrevendo a congruência na forma de divisão euclidiana temos:

$196^{173} = 247 \cdot x + 131$

x =

1470968563562852773907783952400275681724906455785390839690528142394772390217131436545379753846952931011754008394913509072213957915599974566673778407101591511516517190596317621405920696529185547108889585700479237629547459967721466289939994921294419425809130379171934077889845649797545847530636012213858657652407635281279658210469659865085709703462588320658062385476080505247585160862953811958315

Como podemos ver acima, o cálculo da congruência está fora do alcance do lápis e papel, sendo efetuado usando um sistema de computação algébrica (MAPLE), podemos verificar que $196^{173} \equiv 131 \mod 247$

$D \equiv 196^{173} \mod 247 \equiv 196^{2^7} \cdot 196^{2^5} \cdot 196^{2^3} \cdot 196^{2^2} \cdot 196 \equiv 131 \cdot 157 \cdot 92 \cdot 118 \cdot 196 \equiv 131 \mod 247$.

Pensando na era computacional onde as mensagens são enviadas pela Internet, como se usa o sistema de criptografia RSA?

Já sabemos que o computador usa números binários representando cada caractere, então o texto é convertido em números binários assim que é escrito, esses números assim como os decimais são cifrados e decifrados, como já explicado, de acordo com a fórmula (4) de criptografar, e com a fórmula (5) de decriptar.

Na prática os números p e q são muito grandes, de forma que fatorar n para descobri-los e ter acesso ao ϕ, e consequentemente ao d, *a* chave privada, é pouco provável. Diz Schokranian [25] :"Para que as mensagens não possam ser decifradas no tempo padrão, é importante que p e q sejam escolhidos de tal forma que a fatoração de n seja difícil."

Portanto, o RSA é seguro quando não se consegue calcular d, conhecendo apenas n e e, tendo então que tentar fatorar n, e de acordo com Coutinho [4], "...se n for grande, este é um problema muito difícil, já que não são conhecidos algoritmos rápidos de fatoração."

Então a segurança do RSA depende da escolha dos primos p e q, que devem ser grandes, mas $|p - q|$ não pode ser pequeno, do contrário $n = p \cdot q$ poderá ser fatorado facilmente usando o algoritmo de Fermat.

Segundo Wiliam Crowell, da NSA, in Singh [26]:

> "Se todos os microcomputadores do mundo – aproximadamente 260 milhões de computadores pessoais – fossem colocados para trabalhar em uma única mensagem cifrada PGP, levaríamos, em média, 12 milhões de vezes a idade do universo para decifrar uma única mensagem."

Contudo, a história da criptografia nos faz repensar sobre o fato que, muitas delas foram consideradas inquebráveis, mas mesmo assim sofreram ataques de criptoanalistas e foram decifradas. A criptoanálise desenvolveu técnicas como: *tempest*, a qual intercepta mensagens antes de cifradas; vírus, os quais conseguem anotar a chave utilizada e o cavalo de Tróia, o qual envia cópias dos textos originais. Todas essas são úteis para coleta de informações, mas o objetivo vai mais além: quebrar a cifra RSA.

No futuro, provavelmente, teremos o computador quântico, que já é objeto de pesquisa, esse será capaz de quebrar a cifra RSA. Não se sabe quando os problemas de construir tais computadores serão superados, mas os criptógrafos já estudam a chamada criptografia quântica, um sistema que garantiria a segurança total das mensagens, sendo absolutamente inquebrável, porém esse sistema precisa ser aperfeiçoado para se tornar prático e operar através de longas distâncias.

3.1 Atividades

A criptografia RSA é mais complexa e só deve ser trabalhada em sala de aula se o professor entender que seus alunos estão preparados para compreender o processo de cifragem e decifragem. Mas sem dúvida ela deve ser mencionada e

mostrada aos alunos, no caso, do Ensino Médio, para que eles possam visualizar a importância que o estudo e pesquisas matemáticas trazem para seus cotidianos.

Nos exercícios abaixo utilizaremos a tabela 11, e a implementação RSA explicada no capítulo 3.

Nível 2

1) Em posse da chave pública (7, 51), cifre por RSA a palavra FATORAR. Depois descubra os valores de p e q e então a chave privada.

Substituição por números: 15102924271027
Separação em blocos de números menores que n(estamos apresentando uma das formas):

1 - 5 - 10 - 29 - 2 - 42 - 7 - 10 - 27

Cálculo da congruência: $C \equiv D^e \mod n$

$C \equiv 1^7 \mod 51 \longrightarrow 1^7 \equiv 1 \mod 51 \longrightarrow C = 1$
$C \equiv 5^7 \mod 51 \longrightarrow 5^7 = 78125$ e $78125 \equiv 44 \mod 51 \longrightarrow C = 44$
$C \equiv 7^7 \mod 51 \longrightarrow 7^7 = 823543$ e $823543 \equiv 46 \mod 51 \longrightarrow C = 46$
$C \equiv 10^7 \mod 51 \longrightarrow 10^7 = 10^3 \cdot 10^4$, $10^3 \equiv 31 \mod 51$ e $10^4 \equiv 4 \mod 51$
$\longrightarrow 124 \equiv 22 \mod 51 \longrightarrow C = 22$
$C \equiv 29^7 \mod 51 \longrightarrow 29^7 = 29^3 \cdot 29^4$, $29^3 \equiv 11 \mod 51$ e $29^4 \equiv 13 \mod 51$
$\longrightarrow 143 \equiv 41 \mod 51 \longrightarrow C = 41$
$C \equiv 27^7 \mod 51 \longrightarrow 27^7 = 27^3 \cdot 27^4$, $27^3 \equiv 48 \mod 51$ e $27^4 \equiv 21 \mod 51$
$\longrightarrow 1008 \equiv 39 \mod 51 \longrightarrow C = 39$
$C \equiv 42^7 \mod 51 \longrightarrow 42^7 = 42^3 \cdot 42^2 \cdot 42^2$, $42^3 \equiv 36 \mod 51$ e $42^2 \equiv 30 \mod 51$
$\longrightarrow 32400 \equiv 15 \mod 51 \longrightarrow C = 15$

Mensagem: 1, 44, 22, 41, 26, 15, 46, 22, 39
Fatorando: $n = 51 \longrightarrow 51 = 3 \cdot 17 \longrightarrow p = 3$ e $q = 17$
Chave privada: $\phi(51) = (3-1) \cdot (17-1) = 32$
$7 \cdot d \equiv 1 \mod 32 \longrightarrow 32 \cdot k = 7.d + 1$ para $k = 9$,
$288 = 7 \cdot 41 + 1 \longrightarrow 1 = 288 + (-41) \cdot 7$
$d = 288 - 41 = 247$.

Considerações Finais

Ao longo desse trabalho tivemos como objetivo a elaboração de um material adequado para enriquecer a prática do professor de matemática atuante em sala de aula, lhe dando um embasamento teórico e prático sobre criptografia, de forma que ele possa se utilizar desses para contextualizar conteúdos do currículo básico escolar, principalmente os destacados no trabalho: Análise combinatória, Funções, Matrizes, Algoritmo da Divisão entre outros.

Com isso, além de estimular a aprendizagem por parte do aluno, também buscamos primeiramente motivar o professor, despertando nele curiosidade sobre assuntos do seu cotidiano que podem ser investigados e aplicados a sala de aula, assim como a criptografia nos trouxe essa realidade, um tema a principio tão distante do ensino fundamental e médio, mas que aos poucos nos deu a oportunidade de ver a matemática que ensinamos todos os dias com outros olhos, reforçando ainda mais sua significância.

Inquestionavelmente a Criptografia é um assunto interessante, que nos fez mergulhar na sua história conhecendo sua importância no desenvolvimento da sociedade e nos surpreendendo com a relevante matemática envolvida na sua evolução até os dias de hoje. Embora a criptografia tenha encontrado na matemática a solução para seus problemas até o momento obtendo uma cifra extremamente eficaz, sua história não acaba aqui.

Referências

[1] Aldeia numa boa, Criptografia numa boa, *Frequência das Letras*,Disponível em http://www.numaboa.com.br/criptografia/criptoanalise/310-frequencia-portugues?showall=&limitstart= , Acessado em setembro, 23, 2014.

[2] Beker, H. ; Piper, F.,*Cipher systems: the protection of communications*, Northwood Bookds, London, 1982.

[3] Camp, Dane R., *Secret Codes with Matrices*, Mathematics Teacher, 78,(December 1985), pp. 676 - 680.

[4] Coutinho, Severino C.,*Números Inteiros e Criptografia RSA*, 2^a Edição, Rio de Janeiro, IMPA, 2013.

[5] Couto, Sérgio Pereira, *Códigos e Cifras: da antiguidade à era moderna*, Rio de Janeiro, Novaterra, 2008.

[6] Cruz, Edilson F. da, *A criptografia e seu papel na segurança da Informação e das comunicações*, Brasília, Universidade de Brasília, 2009. Disponível em http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/edilson_fernandes.pdf, acessado em: 10 out. 2014.

[7] *Diretrizes Curriculares da Educação Básica (DCEs)*, Secretaria de Estado da Educação do Paraná, Departamento de Educação Básica, disponível em:www.educadores.diaadia.pr.gov.br/arquivos/File/diretrizes/dce mat.pdf, acessado em: 02 de dez. 2014.

[8] Garcia, Arnaldo; Lequain, Yves, *Elementos da Álgebra*, 4^a Edição, Rio de Janeiro, IMPA, 2006.

[9] Gonçalves, Adilson, *Introdução à Algebra*, 5^a Edição, Rio de Janeiro, IMPA, 2007.

[10] Gorini, catherine A., *Using Clock Arithmetic to Send Secret Messages*, Mathematics Teacher, 89,(February 1996), pp. 100 - 104.

[11] Groenwald, Claudia Lisete O., *Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia*, XIII Conferência Interamericana de Educação Matemática, disponível em: www.gente.eti.br/lematec/CDS/XIIICIAEM/691.pdf, acessado em: 19 de jan. 2015.

[12] Hardy, G. H., *Apology Matematics*, disponível em: http://www.math.ualberta.ca/mss/misc/A%20Mathematician's%20Apology.pdf, acessado em: 10 out. 2014.

[13] Landau, Edmund; Hermann, Georg, *Teoria Elementar dos Números*, Rio de Janeiro, Ciência Moderna, 2002.

[14] Lefton, Phyllis, *Number Theory and Public - Key Cryptography*, Mathematics Teacher, 84,(January 1991), pp. 54 - 62.

[15] *Lei de Diretrizes e Bases da Educação Nacional Lei 9394/96(LDB)*, 2^a Edição, Paraná, APP- Sindicato, 1996.

[16] Menezes, A. J.; Van O.; Paul C.; and Vanstone, S. A.,*Handbook of Applied Crytpography*, CRC Press, 1997.

[17] Menezes, S., *Mensagens Secretas com Conteúdos Matemáticos da Educação Básica*, Sociedade Brasileira de Educação Matemática, disponível em: eemat.sbemrj.com.br/wp-content/uploads/2014/10/MC3 Sandra MariaLucia.pdf, acessado em: 19 de jan. 2015.

[18] Olgin, C. de A., *Criptografia e os conteúdos matemáticos do Ensino Médio*, XIII Conferência Interamericana de Educação Matemática, disponível em: www.gente.eti.br/lematec/CDS/XIIICIAEM/2092.pdf, acessado em: 19 de jan. 2015.

[19] *Parâmetros Curriculares Nacionais (PCNs), ensino médio*, Ministério da Educação, disponível em: portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf, acessado em: 18 de jan. 2015.

[20] *Parâmetros Curriculares Nacionais (PCNs), séries iniciais*, Ministério da Educação, disponível em: portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf, acessado em: 18 de jan. 2015.

[21] Petras, Richard T., *Privacy for the Twenty - First Century*, Mathematics Teacher, 94,(November 2001), pp. 689 - 707.

[22] Rosen, Kenneth H., *Elementary Number Theory and its Applications*, Addison e Wesley Publishing Company, 1983.

[23] Sá, Ilydio P, de, *Tratamento da Informação na educação básica: Aritmética Modular e os Códigos de identificação do cotidiano*, disponível em: www.sbembrasil.org.br/files/ix enem/Minicurso/Trabalhos/MC26269805791T.rtf, acessado em: 14 de nov. 2014.

[24] Santos, José Plínio de O., *Introdução à Teoria dos Números*, 3^a Edição, Rio de Janeiro, IMPA, 2011.

[25] Shokranian, S., *Criptografia para Iniciantes*,Ciência Moderna,2^a Edição, 2012.

[26] Singh, S., *O livro dos Códigos:A ciência do sigilo - do antigo Egito à Criptografia Quântica*,Record,10^a Edição, 2014.

[27] Wrigth, Marie A., *Convectional Cryptography*, Mathematics Teacher, 86,(March 1993), pp. 249 - 251.

Apêndice

1. Sugestão de Filme:

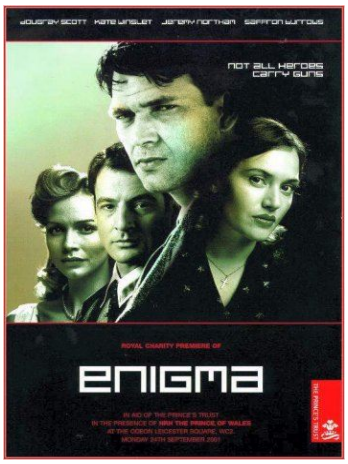


Figura 5: Filme Enigma

Título: ENIGMA

Diretor: Michael Apted

Produção: Mick Jagger e Lorne Michaels

Companhias produtoras: Intermedia e Broadway Video

Lançado em: 24 de Setembro de 2001

Nacionalidade: Alemanha, Holanda, EUA e Reino Unido

Gênero: Suspense

Duração: 1h48min

Disponível em:

http://www.filmesonlinegratis.net/assistir–enigma–dublado–online.html

Sinopse:

Em março de 1943, a equipe de elite dos decodificadores da Inglaterra em Bletchley Park, tem uma responsabilidade monumental: decifrar o Enigma, um código ultraseguro utilizado pelos nazistas para enviar mensagens aos seus submarinos. O desafio fica ainda maior quando se sabe que uma grande esquadra de navios mercantis está prestes a cruzar o Atlântico e cerca de dez mil homens correrão perigo caso a localização dos submarinos alemães não seja logo descoberta, o que apenas poderá ocorrer quando o Enigma for decifrado. Para liderar este trabalho é chamado Tom Jericho (Dougray Scott), um gênio da matemática que consegue realizar tarefas consideradas

impossíveis pelos especialistas. Porém, ao mesmo tempo em que Jericho se envolve cada vez mais com a decodificação do Enigma ele precisa estar atento à sua namorada Claire (Saffron Burrows), uma sedutora e misteriosa mulher que pode estar trabalhando como espiã para os alemães.

Em sala de aula:

O filme relata um trecho de como a Criptografia e os matemáticos foram importantes na história e no percurso da Guerra, embora esteja apoiado num romance, seu conteúdo serve como base para o professor iniciar e estimular os alunos a estudar Criptografia. Por conter algumas cenas fortes, aconselha-se para o Ensino Médio.

2. Geogebra:

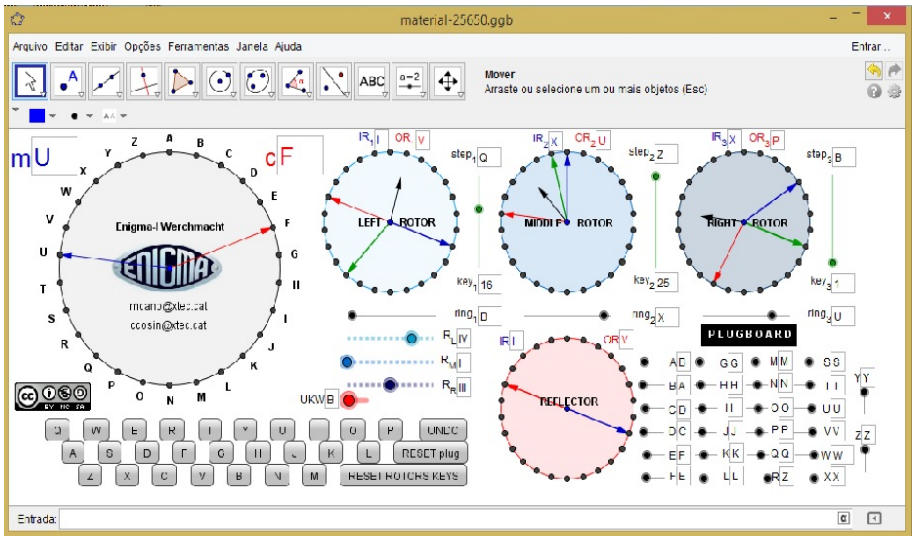


Figura 6: Tela da Enigma no Geogebra

Este arquivo simula o funcionamento da máquina Enigma e pode ser baixado para uso em qualquer computador que já tenha instalado o software Geogebra.

É bem interessante, pois os alunos podem vivenciar como a máquina Enigma funcionava, mas de forma tecnológica.

Para uso desse arquivo recomendo ao professor que o experimente bastante antes de levar à sala de aula devido a sua complexidade.

Está disponível e encontra-se explicação de uso em:

http://tube.geogebra.org/material/show/id/25650

Para mais informações e leitura sobre a máquina Enigma:

http://www.cryptomuseum.com/crypto/enigma/index.htm

3. Software Enigma:

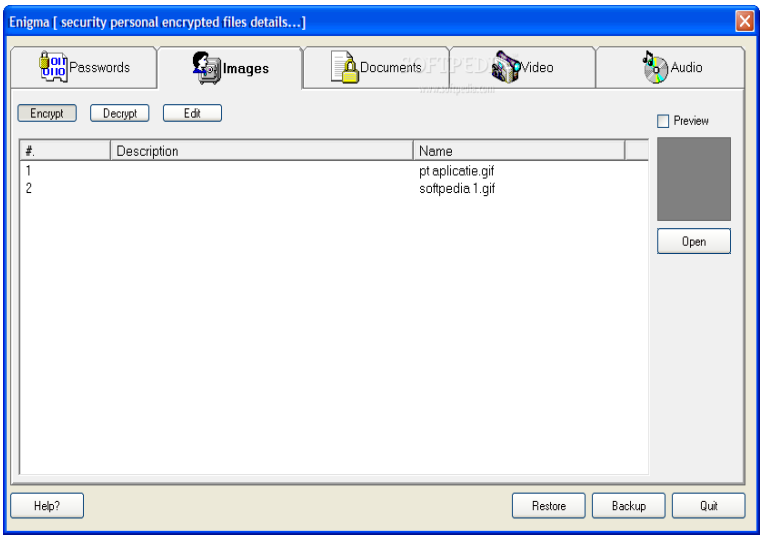


Figura 7: Tela do Software Enigma

É um software de criptografia pago, mas pode ser mencionado para os alunos como curiosidade, para que eles saibam que a criptografia está disponível para a sociedade, embora não tão aperfeiçoada quanto a que é usada pelos bancos e departamentos de segurança.

Esse software permite ao usuário armazenar imagem, vídeo, documentos, áudios e senhas para que só ele possa visualizálos. O software Enigma, tranca todas as informações em um único banco de dados criptografado, e permite criptografar e armazenar quase qualquer coisa para que somente o usuário possa acessar os arquivos através de uma senha mestra escolhida por ele. Todos ou qualquer um dos arquivos criptografados podem ser restaurado ao seu estado original a qualquer momento. O usuário ainda pode até mesmo fazer backup e restaurar todo o banco de dados para um CD ou pen drive para garantir que não perca nada.

Disponível para compra em:

http://www.softpedia.com/get/Security/Encrypting/Enigma.shtml

4. Sites interessantes:

Esses sites possuem reportagens, explicações, exemplos, atividades onlines e até prêmios para quem conseguir decifrar alguns códigos.

http://www.numaboa.com.br/criptografia

http://oglobo.globo.com/sociedade/tecnologia/livro–jogo–esconde–pistas–que–darao– premio–de–us–500–mil–quem–desvendar–misterio–14253987

http://super.abril.com.br/tecnologia/segredo–criptografia–441354.shtml

http://www.zahar.com.br/sites/default/files/arquivos/trecho_SAUTOY _Os-MisteriosDosNumeros.pdf

http://www.abc.org.br/article.php3?id_article=3525

http://www.foxplaybrasil.com.br/show/10857–jogos–numericos

5. Programas que facilitam os cálculos:

   Software MatLab

   http://www.wolframalpha.com (calculadora on line)

6. Literatura:

   Muitos autores que gostavam da criptografia incluíam-na em suas obras, alguns:

   Dan Brown—Obras: Fortaleza Digital; O Código da Vinci

   Júlio Verne—Obras: Viagem ao Centro da Terra; Mathias Sandrof

   Edgar Allan Poe—Obras: O Escaravelho de Ouro

   Arthur Conan Doyle—Obras: A Aventura dos Homenzinhos Dançantes; O Vale do Medo

   Umberto Eco—Obra: O Nome da Rosa

7. Sugestão de Filme:

Figura 8: O Jogo da Imitação

Título: O Jogo Da Imitação

Diretor: Morten Tyldum

Produção: Nora Grossman, Ido Ostrowski e Teddy Schwarzman

Companhias produtoras: Black Bear Pictures e Bristol Automotive

Lançado em: 05 de fevereiro de 2015

Nacionalidade: EUA e Reino Unido

Gênero: Drama/ Biografia

Duração: 1h55min

Sinopse:

Durante a Segunda Guerra Mundial, o governo britânico monta uma equipe que tem por objetivo quebrar o Enigma, o famoso código que os alemães usam para enviar mensagens aos submarinos. Um de seus integrantes é Alan Turing (Benedict Cumberbatch), um matemático de 27 anos estritamente lógico e focado no trabalho, que tem problemas de relacionamento com praticamente todos à sua volta. Não demora muito para que Turing, apesar de sua intransigência, lidere a equipe. Seu grande projeto é construir uma máquina que permita analisar todas as possibilidades de codificação do Enigma em apenas 18 horas, de forma que os ingleses conheçam as ordens enviadas antes que elas sejam executadas. Entretanto, para que o projeto dê certo, Turing terá que aprender a trabalhar em equipe e tem Joan Clarke (Keira Knightley) sua grande incentivadora.

Em sala de aula:

O filme relata um trecho de como a Criptografia e os matemáticos foram importantes na história e no percurso da Guerra, em particular a história do matemático Alan Turing. Seu conteúdo serve como base para o professor iniciar e estimular os alunos a estudar Criptografia.

8. Sugestão de Filme:

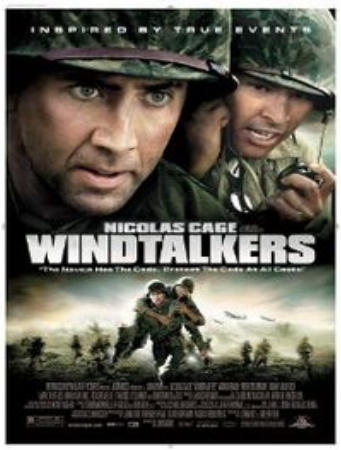


Figura 9: Filme Windtalkers

Título: Windtalkers ou Códigos de Guerra

Diretor: John Woo

Companhia produtora: MGM

Lançado em: 2002

Nacionalidade: Estados Unidos

Gênero: Ação e guerra

Duração: 2h14min

Sinopse:

Durante a Segunda Guerra Mundial, ano de 1944, os Estados Unidos levam adiante a guerra contra o Japão, nas ilhas do Pacífico. Mas, algo vai mal para os americanos: o inimigo tem conseguido, de forma inteligente e constante, decifrar todos os códigos utilizados para cifrar as comunicações, e infligido, deste modo, muitas baixas e perdas.

Logo é desenvolvido um novo código, este sendo totalmente baseado na desconhecida e complexa língua dos índios Navajos, e, por isto mesmo, perfeito para o objetivo. Para utilizar o novo código são recrutados dezenas de navajos, que, incorporados às forças armadas, recebem treinamento militar e, principalmente, se tornam aptos a utilizar o código em qualquer situação.

Como tal código não poderia cair nas mãos do inimigo, algumas medidas são tomadas para resguardá-lo. Alguns dentre os melhores fuzileiros americanos são convocados para fazer a guarda pessoal dos codificadores: um deles é o sargento Joseph Enders, único sobrevivente de uma terrível batalha nas Ilhas Salomão, interpretado por Nicolas Cage.

Após uma breve recuperação no hospital naval, Enders assume a missão e recebe de seu oficial superior uma ordem de valor moral duvidoso: proteja o código a qualquer custo!

Em sala de aula:

O filme é baseado na incrível e verídica história da participação de membros da tribo ameríndia dos Navajos na criação de um código baseado em sua língua, e sua colaboração heróica para a vitória norte-americana sobre os japoneses em 1945. O professor pode trabalhar a importância da criptografia, e destacar que esse foi o único código nunca decodificado.

9. Sugestão de Filme:

Figura 10: Filme U–571

Título: U–571

Diretor: Jonathan Mostow

Produção: Dino De Laurentiis e Martha De Laurentiis

Companhias produtoras: Dino De Laurentiis Company e distribuído por Universal Pictures

Lançado em: 21 de Abril de 2000

Nacionalidade: Estados Unidos e França.

Gênero: Ação

Duração: 1h56min

Sinopse:

Este filme conta a história do submarino alemão que passa por problemas no Atlântico Norte. Devido a isso, pedem ajuda a outro submarino alemão, tendo a comunicação interceptada pelos Aliados. O submarino americano S-33, do comandante Dahlgren, se passa por alemão para capturarem a máquina alemã de criptografia Enigma, que está a bordo do submarino avariado.

O submarino americano é explodido pelo submarino alemão que socorreria o outro avariado. Desta forma os tripulantes americanos que estavam a bordo do submarino avariado tiveram que permanecer nele e seguir para a costa inglesa. Mas no caminho encontram um destróier alemão, que tem sua estação de rádio explodida pelos americanos. O submarino mergulha e o destróier começa a lançar cargas de profundidade, que danificam o submarino.

O capitão do u-boat resolve descer a 200 metros de profundidade, onde a pressão é tão grande que danifica o casco do submarino. A única chance

do u-boat é destruir o navio é usando um torpedo localizado na parte de trás do submarino e que está sem pressão para ser lançado. Um marinheiro tenta restabelecer a pressão e consegue, mas morre. O submarino explode o navio, mas o u-boat afunda. Os sobreviventes se abrigam em um bote.

Em sala de aula:

O filme relata como a Europa teve acesso ao livro de ligações diárias da máquina Enigma, ou seja, esse filme é o ínicio do filme Enigma sugerido. Seu conteúdo serve como base para o professor iniciar e estimular os alunos a estudar Criptografia.

Anexos

PERMUTAÇÃO

Nível 1

1) Alice cifrou a palavra PAZ usando permutação das letras e mandou através de um bilhete para sua colega Fernanda. De quantas, e quais as maneiras que Fernanda pode ter recebido esse bilhete?

2) Você e seus amigos tem um grupo no WhatsApp. Robson enviou ao grupo SARERPSU! Propondo que pagaria uma pizza para quem decifrasse. Decifre a mensagem.

3) No intervalo da aula, Ana recebeu no celular a seguinte mensagem: ECOVE DNILA, que está criptografada. Decripte-a para Ana.

4) Carlos quer convidar para o seu time de futebol um aluno artilheiro de outra turma, mas ninguém pode saber. Como são muito amigos eles já têm acordado um método de criptografia por ferrovia em duas linhas. Como ficará cifrada a pergunta: QUER SER DO MEU TIME NO TORNEIO DA ESCOLA?

Nível 2

1) João precisa mandar para Aline a mensagem: ME ENCONTRE NA ESCOLA. Os dois têm conhecimento da chave: blocos de 3 letras, permutação entre 1º e 2º bloco, 3º e 4º bloco e assim por diante até terminarem os blocos, e permutação entre a 1ª e 3ª letra de cada bloco. Como Aline receberá a mensagem?

2) Considere: TAME TAMI EACL AGEL

a) O que está escrito nessa mensagem?

b) Qual a chave de permutação?

c) Quantas permutações são possíveis em cada bloco?

d) Se cada bloco usar uma permutação diferente dos demais, de quantas formas poderei escrever a mensagem?

3) Quantos anagramas a palavra ESCOLA tem se:

a) S for a primeira letra?

b) S for a primeira e C a última letra?

c) S for a primeira, C a última letra e as letras OL permanecerem juntas nessa ordem?

4) Decifre o ditado popular usando a cerca de ferrovia e diga quantas linha você precisa usar:

AIESDOGCEEROEUSISMSCCLAIOOHORNMEPMHIAOAELPBOCAARS EMREOM

CIFRA DE CÉSAR

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

Tabela Cifra de César

Nível 1

1) Júlio César, Imperador Romano, costumava utilizar a criptografia para se comunicar com seus exércitos. Decifre a mensagem que Júlio enviou, ao seu oficial Cícero, utilizando a Cifra de César: DMXGDHVWDDFDPLQKR.

2) Dudu gostou muito da Cifra de César e resolveu usá-la para mandar um recado ao seu amigo Daniel. Como Daniel receberá a seguinte mensagem?

DANI VAMOS JOGAR VIDEO GAME HOJE A TARDE?

Nível 2

1) Edgar Allan Poe, autor do conhecido poema O Corvo, tinha um grande interesse por códigos e cifras, em seu conto mais famoso O Escaravelho de Ouro, o protagonistas tem que decifrar uma mensagem. Agora, decripte uma de suas frases, onde a chave é o título do seu conto mais famoso.

"CARHYZOBZAIHCOIBOWOMGOISZXZSGHSOZGHJXHSOCOEAWATO.
ZIAKKYHSZDKHTAZVZIJZ."

2) Descubra o título de uma das obras de Dalton Trevisan, escritor curitibano, sabendo que na cifragem foi utilizado algum dos 26 deslocamentos possíveis.

TBQJHRPSTRJGXIXQPETGSXSP

CIFRA 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

Quadrado de Vigenère

Nível 1

1) Com a palavra-chave CÓDIGO, cifre o verso abaixo de Memória (Carlos Drummond de Andrade) pelo quadro de Vigenère.

"Mas as coisas findas
muito mais que lindas,
essas ficarão."

Nível 2

1) A frase VPKMJOCGPJYIAVZRPJ está cifrada de acordo com o quadro de Vigenère. Em posse da código-chave L3P11, que está no texto abaixo, decifre-a:

Texto:

´´E assim, aos poucos, ela se esquece dos socos, pontapés, golpes baixos que a vida lhe deu, lhe dará. A moça - que não era Capitu, mas também tem olhos de ressaca - levanta e segue em frente. Não por ser forte, e sim pelo contrário: por saber que é fraca o bastante para não conseguir ter ódio no seu coração, na sua alma, na sua essência. E ama, sabendo que vai chorar muitas vezes ainda. Afinal, foi chorando que ela, você e todos os outros, vieram ao mundo."

Dom casmurro (Machado de Assis)

ADFGVX

/	A	D	F	G	V	X
A	k	1	g	y	5	f
D	l	a	4	h	2	m
F	s	3	z	q	7	t
G	v	j	b	9	i	e
V	r	8	p	w	0	u
X	c	x	6	o	d	n

Cifra ADFGVX

Nível 1

1) Na Primeira Guerra uma cifra muito famosa foi a conhecida ADFGVX. Se coloque no lugar de um soldado e cifre a mensagem PERIGO para seus amigos soldados, utilizando essa cifra.

a) Faça a substituição através da tabela dada.

b) Faça a transposição através da palavra-chave VIDA.

Nível 2

1) Cifre a palavra PASSÁRGADA utilizando o método ADFGVX e a palavra-chave RUA.

NÚMEROS BINÁRIOS

A	1000001	H	1001000	O	1001111	V	1010110
B	1000010	I	1001001	P	1010000	W	1010111
C	1000011	J	1001010	Q	1010001	X	1011000
D	1000100	K	1001011	R	1010010	Y	1011001
E	1000101	L	1001100	S	1010011	Z	1011010
F	1000110	M	1001101	T	1010111		
G	1000111	N	1001110	U	1010101		

ASCII

Nível 1

1) Cifre a palavra LIVRO através de uma cifra de substituição, use a palavra TIGRE como chave, da seguinte forma: escreva ambas em bits via ASCII, então, na junção da mensagem com a palavra-chave, se os dígitos forem iguais escreva na mensagem criptografada 0 e se os dígitos forem diferentes escreva 1.

Nível 2

1) Cifre o nome FERMAT através de uma transposição, trocando os dígitos da palavra, o primeiro com o segundo, o terceiro com o quarto, e assim por diante.

FUNÇÕES

a	b	c	d	e	f	g	h	i	j	k	l	m
1	2	3	4	5	6	7	8	9	10	11	12	13
n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

Substituição de letras por números

Nível 1

1) Lari encontrou um bilhete embaixo da sua carteira: BJNOJHPDOJYZPJXZ, como sua professora de matemática havia trabalhado em sala criptografia, desconfiou que aquelas letras poderiam estar escondendo alguma mensagem, curiosa levou para casa e tentou decifrá-lo, já descobriu que foi utilizado a seguinte regra para criptografar: valor da letra -5. Com essa informação decifre a mensagem.

2) A professora Kelly propôs aos alunos para escolherem um trecho de uma música que gostam e cifrarem para colocar no mural da sala de aula como desafio da semana. Guilherme escolheu o seguinte trecho da música do Legião Urbana: "É PRECISO AMAR AS PESSOAS COMO SE NÃO HOUVESSE AMANHÃ" e resolveu cifrá-lo aplicando os seguintes cálculos: subtrair 3 e multiplicar por 5. Como ficará sua mensagem após cifrada?

Nível 2

1) O professor Rodrigo toda sexta passa um desafio aos seus alunos referente a algum conteúdo que ele trabalhou durante a semana. Nessa semana ele explicou funções e também como curiosidade explicou criptografia, então no desafio resolveu dar um exercício envolvendo ambos os assuntos. Ele apresentou a função que utilizou para criptografar uma frase de Einstein e pediu aos seus alunos para de terminarem a função inversa e a mensagem original.

Função cifradora: $y = 3 \cdot x - 16$ e

Mensagem cifrada: $29, 47, 26, 11, -7, 29, 20, 47, 5, -13, 38, 29, 26, -4, -1, 29, 41, 47, -7, -1, 41, 41, 29, 50, -1, 23, -13, 26, 44, -1, 41, -4, 29, 44, 38, -13, -10, 20, 8, 29, -1, 26, 29, -4, 11, -1, 11, 29, 26, -13, 38, 11, 29.$

2) Cifre a palavra CIDADE através da função exponencial $y = 2^x - 3$.

3) Cifre a palavra ELEFANTE através da função polinomial cifradora: $f(x) = x^3 - x^2 - 2x + 5$.

MATRIZES

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Substituição de letras por números

Nível 2

1) Criptografe a frase no $\mathbb{R}^2$, através do processo $B \cdot M = C$ onde a matriz chave é $B = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$, M a matriz original com as letras dispostas ordenadamente nas colunas e C será a mensagem cifrada.

Frase: INFORMAÇÕES, SEGREDOS, MATRIZES E CRIPTOGRAFIA.

2) Sabendo que a matriz chave $A = \begin{pmatrix} 3 & 4 \\ 1 & 0 \end{pmatrix}$ foi usada para cifrar a partir do método $A \cdot M = C$ (M matriz original, com letras ordenadas em colunas e C matriz cifrada), determine a inversa de A e decifre a seguinte mensagem descobrindo qual é a importância da criptografia: 148, 20, 128, 8, 8, 0, 36, 8, 12, 0, 28, 4, 85, 23, 118, 6, 66, 22, 47, 13, 100, 0.

3) Em uma prova de matemática o professor solicitou em uma das questões que o aluno desenhasse e explicasse um sólido, cujo nome foi cifrado pela multiplicação de matrizes pelo processo $M \cdot A = E$, onde M é a matriz que contém o nome do sólido ordenado na linhas, A é a matriz chave e E a matriz cifrada. Descubra qual é o sólido, dadas $A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$ e $E = \begin{pmatrix} 40 & -18 \\ 13 & -4 \\ 17 & 0 \end{pmatrix}$.

ARITMÉTICA MODULAR

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Substituição de letras por números

Nível 1

1) O relógio está marcando 8:00, e ainda é de manhã, minha mãe me avisou que daqui a 9 horas tenho consulta médica.

a) Para que horas está agendada a consulta?

b) Se estivéssemos trabalhando com um relógio que conta de 12 em 12 horas ao invés das 24 horas o habitual no Brasil, que horário é a consulta?

c) O algoritmo da divisão é **dividendo = quociente x divisor + resto**, se o divisor é 12, o dividendo 17, e o quociente 1, qual é o resto? Qual a relação com os resultados anteriores?

2) Joana faz aniversário dia 1 de janeiro e sua mãe dia 17 de abril. Sabendo que seu aniversário caiu em uma quarta em 2014, em que dia da semana caiu o aniversário de sua mãe nesse mesmo ano? (não vale olhar no calendário, é claro!).

3) A informação que devemos conhecer para trabalhar problemas periódicos através da aritmética modular é o ..... do fenômeno. Esse valor será o ..... da divisão. E a aritmética modular faz uma relação entre os números que apresentam o mesmo ..... quando divididos por um mesmo número não nulo.

4) Cifre NÚMERO, sendo o quociente 2, o divisor é 26 e o resto é o valor de cada letra da palavra, e o dividendo é a cifra.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Substituição de letras por números

Nível 2

1) Resolva as congruências:

a) $93 \equiv x \mod 5$

b) $(26 + 32) \equiv x \mod 7$

c) $(8.43) \equiv x \mod 8$

d) $7^{26} \equiv x \mod 12$

e) $56^{13} \equiv x \mod 13$

f) $x \equiv 2 \mod 30$

2) No CPF, o décimo dígito(que é o primeiro dígito verificador) é o resultado de uma congruência módulo 11, de um número obtido por uma operação dos primeiros nove dígitos. Devemos multiplicá-los, nessa ordem, pelos valores 1, 2, 3, 4, 5, 6, 7, 8, 9 e somar os produtos obtidos. O décimo dígito, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \mod 11$. Note que tal número será o próprio resto da divisão por 11 da soma obtida. Suponha que o CPF de uma pessoa é formado pelos os seguintes nove primeiros dígitos: 245.103.201, determine através do processo acima o décimo dígito:

Para cifrar usamos de maneira geral $C \equiv a \cdot P + k \, mod \, 26$

Para decifrar usamos $P \equiv \overline{a} \cdot (C - k) \, mod \, 26$,

P – número da letra original

C – número da letra cifrada

a – número inteiro tal que $(a,26)=1$

k – número inteiro positivo

$\overline{a}$ - inverso de a, ou seja, $\overline{a} \cdot a \equiv 1 \, mod \, 26$

Quadro - Método para criptografar por aritmética modular

3) Criptografe TECNOLOGIA, para $a = 1$ e $k = 3$.

4) Verifique se é possível usar $a = 7$ e use $k = 10$. Depois cifre a palavra SECRETO com esses valores.

RSA

a	b	c	d	e	f	g	h	i	j	k	l	m
10	11	12	13	14	15	16	17	18	19	20	21	22
n	o	p	q	r	s	t	u	v	w	x	y	z
23	24	25	26	27	28	29	30	31	32	33	34	35

Conversão de letras por números

Nível 2

1) Em posse da chave pública (7, 51), cifre por RSA a palavra FATORAR. Depois descubra os valores de p e q e então a chave privada.