UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Criptografia: dos rudimentos à atualidade

Emerson Joaquim de Araújo

Rio de Janeiro
2018

Emerson Joaquim de Araújo

Criptografia: dos rudimentos à atualidade

Trabalho de Conclusão de Curso apresentado ao
Programa de Pós-graduação em Matemática
PROFMAT da UNIRIO, como requisito para a
obtenção do grau de MESTRE em Matemática.

Orientador: Ronaldo da Silva Busse
Doutor em Matemática - UFRJ

Rio de Janeiro
2018

De Araújo, Emerson Joaquim

Criptografia: dos rudimentos à atualidade / Emerson Joaquim de Araújo – 2018

76.p

1.Matemática 2. Álgebra. I. Título

Criptografia: dos rudimentos à atualidade

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Aprovado em 12/12/2018

BANCA EXAMINADORA

Ronaldo da Silva Busse
Doutor em Matemática – UFRJ

Fábio Xavier Penna
Doutor em Matemática – IMPA

Vânia Cristina Machado
Doutora em Matemática – UFRJ

Dedicatória

A Deus, o Autor e Consumador de minha fé, a minha esposa por ter me dado forças nos momentos difícies ao longo dessa jornada, aos meus pais por mim guiarem ao caminho do estudo e aprendizagem e a todos meus colegas do PROFMAT que de alguma forma contribuíram para a conclusão deste trabalho.

Agradecimentos

Ao fim desta caminhada aproveito para agradecer àqueles que, direta e indiretamente, contribuíram nesta conquista, por isso agradeço:

A Deus, por ter me orientador e dado forças para continuar enfrentando as dificuldades ao longo do curso e por esta concedendo mais uma conquista na minha vida.

A minha amada e querida esposa, pelo apoio e compreensão, mesmo nos momentos de estresse.

Ao Professor Ronaldo, orientador deste trabalho, que de forma compreensiva e acolhedora deu um “norte” no desenvolvimento dessa obra.

A todos os professores do PROFMAT – UNIRIO, que contribuíram de forma significativa com profissionalismo, dedicação, incentivo e qualidade das aulas.

Aos colegas do PROFMAT, pelos momentos de convivência e conhecimentos compartilhados. Em particular a Alcebiades, João Jolvino, Márcio, Luiz Leão, Luciane, Leandro e Vandré pela amizade e companherismo.

Enfim, a todos que contribuíram para que essa conquista fosse possível.

Resumo

Este trabalho tem por objetivo apresentar a evolução da criptografia e mostrar de forma clara e concisa a diferença existente entre a criptografia simétrica e a assimétrica, detalhando em exemplo o seu funcionamento. Apresenta, ainda, um breve histórico sobre o desenvolvimento da criptografia, desde o seu surgimento até a Era Moderna, mostrando como a evolução dos antigos métodos criptográficos culminaram nos mais modernos sistemas de criptografia. Finalmente, para melhor compreensão do contéudo, também é feito um resumo de tópicos da Teoria dos Números.

Palavras-chave: Criptografia, criptografia simétrica, criptografia assimétrica.

Abstract

This work aims to present the evolution of cryptography and to show in a clear and concise way the difference between symmetric and asymmetric cryptography, describing in detail their operation. It also presents a brief history of the development of cryptography, from its inception to the Modern Era, showing how the evolution of the old cryptographic methods culminated in the most modern cryptography systems. Finally, for a better understanding of the content, a summary of Number Theory topics will also be done.

Keywords: cryptography, symmetric cryptography, asymmetric cryptography.

LISTA DE FIGURAS

Sumário

Introdução

Um dos problemas enfrentados pelos seres humanos ao longo do tempo foi a nessecidade de trocar informações, sem perigo de interceptação, desde a mais remota civilização até os dias modernos este continua sendo um dos desafios mais intrigantes.

A palavra criptografia vem do grego Kryptós “escondido” e gráphein “escrita”, e por definição é a ciência que estuda as formas e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível aos que não tem acesso as convenções previamente estabelecidas, e a criptoanálise é a ciência que estuda as formas de se decifrar tais informações.

Ao longo do tempo a evolução criptográfica tornou-se necessária, pois os métodos usados estavam ficando absoleto e de fácil decodificação, devido a isto surgiu a necessidade de usar cada vez mais técnicas e métodos de difícil solução.

Atualmente a criptografia consiste em uma série de fórmulas matemáticas, em que se utiliza um segredo (chamado de chave) para cifrar e decifrar as mensagens. Este segredo pode ser o mesmo para as duas operações (criptografia simétrica) ou pode haver segredos diferentes, um para cifrá-la e outro para decifrá-la (criptografia assimétrica).

Neste trabalho iremos mostrar como a criptografia evoluiu ao longo dos séculos e estudar alguns algortimos simétricos e assimétricos, onde mostraremos de forma concisa e simples o funcionamento dos mesmos através de exemplos simples, mas ao mesmo tempo complexo, pois a realização dos passos requer uma atenção ímpar.

Definiremos para compreenssão e fácil entendimento alguns termos segundo Stallings (2015). Uma mensagem original é conhecida como texto claro, enquanto a mensagem codificada é chamada de texto cifrado. O processo de converter um texto claro em um texto cifrado é conhecido como cifração ou encriptação; restaurar o texto claro a partir do texto cifrado é decifração ou decriptação. Os muitos esquemas utilizados para encriptação constituem a área de estudo conhecida como criptografia. Esse esquema é designado sistema criptográfico ou cifra. As técnicas empregadas para decifrar uma mensagem sem qualquer conhecimento ou detalhes de encriptação estão na área da criptoanálise, que é o que os leigos chamam de “quebrar o código”. As áreas da criptografia e criptoanálise, juntas, são chamadas de criptologia.

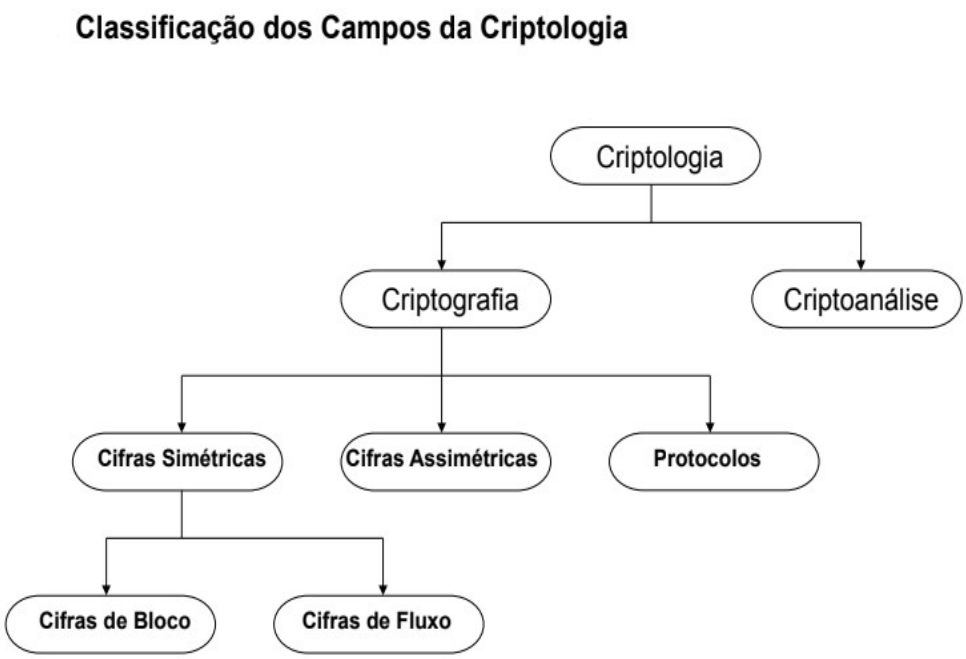


Figura 1: Classificação dos Campos da Criptologia
(Fonte: Entendendo Criptografia – Um livro texto para estudantes e profissionais)

No primeiro capítulo, apresentaremos um resumo histórico, mostrando a evolução da criptografia desde a Civilização Egípcia à Segunda Guerra Mundial.

No segundo capítulo, apresentaremos os conceitos preliminares em teoria dos números e a noção de número primo, que será o ingrediente fundamental para o desenvolvimento da criptografia simétrica e mais ainda na assimétrica.

No terceiro capítulo, apresentaremos com mais detalhes a criptografia simétrica, onde abordaremos o modelo da cifra, formas de ataques, algumas das principais técnicas de encriptação e culminaremos com o Data Encryption Standard (DES), que foi o algoritmo de encriptação simétrica dominante por muitos anos, especialmente em aplicações financeiras.

Finalmente, no quarto capítulo, apresentaremos a criptografia assimétrica, onde mostraremos o modelo da cifra, a criptoanálise de chave pública, o algoritmo RSA, a descrição matemática do algoritmo RSA e um exemplo do RSA.

CAPÍTULO 1

Navegando na história da Criptografia

1.1 – IDADE ANTIGA

1.1.1 – Khnumhotep II

Segundo Kahn (1996), um dos primeiros relatos que se tem sobre um texto escrito que incorporou um dos elementos essenciais da criptografia: uma transformação deliberada da escrita, data de 1900 a.c., a história aconteceu numa vila egípcia perto do rio nilo chamada Menet Khufu. O Khnumhotep II, homem de grande importância, arquiteto do faraó Amenemhet II, construiu alguns monumentos para o faraó, os quais precisavam ser documentados, contudo essas informações, escritas em tabletes de argila, não deveriam cair no domínio público. Foi então que o escriba Khnumhotep II teve a ideia de substituir algumas palavras ou trechos de texto desses tabletes. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro - morreria de fome e sede, perdido nas catacumbas da pirâmide, pois os faraós acreditavam que a morte era apenas uma passagem para outra vida e com isto, em sua tumba deveria ter tudo que uma pessoa precisaria para viver, tais como: ouros, comidas, roupas, utensílios, etc.

Figura 2: Tumba de Khnumhotep II
(Fonte: https://br.pinterest.com/pin/363243526177139263/)

1.1.2 – Mesopotâmia

Para Kahn (1996), a quarta grande civilização da antiguidade, a Mesopotâmia, superou o Egito na questão criptográfica, pois foi por volta de 1500 a.c. chegou a um nível bastante moderno, o primeiro registro do uso da criptografia nesta região está numa fórmula para fazer esmaltes para cerâmica. O tablete usava símbolos especiais que podem ter vários significados diferentes.

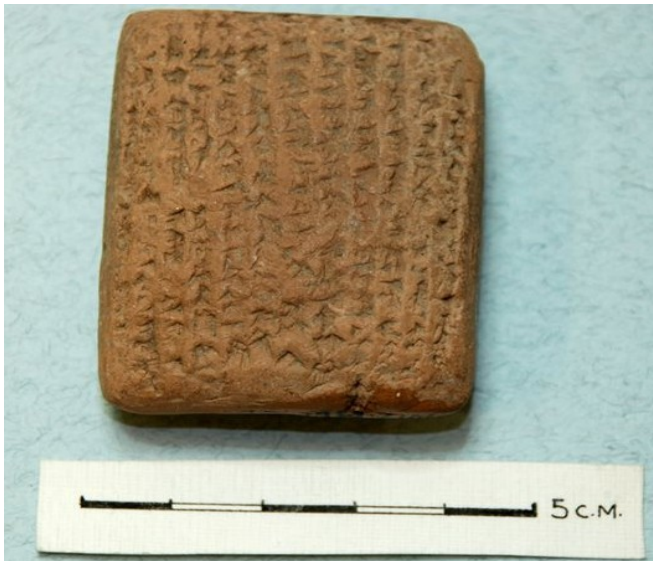


Figura 3: Tablete de cerâmica da Mesopotâmia
(Fonte: https://www.museum.ie/The-Collections/ Documentation-Discoveries/March-2016/Cuneiform-tablets-the-genesis-of-documentation)

Nessa época os egípcios, chineses, indianos e os mesopotâmios desenvolveram a esteganografia[1] (escrita cifrada):

- Tatuagens com mensagens na cabeça de escravos. Infelizmente era preciso esperar o cabelo crescer para esconder a mensagem. A decifração era feita no barbeiro.
- Marcas na parte interna de caixas de madeira usadas para transportar cera. As marcas eram escondidas com cera nova. Para decifrar, bastava derreter a cera.
- Mensagens colocadas dentro do estômago de animais...e também de humanos.

1.1.3 – Antigo Testamento

Segundo Kahn (1996), também foram descobertos escritos em Uruk (atual Iraque) em

1 Esteganografia era uma palavra absoleta que foi revivida por David Kahn e recebeu o significado que tem hoje.

que os escribas ocasionalmente convertiam os nomes dos reis selêucidas em números.

As sagradas escrituras não escaparam a um toque de criptografia, a tradição hebraica oferece pelo menos duas dessas conversões no Antigo Testamento (nenhum é registrado para o novo). Em Jeremias 25:26 e 51:41, a forma SESAQUE aparece no lugar de Babel ("Babilônia"). A segunda ocorrência demonstra claramente a falta de um motivo de sigilo, uma vez que a frase com *SESAQUE* é imediatamente seguida por uma usando "Babilônia": Como foi tomada SESAQUE, e apanhada de surpresa a glória de toda a terra! Como se tornou Babilônia um espanto entre as nações. A confirmação de que SESAQUE é realmente um substituto para Babel e não um lugar totalmente separado vem da Septuaginta e dos Targuns, as paráfrases aramaicas da Bíblia, que simplesmente usam "Babel", onde a versão do antigo Testamento tem SESAQUE. A segunda transformação, em Jeremias 51:1, coloca LEB KAMAI ("coração do rei") para KASHDIM ("caldeus"). Ambas as transformações resultaram de aplicação de uma substituição tradicional de letras chamada "atbash", na qual a última letra do alfabeto hebraico substitui a primeira letra e vice-versa, a penúltima substitui a segunda e vice-versa, e assim por diante. É o hebraico equivalente de a = z, b = y, c = x, …, z = A. Estas cifras baseiam-se no sistema de substituição simples (ou substituição monoalfabética).

Figura 4: Cifras hebraicas
(Fonte: http://www.quadibloc.com/crypto/ppen01.htm)

1.1.4 – Bastão de Licurgo

Conforme explica Singh (2007), outra forma usada na antiguidade para criptografar mensagens é o scytale ou bastão de Licurgo, foram usados pelos espartanos, os mais guerreiros dos gregos, esse foi o primeiro sistema de criptografia militar. No quinto século a.c., eles empregaram esse dispositivo que é o aparato mais antigo usado na criptografia e um dos poucos já inventados em toda a história da ciência para cifras de transposição. O sistema consiste em um bastão ou cajado de madeira em torno do qual uma tira de papiro, couro ou pergaminho é enrolada, a mensagem secreta é escrita no pergaminho no sentido do comprimento do bastão, o pergaminho é então desenrolado e enviado ao seu destino com as letras desconectadas e sem sentido, ou seja, a mensagem foi cifrada. Para que o destinatário consiga decifrar a mensagem é necessário que possua um bastão de mesma espessura e diâmetro que o primeiro, pois com isto conseguiria formar a mensagem enviada.

Figura 5: Bastão de Licurgo
(Fonte: Singh, 2007, p. 24)

1.1.5 – Cifra de César

Segundo Singh (2007), o primeiro documento que usa uma cifra de substituição com propósito militar aparece nas Guerras da Gália de Júlio César, imperador romano. Ele descreve como enviou uma mensagem para Cícero, que estava prestes a se render, pois estava cercado pelo exército inimigo. Nessa ocasião ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo. César descreve a dramática entrega da mensagem: “O mensageiro recebeu instruções para que, se não pudesse se aproximar, jogasse uma lança com a mensagem amarrada por uma tira de couro, dentro das fortificações do campo... Com medo, o gaulês arremessou a lança como fora instruído. Por acaso a arma encravou-se em uma torre e passou dois dias sem ser vista pelos nossos soldados, até que, no terceiro dia, um soldado a viu, retirando-a e entregando a mensagem

para Cícero. Ele a leu e depois a recitou em voz alta para a tropa em formação, trazendo grande alegria para todos."

Embora o imperador tenha usado a substituição das letras do alfabeto romano por letras gregas, a sua máxima em criptografar mensagens consiste em alterar as letras desviando-as em três posições, ou seja, A se tornando D, B se tornando E, etc. A seguir, um exemplo clássico da cifra de César:

Mensagem original: ATACAR PELO NORTE

Mensagem cifrada: DWDFDU SHOR QRUWH

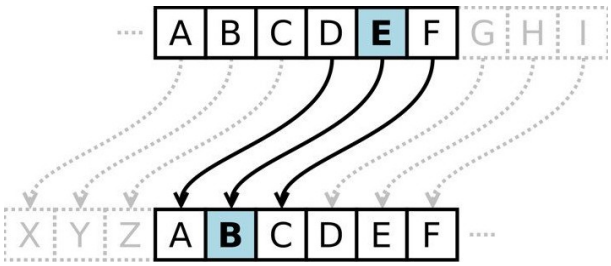


Figura 6: Cifra de César
(Fonte: https://pplware.sapo.pt/linux/whatcripto-identificador-decifrador-cifras-criptograficas/#foobox-1/3/Whatcripto_4.jpg).

Esse método possui uma fraqueza simples de se notar, pois uma simples análise das letras do idioma e um bom conhecimento de sua estrutura é possível uma pessoa decifrar a mensagem. Por exemplo, no caso do Português, é fácil verificar que a letra A aparece com maior frequência que as demais letras e que a letra Q sempre é precedida pela letra U.

1.1.6 – Outros destaques na idade Antiga

1.1.6.1 – Euclides de Alexandria (330 a.c. a 270 a.c.)

Compilou e sistematizou o que havia na época sobre geometria e teoria dos números. Escreveu "Elementos", obra que influênciou de forma significativa a criptografia moderna nos computadores.

1.1.6.2 – Erastótenes de Cirene (276 a.c. a 194 a.c.)

Criou o método conhecido como o "Crivo de Erastótenes", usado para identificar números primos.

1.1.7 – Políbio (204 a.c. a 122 a.c.)

Segundo Kahn (1996), Políbio inventou um sistema de sinalização que foi adotado amplamente como método criptográfico. Ele organizou as letras em um quadrado 5x5 e numerou as linhas e colunas.

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

Figura 7: Código Políbio

(Fonte: https://3l3m3nt4l.blogspot.com.br/2017/01/el-cuadrado-de-polibio.html)

Cada letra pode ser representada por dois números – o da linha e o da coluna. Assim, M = 32, P = 35. Políbio sugeriu que esses números fossem transmitidos por meio de tochas, ou seja, três tochas na mão direita e duas na mão esquerda representando o M, por exemplo. Esse método pode sinalizar mensagens por longas distâncias.

1.2 – IDADE MÉDIA

De acordo com Schneeberger (2007), esse período está compreendido entre os anos 476 a 1453, costuma-se ainda chamar a Idade Média de “Idade das Trevas”, pois teria sido uma época de muita ignorância e obscurantismo. Porém essa qualificação não corresponde à realidade. Além de ser pejorativa e preconceituosa, a pessoa que assim se manifesta revela desconhecimento histórico, pois foi uma época de notáveis realizações culturais, especialmente as da civilização muçulmana.

Nesse período se destacou o árabe Al-Kindi (Iraque, 801-853), conhecido como o filósofo dos árabes, foi o precursor da criptoanálise para a substituição monoalfabética, publicou um manuscrito sobre a decifração de mensagens criptográficas.

Figura 8: Al-Kindi
(Fonte:http://www.muslimheritage.com/)

De acordo com Wazlawick (2016), o manuscrito incluía uma descrição do método de análise de frequência para a decifração de mensagens criptográficas simples. Suponha, por exemplo, uma criptografia simples de substituição de símbolos na qual cada letra da mensagem original é substituída pela letra seguinte do alfabeto e o Z substituído pelo A. Com essa técnica, uma palavra escrita, por exemplo como “dsquphsbgjb” seria decifrada se substituíssemos cada letra imediatamente anterior no alfabeto, resultando assim na palavra: “criptografia”.

Agora imagine que as letras fossem substituídas de forma não tão lógica, como por exemplo, “A” por “N”, “B” por “%”, “C” por “9” etc. Como você decifraria uma mensagem como “HGS&JW%@KKS”? Sem saber o método de criptografia fica muito difícil traduzir a mensagem, pois cada caractere na frase pode ser, em princípio, qualquer uma das letras, números ou sinais especiais utilizados na escrita.

O método descrito por Al-Kindi baseia-se em uma análise estatística da frequência de cada letra numa determinada língua. Wazlawick (2016) mostra que em português, por exemplo, a letra mais frequente em textos é a letra “A”, que aparece em média 14,63%, seguida da letra “E” com uma média de 12,57%. Assim, em uma mensagem criptografada suficientemente longa, que se saiba estar escrita originalmente em português, um caractere que apareça por volta de 14,63% das vezes tem grande chance de ser a letra “A”. Já um caractere que apareça cerca de 12,57% das vezes tem chance de ser a letra “E”. E assim por diante.

1.3 – IDADE MODERNA

Schneeberger (2006) explica como ocorreu o desenvolvimento cultural nesse época:

> As condições básicas que proporcionaram o renascimento cultural foram as transformações socioeconômicas ocorridas na Europa durante a Baixa Idade Média, com destaque para a expansão urbano comercial, a ascensão da burguesia, o fortalecimento do poder real, a fundação das universidades e a renovação dos contatos com o mundo oriental.

A Itália foi a primeira a acordar, sendo responsável pelos primeiros grandes avanços, tanto na política, com Maquiavel, na medicina, com Leonardo da Vinci, na arte, com Michelangelo, entre outras. Em relação a criptografia destaca-se o italiano *Leone Battista Alberti*.

1.3.1 Disco de Alberti

Conforme explica Kahn (1996), Leone Battista Alberti é conhecido como o pai da criptografia ocidental, ele publicou, em 1466, o livro *Modes scribendi in ziferas*, onde fala do disco de cifra, o primeiro sistema polialfabético conhecido.

Figura 9: Leone Battista Alberti
(Fonte: https://gl.wikipedia.org/wiki/Leon_Battista_Alberti)

O disco de cifra era constituído por dois discos concêntricos e de raios diferentes. O disco maior era fixo, e o menor móvel. Alberti dividiu cada uma das circunferências em vinte e quatro setores, em cada um dos setores do disco maior escreveu o alfabeto em letras maiúsculas pela sua ordem normal, mas não continha as letras H, J, K, U, W e Y, nos quatro setores que sobraram colocou os algarismos 1, 2, 3 e 4.

Figura 10: Disco de Alberti
(Fonte: http://www.mateureka.it/wp-content/uploads/2012/11/disco-cifrante-leon-battista-alberti.jpg)

No disco fixo, colocou de uma forma normal, em cada um dos setores, as letras do alfabeto, que eram 20, e os numerais 1, 2, 3 e 4.

Já no disco móvel, colocou, em ordem aleatória, as letras minúsculas do alfabeto (exceto as letras j, u e w) mais a palavra et (que significa e).

Uma das desvantagens deste método, é que emissor e receptor têm que ter dois discos iguais e muito bem guardados, pois a segurança deste sistema depende de ocultar os discos de olhos indiscretos.

Segue abaixo um exemplo prático extraído de uma avaliação da disciplina de Criptografia do Centro de Educação a Distância do Estado do Rio de Janeiro (CEDERJ):

Para codificar ou decifrar mensagens utilizando discos de Alberti ou discos de cifras procedemos do seguinte modo:

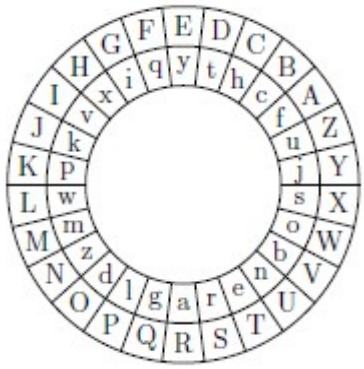
(i) Escolhemos a letra-chave (letra minúscula) e a palavra-chave (letras maiúsculas).

(ii) Coincidimos a letra-chave com a primeira letra da palavra-chave e obtemos a codificação da primeira letra da mensagem original através de sua correspondente no "disco das maiúsculas".

(iii) Coincidimos a letra-chave com a segunda letra da palavra-chave e obtemos a codificação da segunda letra da mensagem original através de sua correspondente no "disco das maiúsculas".

(iv) Repetimos estes procedimentos até a última letra da palavra-chave e, se a codificação não houver terminado, voltamos ao item (i), ou seja, coincidimos a letra-chave com a primeira letra da palavra-chave e obtemos a codificação da letra correspondente da mensagem original, continuando com o processo até concluir a codificação.

Por exemplo: Codifique a palavra cederj utilizando o disco de Alberti da figura abaixo, a **letra-chave n** e a **palavra-chave BOLA**



(i) coincidimos n com B e a letra maiúscula correspondente a c é I.

(ii) coincidimos n com O e a letra maiúscula correspondente a e é N.

(iii) coincidimos n com L e a letra maiúscula correspondente a d é F.

(iv) coincidimos n com A e a letra maiúscula correspondente a e é Z.

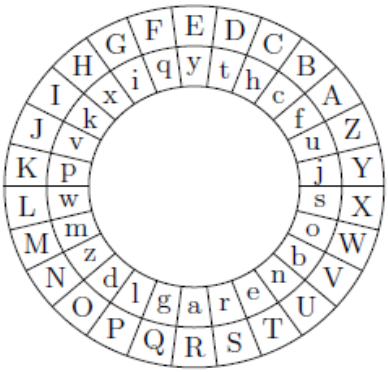
(v) coincidimos n com B e a letra maiúscula correspondente a r é Z.

(vi) coincidimos n com O e a letra maiúscula correspondente a j é S.

- A codificação de cederj é INFZZS.

Utilize o disco de Alberti da figura abaixo, a letra-chave k e a palavra-chave MAR para decodificar a mensagem

GUVPFJYVBZBAKBQYBMFUYP. (2.0 pontos)



Solução

Coincidindo a letra-chave k com M, A e R obtemos as três tabelas de decodificação

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

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

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

g	u	v	p	f	j	y	v	b	z	b	a	k	b	q	y	b	m	f	u	y	p
M	A	R	M	A	R	M	A	R	M	A	R	M	A	R	M	A	R	M	A	R	M
U	R	S	O	S	H	I	B	E	R	N	A	M	N	O	I	N	V	E	R	N	O

Portanto, a mensagem decodificada é:

URSOS HIBERNAM NO INVERNO.

1.3.2 Tabula recta

De acordo com Kahn (1996), a polialfabeticidade deu mais um passo em 1518, com o surgimento do primeiro livro impresso sobre criptografia, escrito por um dos mais famosos intelectuais de sua época. Este era Johannes Trithemius, um monge beneditino que se interessava por alquimia e outros poderes místicos, fez dele uma das figuras mais veneradas da ciência oculta.

Figura 11: Johannes Trithemius
(Fonte: https://codesandmagic.files.wordpress.com/2013/03/20710_trithemius_4100.jpg)

Johannes Trithemius criou uma cifra que recebeu o nome de *Tabula recta*, essa cifra foi descrita em um de seus livros, o terceiro volume de uma série. A *Tabula recta* consiste numa tabela de 26x26 preenchida da seguinte maneira: a primeira linha é preenchida com o alfabeto latino em ordem alfabética. A segunda linha é o mesmo alfabeto só que deslocado

uma casa para a esquerda. A terceira linha é deslocada em mais uma casa e assim por diante até chegarmos a 25 deslocamentos. No 26º deslocamento o ciclo se reinicia voltando-se à configuração inicial da primeira linha.


Recta transpositionis tabula.

In hac tabula literarū canonica siue recta tot ex uno & usuali nostre latinarum literarum ipsarum permutationem seu transpositionē habe alphabeta, quot in ea per totum sunt monogramma, uidelicet quate & uigesies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per tidē multiplicata, paulo efficiunt minus q quatuordecē milia.

o ij

Figura 12: Tabula recta
(Fonte: https: www.staff.uni-mainz.de/pommeren/Cryptology/Classic/2_Polyalph/Trithem.gif)

1.3.3 Cifra de Vigenère

Para Kahn (1996), embora os créditos sejam dados ao francês Blaise Vigenère, a cifra foi primeiramente descrita em 1553, por Giovanni Battista Belaso no livro intitulado por *La cifra del Sig Giovan Batista Belaso.* Esta cifra é constituída por 26 cifras de César, com diferentes variações. A diferença é que numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares, enquanto na cifra de Vigenère consiste de várias cifras de César com diferentes valores de deslocamentos.

Vejamos um exemplo para compreendermos o funcionamento da cifra:

Vamos encriptar a frase “matar o rei”, usando a palavra-chave “morte”. A palavra-chave deve ser repetida até completar o comprimento da mensagem a ser enviada, da seguinte forma:

Palavra-chave	m	o	r	t	e		m		o	r	t
Mensagem	m	a	t	a	r		o		r	e	i
Texto cifrado	y	o	k	t	v		a		f	v	b

A primeira letra do texto, que é a letra “m”, é cifrada com o alfabeto da linha “m”, que é a primeira letra da palavra-chave. Procuramos a letra na linha “m” que esteja a coluna “m”, que no caso é a letra “y”. Esta será a primeira letra do texto cifrado.

Passando para a segunda letra do texto normal, que é a letra “a”, procuramos a linha correspondente à letra “o”, segunda letra da chave, e localizamos a letra que esteja na intersecção dessa linha com a coluna da letra procurada, “a”. No caso, a letra é “o”, segunda letra do texto cifrado.

E assim sucessivamente, até o final da cifragem.

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

Figura 13: Cifra de Vigenère
(Fonte: http://cryptograma.blogspot.com.br/2015/06/historia-da-criptografia-cifras-e.html)

A supremacia da cifra de Vigenère teve fim em 1854 quando Charles Babbage, considerado o pai do computador, desenvolveu uma técnica criptanalítica capaz de extrair a chave do criptograma e decifrá-lo.

1.3.4 Cifra de Bacon

De acordo com Kahn (1996), Sir Francis Bacon, o inventor de um sistema esteganográfico, denominado seu alfabeto de bilateral, utilizou a combinação de duas letras, A e B em grupos de cinco. Esta cifra foi conhecida como Cifra de Bacon, hoje, é classificada como decodificação binária de 5 bits.

Letra	Grupo	Binário		Letra	Grupo	Binário
A	aaaaa	00000		N	abbaa	01100
B	aaaab	00001		O	abbab	01101
C	aaaba	00010		P	abbba	01110
D	aaabb	00011		Q	abbbb	01111
E	aabaa	00100		R	baaaa	10000
F	aabab	00101		S	baaab	10001
G	aabba	00110		T	baaba	10010
H	aabbb	00111		U/V	baabb	10011
I/J	abaaa	01000		W	babaa	10100
K	abaab	01001		X	babab	10101
L	ababa	01010		Y	babba	10110
M	ababb	01011		Z	babbb	10111

Figura 14: Cifra de Bacon
(Fonte: https://encdesarrollo.wordpress.com/2012/09/27/esteganografia-en-redes-sociales-2/)

1.4 – Era das Guerras

De acordo com C. L. Barczak (2014), foi durante o século XIX que humanidade teve um progresso considerável em relação ao desenvolvimento das ciências, tecnologias e das artes. No fim desse século a eletricidade e eletrônica tiveram grandes avanços, e um dos grandes marcos na ciência foi a descoberta da propagação das ondas eletromagnéticas por Heinrich Hertz que construiu circuitos para produzir e detectar a radiação eletromagnética. Chamadas de ondas Hertzianas hoje são mais conhecidas como ondas eletromagnéticas ou ondas de rádio.

Ainda segundo C. L. Barczak (2014), a história da invenção do rádio passa pelo Brasil através da figura do padre gaúcho Roberto Landell de Moura (Porto Alegre, 1862-1928), ele desenvolveu aparelhos para transmissão e recepção de voz humana sem a utilização de fios condutores como era usual na época nos sistemas de telefone e telégrafo. Ele fez uma experiência em São Paulo, entretanto o sucesso do feito o fez duvidarem de sua sanidade

mental. Sete anos depois conseguiu a patente brasileira de seu invento. Em 1901, embarcou para os Estados Unidos, mesmo sem apoio das autoridades brasileiras, lá ele conseguiu a patente do transmissor de ondas eletromagnéticas, do telégrafo sem fio e do telefone sem fio.

Entretanto, foi na Europa que outro pesquisador e inventor obteve sucesso com uma invenção similar ao de Landell de Moura, foi o físico italiano Guglielmo Marconi, que de forma independente construiu seus próprios circuitos e aparelhos. Em 1885 ele realizou experiências, demonstrando a possibilidade de telecomunicações a distância por meio de onda eletromagnéticas, no início as transmissões eram feita em pequenas distâncias, mas em 1886 Marconi embarcou para a Inglaterra em busca de apoio e financiamento, o qual conseguiu e de forma eficaz em 1889, ano em que instalou o telégrafo sem fio em dois navios, permitindo a transmissão de mensagens entre localidades distantes e isoladas. Utilizando o código Morse comprovou a possibilidade de comunicação a distância por meio de ondas eletromagnéticas. Em 1909, Marconi recebeu o Prêmio Nobel de Física.

Para Kahn (1996), o rádio foi aproveitado pelos generais logo após seu surgimento, em 1885, e utilizado como instrumento de guerra, pois ampliava de forma significativa a principal vantagem militar: controle instantâneo e contínuo de um exército inteiro por um único comandante, porém a vasta amplificação de comunicações militares pelo rádio era acompanhada por uma probabilidade enorme de interceptação.

1.4.1 – Primeira Guerra Mundial

Conforme explica C. L. Barczak (2014), em 1914, o Cruzador alemão Magdeburg fazia patrulha no Golfo da Finlândia quando foi descoberto por navios russos, para evitar um encontro com os russos o comandante procurou sair do local mantendo-se em silêncio, porém o navio entrou em um nevoeiro e possivelmente por erros de navegação acabou encalhado em águas rasas nas proximidades da Ilha Odensholm (hoje Ilha Osmussar). Não conseguindo se livrar do encalhe, o comandante pediu ajuda a outros navios, porém sem sucesso mesmo depois de muitas tentativas. Sem pode movimentar o navio o comandante decidiu por sua destruição, pois essa seria a melhor forma dos russos não capturar informações imprescindíveis. Entretanto, com a aproximação dos navios russos houve uma grande confusão e muitos dos documentos contendo manuais de códigos e chaves foram deixados para trás, pois antes do comandante dar a ordem de destruição do navio por cargas explosivas,

um tripulante acionou antes que fosse dado a ordem final o que ocasionou o abandono do navio imediatamente e consequentemente a morte de muitos tripulantes. Em virtude de todos esses transtornos muitos documentos e vários livros de códigos acabaram esquecidos. Mesmo depois das explosões, o Magdeburg não afundou permanecendo encalhado. Com isto os marinheiros russos puderam entrar no navio e fazer busca por documentos que pudessem colocar em "xeque" a Alemanha, vários livros de códigos foram encontrados, devido ao grande valor do achado, os russos distribuíram cópias dos livros e das chaves de cifração aos aliados britânicos. Com o auxílio desses achados, os britânicos procuraram decifrar os códigos alemãs, porém não obtiveram sucesso, pois faltava alguma chave.

Só em agosto de 1914 com a captura do navio mercante alemão Hobart, foi possível decifrar os códigos da Marinha alemã, pois neste navio estava o código que faltava. Esse foi o ponto crucial que causou a derrota da Alemanha na Primeira Guerra Mundial.

1.4.2 – Enigma e a Segunda Guerra Mundial

Foi em fevereiro de 1918 que o engenheiro elétrico e inventor alemã Arthur Scherbius submeteu sua patente para uma máquina de cifragem usando rotores. Nessa época, Scherbius fundou a empresa Scherbius & Ritter, junto com seu amigo Richard Ritter. Sinhg (2007) relata o começo:

> Era uma firma de engenharia inovadora que trabalhava com tudo, de turbinas a travesseiros aquecidos. Scherbius estava encarregado da área de pesquisa e desenvolvimento e buscava sempre novas oportunidades. Um de seus projetos era substituir os sistemas de criptografia inadequados, usados na Primeira Guerra Mundial, trocando-se as cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. […] ele desenvolveu uma máquina criptográfica que era basicamente, uma versão elétrica do disco de cifras de Alberti. Chamada de Enigma, a invenção de Scherbius se tornaria o mais terrível sistema de cifragem da História.

Scherbius e Ritter procuraram a Marinha alemã, mas não houve interesse pela máquina. Os oficiais acreditavam que a máquina provia boa segurança, mas não acharam que houvesse tráfego suficiente de informações para torná-la necessária.

Scherbius e Ritter então transferiram os direitos de patente para a *Gewerkschaft Securitas*. Em 09 de julho de 1923, a *Securitas* fundou a *Chiffriermaschine Aktien-Gesellschaft* (ou máquinas de Cifragem de Sociedade Anônima), em cuja diretoria estavam

Scherbius e Ritter, até este momento a Enigma foi produzida e comercializada no meio civil, o primeiro modelo foi denominado enigma A.

Embora não tenha vingado comercialmente, a máquina Enigma, com algumas alterações, foi finalmente adotada pela Marinha alemã em 1926 (Kahn, 1996) e, alguns anos mais tarde, em 1928, e com mais alterações, pelo Exército.

Várias versões da enigma foram adquiridas por diferentes nações, tais como a Polônia, que adquiriu uma versão da Enigma C para estudos pelos serviços de inteligência. A Marinha italiana comprou a Enigma D, assim também como a Espanha durante a Guerra Civil Espanhola. O Exército suiço usou a Enigma modelo K, uma versão modificada da Enigma D. O Japão usou o Enigma T, também chamada de Enigma Tirpiz, uma adaptação da Enigma D.

Dentre os vários modelos da Enigma, a que mais causou transtorno e assombro na sua "quebra" de código foi a Enigma M4, exclusivamente desenvolvida para a divisão U-Boot da *Kriegsmarire* (Marinha Alemã), teve papel fundamental na Batalha do Atlântico e foi introduzida em 1942, os criptoanalistas de Bletchley Park, a chamaram de Shark-key (Chave-tubarão). Seu código permaneceu sem ser quebrado por nove meses, até outubro de 1942, quando livros de códigos novos foram capturados. Os operadores da Enigma recebiam livros códigos mensalmente com a chave para cada dia.

Figura 15: Enigma M4
(Fonte: http://www.jproc.ca/crypto/enigma.html)

1.4.3 – Criptoanalistas de Bletchley Park

"A enigma é uma máquina de cifragem muito complicada e decifrá-la exigiu um imerso poder intelectual" Sighn (2007).

Quando a Primeira Guerra acabou, os criptoanalistas britânicos continuaram monitorando as comunicações alemãs. Mas, em 1926, com a entrada em funcionamento da máquina Enigma, começaram a surgir mensagens impossíveis de serem decifradas, tanto por eles quanto pelos norte-americanos e pelos franceses. O único País que insistiu nas tentativas de decifragem foi a Polônia.

O matemático Marian Rejewski teve um papel fundamental na insistência polonesa, pois ele conseguiu mostrar que a Enigma possuía falhas e esse foi o ponto de partida de estudo dos criptoanalistas de Bletchley Park. Foi quando apareceu a figura do matemático inglês Alan Turing (1912-1954), responsável por identificar a maior fraqueza da máquina Enigma.

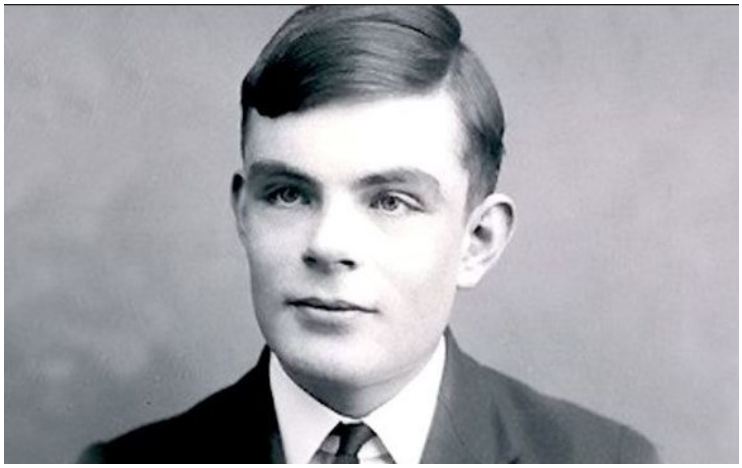


Figura 16: Alan Turing
(Fonte: http://horizontes.sbc.org.br/index.php/2016/11/22/alan-turing-e-a-enigma/)

Turing juntamente com o time de Bletchley Park desenvolveu a máquina Colossus, para decifrar a cifra Lorenz, uma cifra utilizada pelo alto comando alemã.

As informações obtidas em Bletchley Park eram passadas apenas as mais altas patentes militares e membros selecionados do gabinete de guerra. O primeiro ministro britânico Winston Churchill chegou a chamar a grande e heterogênea equipe de "os gansos que botam ovos de ouro e jamais grasnam"(Singh, 2007).

Com as informações privilegiadas, os aliados tinham que manter o segredo sobre a

"quebra" da cifra da Enigma, pois o fator surpresa era singular nas batalhas, pois se os alemãs desconfiassem que suas comunicações não eram mais seguras, as Enigmas seriam reforçadas e Bletchley Park estaria de volta ao ponto de partida. Explica Sighn (2007):

> Como no caso do telegrama Zimmermann, os britânicos tomaram várias precauções para evitar despertar suspeitas, tais como afundar a embarcação alemã depois de roubar seus livros de códigos. Isso faria […] acreditar que o material cifrado fora para o fundo do oceano e não caíra em mãos aliadas.

O segredo em torno de Bletchley Park terminou em 1974 com o lançamento do livro *The Ultra Secret,* de F. W. Winterbotham. Aqueles que tinham contribuído para o esforço de guerra podiam receber então o reconhecimento merecido. Entre eles, Marian Rejewski, que havia sido "relegado ao trabalho de lidar com cifras rotineiras, numa pequena unidade do serviço de informações" (Singh, 2007).

Singh (2017) relata que não ficou claro até hoje porque Rejewski não fora convidado a fazer parte da equipe de criptoanalistas de Bletchley Park, "mas, em consequência disso, ele ignorava completamente as atividades da Escola de Códigos e Cifras do Governo", não sabendo até a publicação do livro *The Ultra Secret* que "suas ideias tinham fornecido o fundamento para a decifragem rotineira da Enigma durante a guerra.

Entre os que não sobreviveram ao fim do segredo, estão Alastair Denniston, o primeiro diretor de Bletchley Park, e Alan Turing.

CAPÍTULO 2

Conceitos básicos de Teoria dos Números

Na teoria dos números os conceitos e as técnicas são muito abstratos, e geralmente é difícil entendê-los intuitivamente sem exemplos. Por conseguinte, este capítulo conterá diversos exemplos, cada um dos quais destacados em uma caixa sombreada. Os conceitos e técnicas abordados neste capítulo são fundamentais para o entendimento dos próximos capítulos. Este capítulo oferece uma visão geral desses conceitos.

2.1 – Divisibilidade e o algoritmo da divisão

Divisibilidade

"Dizemos que um b diferente de zero **divide** a se $a = mb$ para algum m, onde a, b e m são inteiros. Os seja, b divide a se não houver resto na divisão. A notação $b \mid a$ normalmente é usada para indicar que $b \mid a$. Além disso, se $b \mid a$, afirmamos que b é um **divisor** de a."(Stallings, 2015)

Os divisores de 24 são 1, 2, 3, 4, 6, 8, 12 e 24.

Vejamos algumas das propriedades de divisibilidade:

Propriedade 1: Se $a \mid 1$, então $a = \pm 1$.

Propriedade 2: Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

Propriedade 3: Qualquer $b \neq 0$ divide 0.

Propriedade 4: Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Prova: Por suposição $b = aq$ e $c = bp$. Logo, $c = (aq)p = a(qp)$. Então $a \mid c$

5 | 55 e 55 | 165 = 5 | 165

Propriedade 5: Se $b \mid g$ e $b \mid h$, então b $\mid (mg + nh)$ para inteiros quaisquer m e n.

Prova: Observe que:

- Se $b \mid g$, então g tem a forma $g = bg_1$ para algum inteiro g_1.
- Se $b \mid h$, então h tem a forma $h = bh_1$ para algum inteiro h_1.

Assim,

$$mg + nh = mbg_1 + nbh_1 = b(mg_1 + nh_1)$$

e portanto, b divide $mg + ng$.

$a = 6$; $b = 12$; $c = 54$; $d = 3$; $e = 2$
6 | 12 e 6 | 54.
Para mostrar 6 | (3 × 12 + 2 × 54),
temos (3 × 12 + 2 × 54) = 6 (3 × 2 + 2 × 9),
e é óbvio que 6 | (6 (3 × 2 + 2 × 9)).

Algoritmo da divisão

Dado qualquer inteiro positivo *n* e qualquer inteiro não negativo *a*, se dividirmos *a* por *n,* obteremos um quociente inteiro *q* e um resto inteiro *r* que obedecem a seguinte relação:

$$a = qn + r \quad 0 \leq r < n;\ q = [a / n] \qquad \textbf{(2.1)}$$

onde [x] é o maior inteiro menor ou igual a x. A equação 2.1 é chamada de algoritmo da divisão.[2]

A figura 17 ilustra que, para *a e n* positivos, conseguimos sempre encontrar *q* e *r* que satisfazem a relação anterior. Representando os inteiros na linha de números; *a* cairá em algum ponto nessa linha. Começando em 0 prossiga para *n, 2n,* até *qn*, de modo que $qn \leq a$ e $(q + 1)n > a$.

A distância de *qn* e *a* é *r*, e encontramos os valores únicos de *q* e *r*. Chamamos de resíduo o resto *r*.

$a = 13$; $n = 8$; $13 = 1 \times 8 + 5$; $r = 5$ $q = 1$
$a = -13$; $n = 8$; $-13 = (-2) \times 8 + 3$; $r = 3$ $q = -2$
A Figura 17b contém outro exemplo

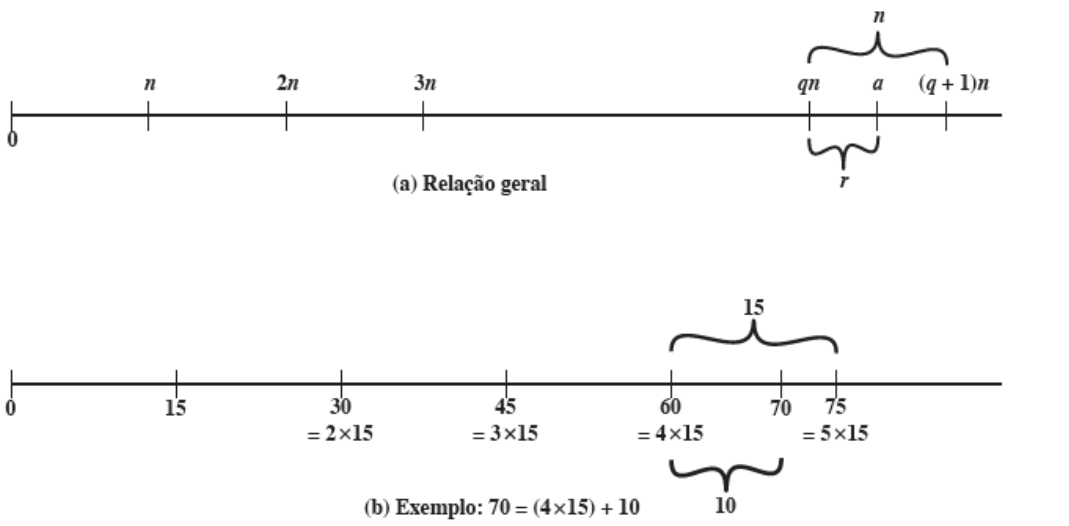


Figura 17: A relacao a = qn + r; 0 ≤ r < n.
(Fonte: Stallings, 2015, p. 66)

2 "A equação expressa um teorema, em vez de um algoritmo; mas, por tradição, este é conhecido como algoritmo da divisão." (Stallings, 2015)

2.2 – Algoritmo de Euclides

Conforme explica Stallings (2015), o algoritmo de Euclides é uma das técnicas mais básicas da teoria dos números, e com este algoritmo conseguimos encontrar o máximo divisor comum de dois inteiros positivos de forma mais simples. Primeiro precisamos de uma definição simples: "dois inteiros são relativamente primos se seu único fator comum inteiro e positivo for 1." (Stallings, 2015)

Máximo divisor comum

"Lembre-se de que *b* diferente de zero é definido como um divisor de *a* se $a = mb$ para algum *m*, onde *a, b* e *m* são inteiros. Usaremos a notação mdc(*a,b*) para significar o **máximo divisor comum** de *a* e *b*, que é o maior inteiro que divide tanto *a* quanto *b*. Também indicamos mdc(0,0) = 0." (Stallings, 2015)

De modo formal, o inteiro positivo *c* é considerado o máximo divisor comum de *a* e *b* se *1*. *c* é um divisor de *a* e de *b;*

2. Qualquer divisor de *a* e *b* é um divisor de *c*.

Uma definição equivalente é a seguinte:

$$\text{mdc}(a,b) = \text{máx}[k, \text{ tal que } k \mid a \text{ e } k \mid b]$$

Temos que ter o máximo divisor comum positivo, mdc(*a,b*) = mdc(*a,-b*) = mdc(*-a,b*) = mdc(*-a,-b*). Geralmente, mdc(*a,b*) = mdc(|*a*|,|*b*|).

mdc(80,15) = mdc(80,-15) = 5

Porém, como todos os inteiros diferentes de zero dividem 0, temos que mdc(*a,*0) = |*a*|.

Falamos que dois inteiros *a* e *b* são relativamente primos se seu único fator comum inteiro e positivo for 1. Isso é o mesmo que dizer que *a* e *b* são relativamente primos se mdc(*a,b*) = 1.

7 e 24 são relativamente primos porque os divisores positivos de 7 são 1 e 7, e os divisores positivos de 24 são 1, 3, 4, 6, 8, 12 e 24, de modo que 1 é o único inteiro nas duas listas.

Encontrando o máximo divisor comum

A descrição do algoritmo creditado a Euclides usado para achar de forma fácil o máximo divisor comum de dois inteiros. Suponhamos que dois inteiros *a* e *b,* de modo que *d* = mdc(*a,b*). Como mdc(|*a*|,|*b*|) = mdc(*a,b*), então podemos assumir que $a \geq b > 0$. Agora,

dividindo a por b e aplicando o algoritmo de divisão, podemos afirmar:

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b \qquad \textbf{(2.2)}$$

"Acontece que, se $r_1 = 0$, então $b \mid a$ e $d = \text{mdc}(a,b) = b$. Mas, se $r_1 \neq 0$, podemos afirmar que $d \mid r_1$. Isto é, por conta das propriedades básicas de divisibilidade: as relações $d \mid a$ e $d \mid b$, juntas, implicam que $d \mid (a - q_1 b)$, o mesmo que $d \mid r_1$. Antes de proceder com o algoritmo de Euclides, precisamos responder à pergunta: Qual é o mdc (b, r_1)? Sabemos que $d \mid b$ e $d \mid r_1$. Agora, pegue qualquer inteiro arbitrário c que divide tanto b quanto r_1.

Assim, $c \mid (q_1 b + r_1) = a$. Visto que c divide tanto a quanto b, devemos ter $c \leq d$, que é o máximo divisor comum de a e b. Portanto, $d = \text{mdc}(b, r_1)$." (Stallings, 2015)

Retornando à equação 2.2. Suponha que $r_1 \neq 0$. Visto que $b > r_1$, podemos dividir b por r_1 e aplicar o algoritmo de divisão para obter:

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

Como antes, se $r_2 = 0$, então $d = r_1$, e, se $r_2 \neq 0$, então $d = \text{mdc}(r_1, r_2)$. Esse processo de divisão continua até que apareça algum resto zero, digamos, na fase $(n+1)$, onde r_{n-1} é dividido por r_n. O resultado é o seguinte sistema de equações:

$$\left.\begin{array}{ll} a = q_1 b + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \bullet & \bullet \\ \bullet & \bullet \\ \bullet & \bullet \\ r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + 0 & 0 < r_3 < r_2 \\ d = \text{mdc}(a, b) = r_n & \end{array}\right\} \qquad \textbf{(2.3)}$$

A cada iteração, temos $d = \text{mdc}(r_t, r_{t+1})$, até que finalmente $d = \text{mdc}(r_n, 0) = r_n$. Com isto acharemos o máximo divisor comum de dois inteiros aplicando de forma repetida o algoritmo da divisão. O esquema descrito é conhecido como o algoritmo de Euclides.

Faremos agora um exemplo com um número grande para mostrar o poder desse algoritmo:

Para encontrar d = mdc(a, b) = mdc(1160718174, 316258250)		
$a = q_1 b + r_1$	1160718174 = 3 × 316258250 + 211943424	d = mdc(316258250, 211943424)
$b = q_2 r_1 + r_2$	316258250 = 1 × 211943424 + 104314826	d = mdc(211943424, 104314826)
$r_1 = q_3 r_2 + r_3$	211943424 = 2 × 104314826 + 3313772	d = mdc(104314826, 3313772)
$r_2 = q_4 r_3 + r_4$	104314826 = 31 × 3313772 + 1587894	d = mdc(3313772, 1587894)
$r_3 = q_5 r_4 + r_5$	3313772 = 2 × 1587894 + 137984	d = mdc(1587894, 137984)
$r_4 = q_6 r_5 + r_6$	1587894 = 11 × 137984 + 70070	d = mdc(137984, 70070)
$r_5 = q_7 r_6 + r_7$	137984 = 1 × 70070 + 67914	d = mdc(70070, 67914)
$r_6 = q_8 r_7 + r_8$	70070 = 1 × 67914 + 2156	d = mdc(67914, 2156)
$r_7 = q_9 r_8 + r_9$	67914 = 31 × 2516 + 1078	d = mdc(2156, 1078)
$r_8 = q_{10} r_9 + r_{10}$	2156 = 2 × 1078 + 0	d = mdc(1078, 0) = 1078
Portanto, d = mdc(1160718174, 316258250) = 1078		

(Fonte: Stallings, 2015, p. 68)

Observe que no exemplo, começamos dividindo 1160718174 por 316258250, o que resulta em 3 com um resto de 211943424. Depois, tomamos 316258250 e o dividimos por 211943424. Continuamos com esse processo até chegarmos a um resto 0, produzindo 1078 como resultado.

2.3 – Aritmética Modular

Módulo

Sendo a um inteiro, e n, um número positivo, definimos a mod n para ser o resto quando a é dividido por n. O inteiro n é chamado de **módulo**. Com isto, para qualquer inteiro a, sempre podemos reescrever a Equação 2.1 da seguinte forma:

$$a = qn + r \quad 0 \leq r < n; q = [a/n]$$

$$a = [a/n] \times n + (a \bmod n)$$

13 mod 9 = 4; - 13 mod 7 = 5

Dois inteiros a e b são considerados **congruentes módulo *n***, se (a mod n) = (b mod n). Isso é escrito como $a \equiv b \pmod{n}$.

$47 \equiv 2 \pmod{15}$; $83 \equiv -7 \pmod{10}$

Note que, se $a \equiv 0 \pmod{n}$, então $n \mid a$.

Propriedades de congruências

Temos por propriedades de congruências:

1. $a \equiv b \pmod{n}$, se $n \mid (a - b)$.
2. $a \equiv b \pmod{n}$ implica $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ implica $a \equiv c \pmod{n}$

$17 \equiv 2 \pmod{5}$ porque $17 - 2 = 15 = 5 \times 3$

$-13 \equiv 5 \pmod{6}$ porque $-13 - 5 = -18 = 6 \times (-2)$

$36 \equiv 0 \pmod{9}$ porque $36 - 0 = 36 = 9 \times 3$

Operações de aritmética modular

Veja que, por definição (Figura 17), o operador (mod n) mapeia todos os inteiros para o conjunto $\{0, 1, \ldots, (n - 1)\}$. Isso sugere a pergunta: podemos realizar operações aritméticas dentro dos limites desse conjunto? A resposta é que podemos; e aritmética modular é como é conhecida essa técnica.

As propriedades da aritmética modular são:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Exemplos:

$13 \bmod 5 = 3$; $19 \bmod 5 = 4$

$[(13 \bmod 5) + (19 \bmod 5)] \bmod 5 = 7 \bmod 5 = 2$

$(13 + 19) \bmod 8 = 32 \bmod 5 = 2$

$[(13 \bmod 5) - (19 \bmod 5)] \bmod 5 = -1 \bmod 5 = 4$

$(13 - 19) \bmod 5 = -4 \bmod 5 = 1$

$[(13 \bmod 5) \times (19 \bmod 5)] \bmod 5 = 12 \bmod 5 = 2$

$(13 \times 19) \bmod 5 = 247 \bmod 5 = 2$

Já na exponenciação realizamos da mesma forma que na aritmética comum.

Para encontrar $13^7 \bmod 11$, podemos proceder da seguinte forma:

$13^2 = 169 \equiv 4 \pmod{11}$
$13^4 = (13^2)^2 \equiv 4^2 \equiv 5 \pmod{11}$
$13^7 \equiv 13 \times 4 \times 5 \equiv 260 \equiv 7 \pmod{11}$

Com isto é possível verificar que as regras da aritmética comum são as mesmas que as usadas na aritmética modular.

2.4 – Números primos

Para Stallings (2015), o estudo dos números primos é de fundamental importância no estudo da teoria dos números. Na realidade, livros inteiros foram escritos sobre o assunto.

Um inteiro $p > 1$ é um número primo se, e somente se, seus únicos divisores forem ± 1 e $\pm p$. Os **números primos** desempenham um papel importante na teoria dos números.

2.4.1 – Teorema Fundamental da Aritmética

Qualquer inteiro $a > 1$ pode ser fatorado de uma forma exclusiva como

$$a = p_1^{a1} \times p_2^{a2} \times \ldots \times p_t^{at}$$

onde $p_1 < p_2 < \ldots < p_t$ são números primos e cada a_t é um inteiro positivo. Isso é conhecido como teorema fundamental da aritmética.

$77 = 7 \times 11$
$1300 = 2^2 \times 5^2 \times 13$
$29645 = 5 \times 7^2 \times 11^2$

2.5 – Teoremas de Fermat e Euler

Segue abaixo dois teoremas bastante importantes no estudo da criptografia de chave pública.

Teorema de Fermat[3]

O teorema de Fermat afirma o seguinte: se p é primo e a é um inteiro positivo não divisível por p, então

$$a^{p-1} = 1 \pmod{p}.$$

$a = 5, p = 17$
$5^2 = 25 \equiv 8 \pmod{17}$

3 Este, às vezes, é conhecido como pequeno Teorema de Fermat.

$5^4 = 64 \equiv 13 (\text{mod } 17)$
$5^8 = 169 \equiv 16 (\text{mod } 17)$
$5^{16} = 256 \equiv 1 (\text{mod } 17)$
$a^{p-1} \equiv 5^{16} = 5^{16} \equiv 1 (\text{mod } 17)$

Outra forma equivalente e de grande utilidade do teorema de Fermat é: se p é primo e a um inteiro positivo, então

$$a^p = a \ (\text{mod } p)$$

$p = 5, a = 3$	$a^p = 3^5 = 243 \ ; \ 3(\text{mod } 5) = a(\text{mod } p)$
$p = 5, a = 10$	$a^p = 10^5 = 100000 \ ; \ 10(\text{mod } 5) \ ; \ 0(\text{mod } 5) = a(\text{mod } p)$

Teorema de Euler

Uma função de grande importância na teoria dos números é a função totiente de Euler, a qual será apresentada antes do teorema de Euler. Essa função "é escrita como $\varphi(n)$, definida como o número de inteiros positivos menores que n e relativamente primos de n. Por convenção, $\varphi(1) = 1$." (Stallings, 2015)

DETERMINE $\varphi(17)$ e $\varphi(25)$.
Como 17 é primo, todos os inteiros positivos de 1 até 16 são relativamente primos de 17. Assim, $\varphi(17) = 16$.
Para determinar $\varphi(25)$, listamos todos os inteiros positivos menores que 25 que são relativamente primos dele:

1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14,
16, 17, 18, 19, 21, 22, 23, 24.

Existem 20 numeros na lista, de modo que $\varphi(25) = 20$.

Na tabela 1 temos uma lista dos 30 primeiros valores de $\varphi(n)$. Observe que $\varphi(1)$ não tem significado, porém seu valor é definido como 1.

Portanto ficar evidente que se p é primo, temos:

$$\varphi(p) = p - 1$$

Supondo que tenhamos dois números primos p e q, com p diferente de q. Conseguiremos mostrar que, para $n = pq$,

$$\varphi(n) = \varphi(pq) = \varphi(p) \times \varphi(q) = (p - 1) \times (q - 1)$$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Tabela 1: Alguns valores da funcão totiente de euler φ(n).
(Fonte: Stallings, 2015, p. 187)

Teorema de Euler: Dados inteiros a, n primos entre si, com $n > 1$, temos que:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$a = 3$; $n = 10$; $\varphi(10) = 4$	$a^{\varphi(n)}(n) = 3^4 = 81 = 1 \pmod{10} = 1 \pmod{n}$
$a = 2$; $n = 11$; $\varphi(11) = 10$	$a^{\varphi(n)}(n) = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod{n}$

Uma outra forma útil de representar o teorema de Euler é:

$$a^{\varphi(n)+1} \equiv a \pmod{n}$$

CAPÍTULO 3
Criptografia ou encriptação Simétrica

Conforme explica Stallings (2015), a encriptação simétrica é também conhecida como encriptação convencional ou encriptação de chave única, ela foi por muito tempo o único tipo em uso antes do desenvolvimento da encriptação por chave pública na década de 1970. Esse continua sendo de longe o mais usado dos dois tipos de encriptação.

3.1 – Modelo de Cifra Simétrica

Segue abaixo um esquema de encriptação simétrica com cinco itens, conforme mostra Stallings (2015):

- **Texto claro:** mensagem ou dados originais onde é possível a compreensão e que servem como entrada do algoritmo de encriptação.
- **Algoritmo de encriptação:** é o que realiza as diversas substituições e transformações no texto claro.
- **Chave secreta:** também é uma entrada para o algoritmo de encriptação. O valor da chave é independente do texto claro e do algoritmo. O algoritmo irá produzir uma saída diferente, dependendo da chave usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.
- **Texto cifrado:** é a mensagem incompreensível, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.
- **Algoritmo de decriptação:** é o algoritmo de codificação executado de modo inverso. Ele apanha o texto cifrado e a chave secreta e produz o texto original.

Ainda segundo Stallings (2015), existem dois requisitos para o uso seguro da encriptação simétrica:

1. O que se precisa é um algoritmo de encriptação forte. Temos que ter no mínimo um algoritmo que qualquer oponente que conheça o algoritmo e tenha acesso a um ou mais textos cifrados não seja capaz de decifrar o texto cifrado ou descobrir a chave. Esse requisito normalmente é indicado de maneira mais forte: o oponente deverá ser incapaz de decriptar o texto cifrado ou descobrir a chave, mesmo que possua diversos

textos cifrados com seus respectivos textos claros.

2. A obtenção dos códigos das chaves secretas entre o emissor e o receptor devem ser obtidas de forma segura e protegida. Pois se alguém conseguir descobrir a chave e o algoritmo, toda a comunicação usando essa chave poderá ser lida.

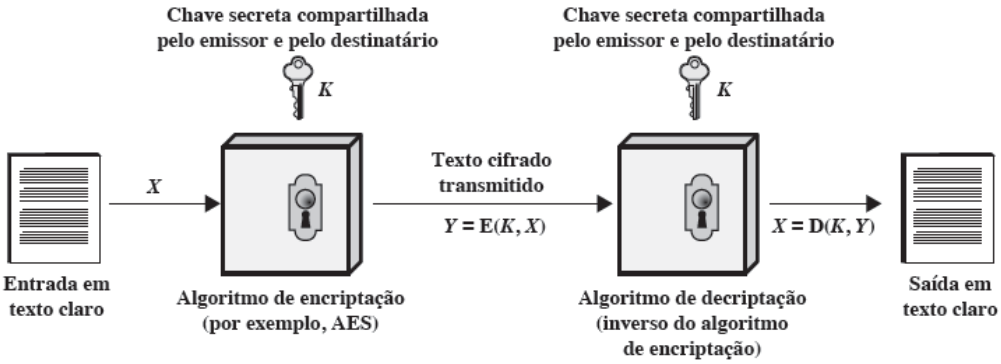


Figura 18: Modelo simplificado da encriptação simétrica
(Fonte: Stallings, 2015, p. 21)

Stallings (2015), explica que não é preciso manter o algoritmo secreto, mas sim a chave secreta. Essa característica da encriptação simétrica é o que a torna viável para uso generalizado. Stallings (2015) afirma: "O fato de que o algoritmo não precisa ser mantido secreto significa que os fabricantes podem desenvolver, e realmente têm desenvolvido, implementações de chip de baixo custo com algoritmos de encriptação de dados. Esse chips são encontrados com facilidade e estão incorporados em diversos produtos." Sendo assim, manter o sigilo da chave é o principal problema no uso da criptografia simétrica.

3.2 – Formas de ataque a um sistema de encriptação

Geralmente, o ataque a um sistema de encriptação tem o objetivo de recuperar a chave em uso, em vez de simplesmente recuperar o texto claro a partir de um único texto cifrado.

Para Stallings (2015), existem duas técnicas gerais para o ataque a um esquema de encriptação convencional, a **criptoanálise** e o **ataque por força bruta**.

Assim Stallings (2015) explica as duas formas de ataque:

- **Criptoanálise:** é o tipo de ataque que utiliza a natureza do algoritmo, e talvez de mais algum conhecimento das características comuns ao texto claro, ou ainda de algumas amostras de pares de texto claro-texto cifrado. Esse é o tipo de ataque que visa explora as especificações do algoritmo para tentar deduzir um texto claro específico ou a chave utilizada.
- **Ataque por força bruta:** é o tipo de ataque onde são testadas todas as chaves

possíveis em um trecho do texto cifrado, até obter uma tradução comprensível para o texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentadas para então se obter sucesso.

Um efeito catastrófico é se algum dos tipos de ataque desses tiver sucesso na dedução da chave todas as mensagens futuras e passadas, encriptadas com essa chave, ficam comprometidas.

3.3 – Técnicas de encriptação

Nesta seção examinaremos algumas técnicas de encriptação clássicas:

3.3.1 – Técnicas de substituição

Para Stallings (2015), uma técnica de substituição é aquela em que as letras do texto claro são substituídas por outras letras, números ou símbolos.[4]

3.3.1.1 – Cifra de César

Conforme explica Stallings (2015), a cifra de substituição que foi elaborado por Júlio Cesar é a mais simples e a mais antiga em uso. A cifra de César envolve substituir cada letra do alfabeto por aquela que fica três posições adiante.

Por exemplo:

claro: a vitória será nossa

cifra: D YLWRULD VHUD QRVVD

Observe que o alfabeto recomeça no final, de modo que a letra Z é a A. Podemos definir a transformação listando todas as alternativas, da seguinte forma:

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

Atribuindo um valor numérico a cada letra:

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

4 Texto claro está sempre em minúsculas; texto cifrado está em maiúsculas.

Observe que o algoritmo é ser expresso da forma a seguir. Para cada letra em texto claro *p*, substitua-a pela letra do texto cifrado *C*:[5]

$$C = E(3,p) = (p + 3) \bmod 26$$

Um deslocamento pode ser de qualquer magnitude, de modo que o algoritmo de César geral é

$$C = E(k,p) = (p + k) \bmod 26$$

onde *k* assume um valor no intervalo de 1 a 25. O algoritmo de decriptação é simplesmente

$$p = D(k,C) = (C - k) \bmod 26$$

Se for conhecido que determinado texto cifrado é uma cifra de César, então uma criptoanálise pela força bruta será facilmente realizada. Basta experimentar todas as 25 chaves possíveis.

3.3.1.2 – Cifras monoalfabéticas

Como visto no subitem anterior, a cifra de César não tem tanta segurança, pois possui apenas 25 chaves possíveis. Para conseguir um aumento considerável no espaço de chaves permitir-se uma substituição arbitrária. Conforme sugere Stallings (2015), iremos definir o termo *permutação.* "Uma permutação é um conjunto finito de elementos *S* em uma sequência ordenada de todos os elementos de *S*, com cada um aparecendo exatamente uma vez. Por exemplo, se *S* = {a, b, c}, existem seis permutações de *S"* (Stallings, 2015)*:*

abc, acb, bac, bca, cab, cba.

Em geral, existem *n*! permutações de um conjunto de *n* elementos, pois o primeiro deles pode ser escolhido de *n* maneiras, o segundo, de *n* – 1 maneiras, o terceiro, de *n* – 2 maneiras, e assim por diante.

Lembrando da atribuição para a cifra de César:

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

Se, em vez disso, a linha "cifra" puder ser qualquer permutação dos 26 caracteres alfabéticos, então haverá 26! ou mais do que 4 x 10^{26} chaves possíveis. Essa técnica é conhecida como **cifra por substituição monoalfabética**, pois um único alfabeto de cifra é utilizado por mensagem.

---

5 Definimos *a* mod *n* como sendo o resto quando *a* é dividido por *n*. Por exemplo, 13 mod 7 = 6

Stallings (2015) explica que as cifras monoalfabéticas são fáceis de se quebrar porque reflete os dados de frequência do alfabeto original.

3.3.1.3 – Cifras polialfabéticas

Stallings (2015) afirma que uma outra forma de melhorar a técnica monoalfabética simples é usar diferentes substituições monoalfabéticas enquanto se prossegue pela mensagem de texto claro. O nome que se dar para essa técnica é **cifra por substituição polialfabética**. Para Stallings (2015), essas técnicas têm as seguintes características em comum:

1. Um conjunto de regras de substituição monoalfabéticas é utilizado.
2. Uma chave define qual regra em particular é escolhida para determinada transformação.

Uma das mais simples e mais conhecida cifras polialfabéticas é a *cifra de Vigenère*.

3.3.2 – Técnicas de transposição

A transposição, consiste em trocar a posição das letras da mensagem original, promovendo uma permutação das letras segundo um algoritmo e uma chave bem determinadas. Uma técnica de transposição muito conhecida é o bastão de Licurgo, conforme visto na seção 1.1.4.

Conforme explica Stallings (2015), a cifra mais simples desse tipo é conhecida como **cerca de trilho** que consiste em escrever o texto claro em uma sequência de diagonais, e depois lido como uma sequência de linhas. Por exemplo, para cifrar a mensagem "*matemática aplicada*" com uma cerca de trilho de profundidade 2, escrevemos o seguinte:

m t m t c a l c d
a e a i a p i a a

A mensagem encriptada é

MTMTCALCDAEAIAPIAA

Para Stallings (2015), esse tipo de cifra seria fácil de ser criptanalisada. Um forma mais difícil seria escrever a mensagem em um retângulo, linha por linha, e a ler coluna por coluna, mas permutar a ordem destas. Nesse caso a chave para o algoritmo seria a ordem das colunas. Por exemplo,

Chave:	4 3 1 2 5 6 7
Texto claro:	a n i m a i s
	e s t a r a m
	a n d a n d o
Texto cifrado:	ITDMAANSNAEAARNIADSMO

Assim, neste exemplo, a chave é 431567. Para codificar iremos iniciar com a coluna rotulada com 1, neste caso, a coluna 3. Escreva todas as letras dessa coluna. Prossiga para a coluna 4, que é rotulada com 2, depois para a coluna 2, então para a coluna 1, por fim a 5, 6 e 7.

3.3.3 – Máquinas de rotor

As máquinas de rotor[6] era a classe de sistemas que tem a aplicação mais importante do princípio de múltiplas etapas de codificação.

Na figura 19 é ilustrado o princípio básico da máquina de rotor. Conforme explica Stallings (2015), a máquina de rotor é composta por um conjunto de cilindros que tem rotação independente, e através dos quais pulsos elétricos podem fluir. Observe que cilindro tem 26 pinos de entrada e 26 pinos de saída, com fiação interna que conecta cada pino de entrada a um único pino de saída. Para efeito de entendimento, iremos mostrar somente três das conexões internas em cada cilindro.

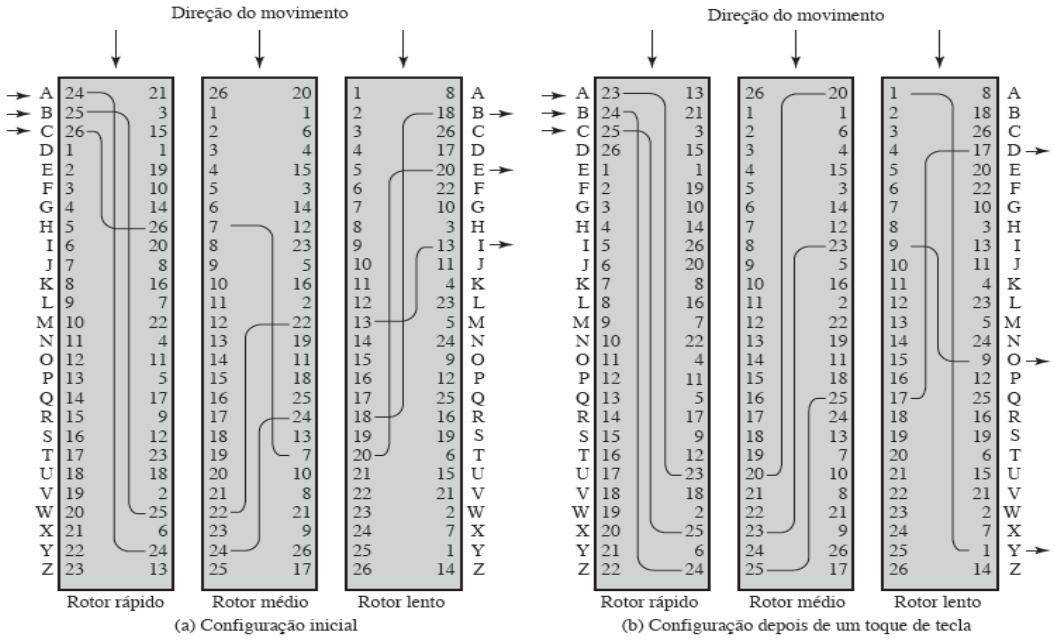


Figura 19: Máquina de três rotores com fiação representada por contatos numerados. (Fonte: Stallings, 2015, p. 38)

6 "Máquinas baseadas no princípio de rotor foram usadas para Alemanha (Enigma) e pelo Japão (Purple) na Segunda Guerra Mundial. A quebra desses dois códigos pelos Aliados foi um fator significativo para o resultado da Guerra."(Stallings,2015)

Se relacionarmos um pino de entrada e saída a apenas uma letra do alfabeto, uma substituição monoalfabética é definida em um único cilindro. Por exemplo, na Figura 19, se um operador pressionar uma tecla para a letra B, um sinal elétrico é aplicado ao segundo pino do primeiro cilindro e flui pela conexão interna para o vigésimo terceiro pino de saída.

Considere uma máquina com um único cilindro conforme sugere Stallings (2015), após pressionar cada tecla de entrada, uma posição é girada no cilindro fazendo com que conexões internas se desloquem de acordo. Com isto, uma cifra de substituição monoalfabética diferente é definida. Após pressionar 26 letras de texto claro, o cilindro giraria 26 vezes, ou seja, voltaria a posição inicial. Assim, conseguimos um algoritmo de substituição polialfabética com um período de 26. É óbvio que um sistema com um único cilindro é simples, além de ser fácil descobrir a chave. O poder da máquina de rotor está no uso de múltiplos cilindros, em que os pinos de saída de um cilindro são conectados aos de entrada do seguinte. A Figura 19 mostra um sistema de três cilindros. A metade esquerda da figura mostra uma posição em que a entrada do operador para o primeiro pino (letra b em texto claro) é direcionada pelos três cilindros para aparecer na saída do segundo pino (letra I em texto cifrado).

Stallings (2015) afirma que: “com múltiplos cilindros, aquele mais próximo da entrada do operador gira uma posição de pino a cada toque de tecla. A metade direita da Figura 19 mostra a configuração do sistema depois de um único toque de tecla. Para cada rotação completa do cilindro interno, o do meio gira uma posição de pino. O resultado é que existem 26 x 26 x 26 = 17.576 alfabetos de substituição diferentes usados antes que o sistema repita. O acréscimo de quarto e quinto rotores resulta em períodos de 456.976 e 11.881.376 letras, rescpectivamente. Assim, determinada configuração de uma máquina de 5 rotores é equivalente a uma cifra de Vigenère com um tamanho de chave de 11.881.376.”

Para Stallings (2015), a máquina de rotor tem um significado bastante importante, pois ela direciona para a cifra mais usada de todos os tempos: Data Encryption Standard (DES).

3.3.4 – Esteganografia

Uma mensagem em texto claro pode estar oculta de duas maneiras, segundo explica Stallings (2015), a **esteganografia** tem como método esconder a existência da mensagem e a criptografia tem como métodos tornar a mensagem ininteligível a estranhos por meio de várias transformações do texto.

“Uma forma simples de esteganografia, mas demorada de se construir, é aquela em que um arranjo de palavras e letras dentro de um texto aparentemente inofensivo soletra a mensagem real. Por exemplo, a sequência de primeiras letras de cada palavra da mensagem geral soletra a mensagem escondida.” (Stallings, 2015)

3.4 – Data Encryption Standard (DES)

O Data Encryption Standard – DES – é um padrão criptográfico criado em 1977 através de uma licitação aberta pela antiga Agência de Segurança Americana – National Security Agency (NSA). O único concorrente foi o algoritmo LUCIFER da International Business Machine – IBM, conforme Schneier (1994). Após algumas modificações no seu código original, chegou-se ao padrão de 64 bits de leitura, aplicando uma chave com 56 bits à mensagem.

Stallings (2015), explica que até o uso do advanced encryption standard (AES), em 2001, o esquems de codificação mais utilizado era o data encryption standard (DES). Pontua que o DES foi adotado no ano de 1977 pelo National Bureau of Standards, agora National Institute of Standards and Technology (NIST), como Federal Information Processing Standard $ (FIPS PUB 46). O algoritmo é conhecido como data encryption algorithm (DEA). O DES funciona do seguinte moso: os dados são codificados em blocos de 64 bits usando uma chave de 56 bits. O algoritmo transforma a entrada de 64 bits em uma série de etapas para a saída de 64 bits. As mesmas etapas, com a chave, são empregadas para reverter a codificação.

Passado anos, o algoritmo de decodificação simétrica dominante foi o DES, especialmente em aplicações financeiras. O DES foi ganhando espaço cada vez mais e em 1994 o NIST reafirmou o DES para uso federal por outros cinco anos, o NIST recomendou o uso do DES para aplicações que não tenham informações de proteção ou confidenciais. Em 1999, o NIST emitiu uma nova versão do seu padrão (FIPS PUB 46-3), que indicava que o DES deveria ser utilizado apenas para sistemas legados, e que o triple DES (que basicamente envolve repetir o algoritmo DES três vezes sobre o texto claro com duas ou três chaves diferentes para produzir o texto cifrado) fosse empregado.

3.4.1 – Encriptação do Data Encryption Standard (DES)

Iremos apresentar esse sistema de encriptação DES segundo Stallings (2015). Na figura 20 iremos apresentar uma ilustração do esquema geral. Para começarmos, introduz-se o

texto claro e a chave, que são as duas entradas necessárias em qualquer esquema de encriptação. Neste caso, o texto claro precisa ter 64 bits de extensão, e a chave tem 58 bits de extensão.[7]

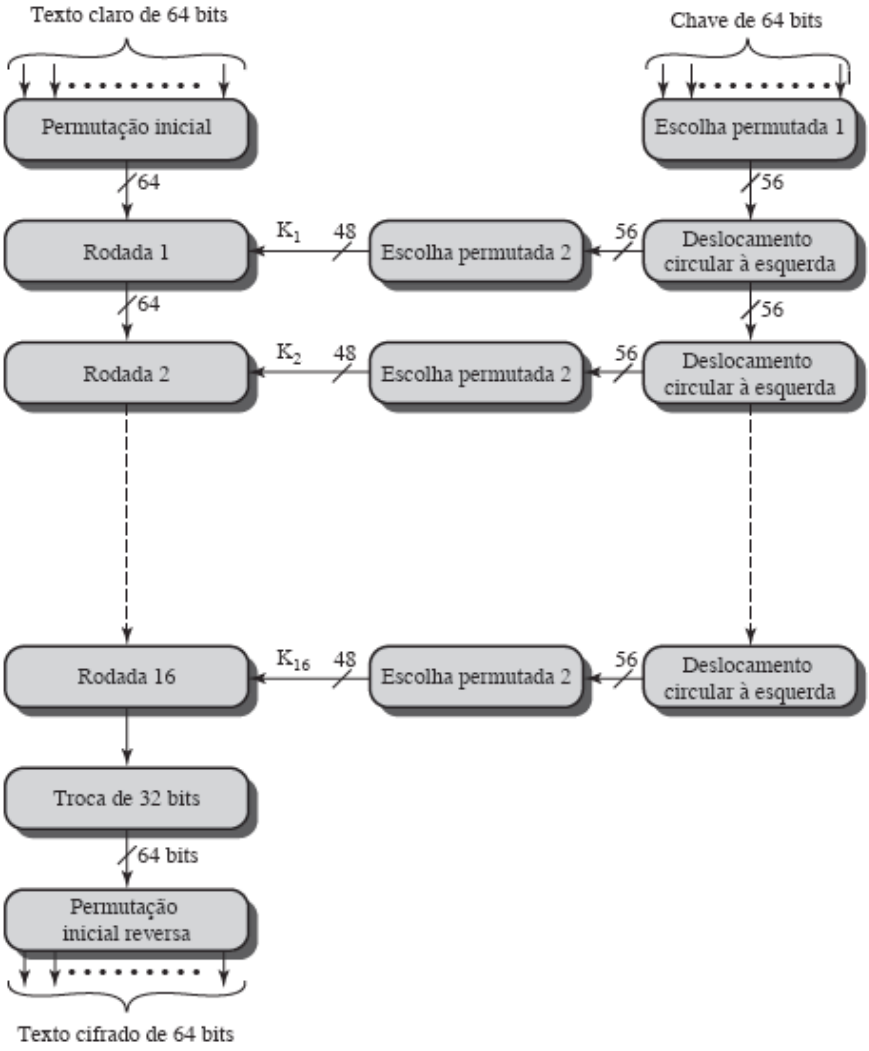


Figura 20: Representação geral do algoritmo de encriptação DES.
(Fonte: Stallings, 2015, p. 55)

"Fazendo uma verificação do lado esquerdo da figura 20, podemos ver que o processamento do texto claro prossegue em três fases. Primeiro, o texto claro de 64 bits passa por uma permutação inicial (IP, do acrônimo em inglês para *initial permutation*), que reorganiza os bits afim de produzir a *entrada permutada*. Isso é seguido por uma fase consistindo em 16 rodas da mesma função, que envolve funções de permutação e substituição. A saída da última (décima sexta) rodada baseia-se em 64 bits que são uma função do texto

7 Na realidade, a funcão espera uma chave de 64 bits como entrada. Porém, somente 56 desses bits são usados; outros 8 bits podem ser empregados como bits de paridade ou simplesmente definidos arbitrariamente.

claro de entrada e da chave. As metades esquerda e direita da saída são trocadas para produzir a pré-saída. Finalmente, a pré-saída é passada por uma permutação [IP^{-1}], que é o inverso da função de permutação inicial, a fim de produzir o texto cifrado de 64 bits." (Stallings, 2015)

Ainda segundo Stallings (2015), o lado direto da Figura 20 mostra a chave que é usada, no caso a de 56 bits. Primeiro, a chave passa por uma função de permutação. Logo após, para cada uma das 16 rodadas, uma subchave (Ki) é produzida pela combinação de um deslocamento circular a esquerda e uma permutação. Uma subchave diferente é produzida para cada função de permutação em cada rodada, por conta dos deslocamentos repetidos dos bits da chave.

3.4.2 – Decriptação do Data Encryption Standard (DES)

A decriptação de uma cifra do DES usar-se basicamente o mesmo algoritmo, apenas alterando a ordem das chaves a serem usadas. Além disso, as permutações inicial e final são invertidas.

3.4.2.1 – Exemplo do DES

Traremos nesta seção um exemplo completo de mensagem encriptada e decriptada pelo sistema criptográfico DES.

Para encriptar devemos converter uma mensagem em uma sequência de números. Para efeito de exemplificação, tomaremos a seguinte tabela de conversão:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	-	0	1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

Tabela 1

O espaço entre palavras será substituído pelo nº. 36. As conversões do texto a ser encriptado será feito sem considerar acentos e letras maiúscula. A vantagem de se utilizar dois dígitos para representar uma letra reside no fato de que tal procedimento evita a ocorrência de ambiguidades. Por exemplo, se *a* fosse convertido em 1 e *b* em 2, teríamos que *ab* seria 12, mas *l* também seria 12. Logo, não poderiamos concluir se 12 seria *ab* ou *l*.

O sistema DES consiste de um algoritmo de criptografia simétrico e polialfabético

com entrada e saída binárias. Sendo assim, uma mensagem a ser enviada deve ser convertida em uma sequência binária.

Como visto anteriormente, o algoritmo precisa de duas entradas: a mensagem a ser enviada e, portanto, codificada e a chave, que é a "senha" que irá manter a transmissão sigilosa.

Consideremos as seguintes tabelas para a construção da Criptografia DES:

59_1	51_2	43_3	35_4	27_5	19_6	11_7	03_8
57_9	49_{10}	41_{11}	33_{12}	25_{13}	17_{14}	09_{15}	01_{16}
60_{17}	52_{18}	44_{19}	36_{20}	28_{21}	20_{22}	12_{23}	04_{24}
58_{25}	50_{26}	42_{27}	34_{28}	26_{29}	18_{30}	10_{31}	02_{32}
64_{33}	56_{34}	48_{35}	40_{36}	32_{37}	24_{38}	16_{39}	08_{40}
62_{41}	54_{42}	46_{43}	38_{44}	30_{45}	22_{46}	14_{47}	06_{48}
63_{49}	55_{50}	47_{51}	39_{52}	31_{53}	23_{54}	15_{55}	07_{56}
61_{57}	53_{58}	45_{59}	37_{60}	29_{61}	21_{62}	13_{63}	05_{64}

TABELA 2: Função permutação I

16_1	32_2	8_3	24_4	64_5	48_6	56_7	40_8
15_9	31_{10}	7_{11}	23_{12}	63_{13}	47_{14}	55_{15}	39_{16}
14_{17}	30_{18}	6_{19}	22_{20}	62_{21}	46_{22}	54_{23}	38_{24}
13_{25}	29_{26}	5_{27}	21_{28}	61_{29}	45_{30}	53_{31}	37_{32}
12_{33}	28_{34}	4_{35}	20_{36}	60_{37}	44_{38}	52_{39}	36_{40}
11_{41}	27_{42}	3_{43}	19_{44}	59_{45}	43_{46}	51_{47}	35_{48}
10_{49}	26_{50}	2_{51}	18_{52}	58_{53}	42_{54}	50_{55}	34_{56}
9_{57}	25_{58}	1_{59}	17_{60}	57_{61}	41_{62}	49_{93}	33_{64}

TABELA 3: Função permutação I^{-1}

15_1	16_2	17_3	18_4	32_5	1_6
19_7	20_8	21_9	22_{10}	2_{11}	3_{12}
23_{13}	24_{14}	25_{15}	26_{16}	4_{17}	5_{18}
27_{19}	28_{20}	29_{21}	30_{22}	6_{23}	7_{24}
31_{25}	32_{26}	1_{27}	2_{28}	8_{29}	9_{30}
3_{31}	4_{32}	5_{33}	6_{34}	10_{35}	11_{36}
7_{37}	8_{38}	9_{39}	10_{40}	12_{41}	13_{42}
11_{43}	12_{44}	13_{45}	14_{46}	14_{47}	15_{48}

TABELA 4: Função expansão X

25_1	26_2	27_3	15_4	16_5	17_6	28_7	29_8
1_9	18_{10}	19_{11}	2_{12}	20_{13}	21_{14}	3_{15}	4_{16}
13_{17}	14_{18}	30_{19}	31_{20}	32_{21}	8_{22}	9_{23}	10_{24}
22_{25}	23_{26}	24_{27}	11_{28}	12_{29}	5_{30}	6_{31}	7_{32}

TABELA 5: Função permutação P

S_1

$1_{0,0}$	$12_{0,1}$	$9_{0,2}$	$5_{0,3}$	$10_{0,4}$	$15_{0,5}$	$6_{0,6}$	$2_{0,7}$	$8_{0,8}$	$11_{0,9}$	$4_{0,10}$	$14_{0,11}$	$7_{0,12}$	$12_{0,13}$	$13_{0,14}$	$2_{0,15}$
$7_{1,0}$	$10_{1,1}$	$2_{1,2}$	$6_{1,3}$	$14_{1,4}$	$3_{1,5}$	$11_{1,6}$	$9_{1,7}$	$15_{1,8}$	$0_{1,9}$	$4_{1,10}$	$12_{1,11}$	$1_{1,12}$	$5_{1,13}$	$3_{1,14}$	$13_{1,15}$
$9_{2,0}$	$0_{2,1}$	$15_{2,2}$	$1_{2,3}$	$2_{2,4}$	$10_{2,5}$	$3_{2,6}$	$11_{2,7}$	$4_{2,8}$	$5_{2,9}$	$13_{2,10}$	$6_{2,11}$	$12_{2,12}$	$7_{2,13}$	$14_{2,14}$	$8_{2,15}$
$0_{3,0}$	$9_{3,1}$	$2_{3,2}$	$12_{3,3}$	$10_{3,4}$	$8_{3,5}$	$15_{3,6}$	$3_{3,7}$	$7_{3,8}$	$11_{3,9}$	$6_{3,10}$	$1_{3,11}$	$4_{3,12}$	$13_{3,13}$	$5_{3,14}$	$14_{3,15}$

S_2

$1_{0,0}$	$10_{0,1}$	$11_{0,2}$	$7_{0,3}$	$2_{0,4}$	$14_{0,5}$	$8_{0,6}$	$15_{0,7}$	$6_{0,8}$	$9_{0,9}$	$12_{0,10}$	$0_{0,11}$	$5_{0,12}$	$3_{0,13}$	$13_{0,14}$	$4_{0,15}$
$7_{1,0}$	$10_{1,1}$	$0_{1,2}$	$5_{1,3}$	$6_{1,4}$	$1_{1,5}$	$11_{1,6}$	$2_{1,7}$	$13_{1,8}$	$12_{1,9}$	$3_{1,10}$	$8_{1,11}$	$14_{1,12}$	$9_{1,13}$	$4_{1,14}$	$15_{1,15}$
$14_{2,0}$	$5_{2,1}$	$7_{2,2}$	$11_{2,3}$	$13_{2,4}$	$0_{2,5}$	$2_{2,6}$	$8_{2,7}$	$10_{2,8}$	$1_{2,9}$	$4_{2,10}$	$15_{2,11}$	$3_{2,12}$	$6_{2,13}$	$9_{2,14}$	$12_{2,15}$
$8_{3,0}$	$2_{3,1}$	$14_{3,2}$	$9_{3,3}$	$15_{3,4}$	$5_{3,5}$	$6_{3,6}$	$11_{3,7}$	$7_{3,8}$	$12_{3,9}$	$1_{3,10}$	$0_{3,11}$	$4_{3,12}$	$14_{3,13}$	$10_{3,14}$	$3_{3,15}$

S_3

$0_{0,0}$	$9_{0,1}$	$4_{0,2}$	$2_{0,3}$	$11_{0,4}$	$7_{0,5}$	$1_{0,6}$	$12_{0,7}$	$13_{0,8}$	$6_{0,9}$	$14_{0,10}$	$8_{0,11}$	$5_{0,12}$	$3_{0,13}$	$10_{0,14}$	$15_{0,15}$
$4_{1,0}$	$2_{1,1}$	$9_{1,2}$	$3_{1,3}$	$5_{1,4}$	$13_{1,5}$	$14_{1,6}$	$6_{1,7}$	$15_{1,8}$	$11_{1,9}$	$1_{1,10}$	$7_{1,11}$	$10_{1,12}$	$12_{1,13}$	$8_{1,14}$	$0_{1,15}$
$1_{2,0}$	$12_{2,1}$	$7_{2,2}$	$10_{2,3}$	$4_{2,4}$	$15_{2,5}$	$9_{2,6}$	$6_{2,7}$	$3_{2,8}$	$8_{2,9}$	$13_{2,10}$	$11_{2,11}$	$0_{2,12}$	$14_{2,13}$	$2_{2,14}$	$5_{2,15}$
$14_{3,0}$	$5_{3,1}$	$10_{3,2}$	$2_{3,3}$	$8_{3,4}$	$9_{3,5}$	$0_{3,6}$	$11_{3,7}$	$12_{3,8}$	$3_{3,9}$	$1_{3,10}$	$6_{3,11}$	$15_{3,12}$	$7_{3,13}$	$4_{3,14}$	$13_{3,15}$

S_4

$9_{0,0}$	$14_{0,1}$	$0_{0,2}$	$13_{0,3}$	$15_{0,4}$	$3_{0,5}$	$5_{0,6}$	$8_{0,7}$	$6_{0,8}$	$11_{0,9}$	$10_{0,10}$	$7_{0,11}$	$1_{0,12}$	$4_{0,13}$	$12_{0,14}$	$2_{0,15}$
$6_{1,0}$	$8_{1,1}$	$9_{1,2}$	$3_{1,3}$	$10_{1,4}$	$15_{1,5}$	$0_{1,6}$	$5_{1,7}$	$1_{1,8}$	$13_{1,9}$	$7_{1,10}$	$4_{1,11}$	$12_{1,12}$	$2_{1,13}$	$11_{1,14}$	$14_{1,15}$
$14_{2,0}$	$0_{2,1}$	$3_{2,2}$	$6_{2,3}$	$5_{2,4}$	$12_{2,5}$	$9_{2,6}$	$15_{2,7}$	$8_{2,8}$	$7_{2,9}$	$13_{2,10}$	$10_{2,11}$	$11_{2,12}$	$1_{2,13}$	$2_{2,14}$	$4_{2,15}$
$13_{3,0}$	$3_{3,1}$	$15_{3,2}$	$0_{3,3}$	$1_{3,4}$	$9_{3,5}$	$14_{3,6}$	$8_{3,7}$	$10_{3,8}$	$4_{3,9}$	$5_{3,10}$	$6_{3,11}$	$7_{3,12}$	$12_{3,13}$	$2_{3,14}$	$11_{3,15}$

TABELA 6: Caixas S (primeira parte).

S_5

$6_{0,0}$	$8_{0,1}$	$2_{0,2}$	$12_{0,3}$	$3_{0,4}$	$7_{0,5}$	$0_{0,6}$	$15_{0,7}$	$9_{0,8}$	$1_{0,9}$	$11_{0,10}$	$4_{0,11}$	$14_{0,12}$	$5_{0,13}$	$13_{0,14}$	$10_{0,15}$
$14_{1,0}$	$12_{1,1}$	$0_{1,2}$	$2_{1,3}$	$6_{1,4}$	$11_{1,5}$	$4_{1,6}$	$8_{1,7}$	$10_{1,8}$	$9_{1,9}$	$5_{1,10}$	$15_{1,11}$	$7_{1,12}$	$3_{1,13}$	$1_{1,14}$	$13_{1,15}$
$0_{2,0}$	$4_{2,1}$	$10_{2,2}$	$5_{2,3}$	$13_{2,4}$	$6_{2,5}$	$15_{2,6}$	$2_{2,7}$	$7_{2,8}$	$12_{2,9}$	$3_{2,10}$	$14_{2,11}$	$8_{2,12}$	$11_{2,13}$	$9_{2,14}$	$15_{2,15}$
$15_{3,0}$	$11_{3,1}$	$4_{3,2}$	$8_{3,3}$	$13_{3,4}$	$6_{3,5}$	$0_{3,6}$	$12_{3,7}$	$5_{3,8}$	$14_{3,9}$	$2_{3,10}$	$9_{3,11}$	$13_{3,12}$	$3_{3,13}$	$10_{3,14}$	$7_{3,15}$

S_6

$7_{0,0}$	$12_{0,1}$	$0_{0,2}$	$5_{0,3}$	$14_{0,4}$	$3_{0,5}$	$9_{0,6}$	$10_{0,7}$	$1_{0,8}$	$11_{0,9}$	$15_{0,10}$	$6_{0,11}$	$4_{0,12}$	$8_{0,13}$	$2_{0,14}$	$13_{0,15}$
$2_{1,0}$	$9_{1,1}$	$14_{1,2}$	$0_{1,3}$	$11_{1,4}$	$6_{1,5}$	$5_{1,6}$	$12_{1,7}$	$4_{1,8}$	$7_{1,9}$	$3_{1,10}$	$10_{1,11}$	$8_{1,12}$	$13_{1,13}$	$15_{1,14}$	$1_{1,15}$
$8_{2,0}$	$5_{2,1}$	$3_{2,2}$	$15_{2,3}$	$13_{2,4}$	$10_{2,5}$	$6_{2,6}$	$0_{2,7}$	$2_{2,8}$	$14_{2,9}$	$12_{2,10}$	$9_{2,11}$	$1_{2,12}$	$4_{2,13}$	$11_{2,14}$	$7_{2,15}$
$11_{3,0}$	$6_{3,1}$	$5_{3,2}$	$3_{3,3}$	$0_{3,4}$	$9_{3,5}$	$12_{3,6}$	$15_{3,7}$	$13_{3,8}$	$8_{3,9}$	$10_{3,10}$	$4_{3,11}$	$14_{3,12}$	$7_{3,13}$	$1_{3,14}$	$2_{3,15}$

S_7

$10_{0,0}$	$6_{0,1}$	$9_{0,2}$	$13_{0,3}$	$5_{0,4}$	$4_{0,5}$	$14_{0,6}$	$0_{0,7}$	$8_{0,8}$	$1_{0,9}$	$11_{0,10}$	$7_{0,11}$	$15_{0,12}$	$12_{0,13}$	$2_{0,14}$	$3_{0,15}$
$2_{1,0}$	$12_{1,1}$	$0_{1,2}$	$3_{1,3}$	$10_{1,4}$	$14_{1,5}$	$4_{1,6}$	$13_{1,7}$	$9_{1,8}$	$11_{1,9}$	$6_{1,10}$	$15_{1,11}$	$1_{1,12}$	$5_{1,13}$	$7_{1,14}$	$8_{1,15}$
$0_{2,0}$	$7_{2,1}$	$13_{2,2}$	$8_{2,3}$	$6_{2,4}$	$1_{2,5}$	$9_{2,6}$	$3_{2,7}$	$10_{2,8}$	$2_{2,9}$	$14_{2,10}$	$4_{2,11}$	$5_{2,12}$	$15_{2,13}$	$11_{2,14}$	$12_{2,15}$
$15_{3,0}$	$3_{3,1}$	$10_{3,2}$	$2_{3,3}$	$8_{3,4}$	$9_{3,5}$	$4_{3,6}$	$14_{3,7}$	$5_{3,8}$	$12_{3,9}$	$7_{3,10}$	$1_{3,11}$	$11_{3,12}$	$0_{3,13}$	$13_{3,14}$	$6_{3,15}$

S_8

$15_{0,0}$	$12_{0,1}$	$8_{0,2}$	$2_{0,3}$	$4_{0,4}$	$9_{0,5}$	$1_{0,6}$	$7_{0,7}$	$5_{0,8}$	$11_{0,9}$	$3_{0,10}$	$14_{0,11}$	$10_{0,12}$	$0_{0,13}$	$6_{0,14}$	$13_{0,15}$
$10_{1,0}$	$6_{1,1}$	$9_{1,2}$	$0_{1,3}$	$12_{1,4}$	$11_{1,5}$	$7_{1,6}$	$13_{1,7}$	$15_{1,8}$	$1_{1,9}$	$3_{1,10}$	$14_{1,11}$	$5_{1,12}$	$2_{1,13}$	$8_{1,14}$	$4_{1,15}$
$1_{2,0}$	$4_{2,1}$	$11_{2,2}$	$13_{2,3}$	$12_{2,4}$	$3_{2,5}$	$7_{2,6}$	$14_{2,7}$	$10_{2,8}$	$15_{2,9}$	$6_{2,10}$	$8_{2,11}$	$0_{2,12}$	$5_{2,13}$	$9_{2,14}$	$2_{2,15}$
$13_{3,0}$	$2_{3,1}$	$8_{3,2}$	$4_{3,3}$	$6_{3,4}$	$15_{3,5}$	$11_{3,6}$	$1_{3,7}$	$10_{3,8}$	$9_{3,9}$	$3_{3,10}$	$14_{3,11}$	$5_{3,12}$	$0_{3,13}$	$12_{3,14}$	$7_{3,15}$

TABELA 6: Caixas S (segunda parte).

O texto claro convertido em uma sequência binária é dividido em blocos M que podem ser de 64 dígitos cada.

Consideremos a função I que permuta a posição dos 64 dígitos do bloco M. Geralmente I é definida por uma tabela.

Para efeito de compreensão do algoritmo, chamemos a imagem I(M) de N_0 e descrevamos uma rodada do algoritmo (geralmente são realizadas 16 rodadas), que:

(i) Dividamos o bloco N_0 de 64 dígitos em duas partes: a parte "esquerda", que chamaremos de E_0 e a parte "direita" que chamaremos de D_0.

(ii) Consideremos a função X que expande o bloco D_0, de 32 dígitos, para um bloco $X(D_0)$ de 48 dígitos. Além da expansão, nessa etapa temos também uma permutação de dígitos, uma vez que, à semelhança de I, X é dada por uma tabela.

(iii) Consideremos um bloco aleatório de 48 dígitos binário que denotaremos por K_1. Esse bloco é parte das chaves do sistema criptográfico (para cada rodada há uma chave).

(iv) Uma soma binária dígito a dígito entre $X(D_0)$ e K_1 é realizada.

(v) O bloco $X(D_0) + K_1$ é dividido em blocos B_1, …, B_8 de 6 dígitos cada e, utilizando 8 funções redutoras S_1, …, S_8. Essas funções transformam B_i de 6 dígitos em blocos B'_i de 4 dígitos. Desse modo, o bloco $X(D_0) + K_1$ é transformado em um bloco S de 32 dígitos.

(vi) Uma outra permutação de dígitos P é aplicada ao bloco S.

(vii) Uma outra soma binária dígito a dígito é feita entre o bloco P(S) e o bloco E_0. Essa soma é chamada de D_1.

(viii) Definimos o bloco E_1 como sendo o bloco D_0.

(ix) Um novo bloco N_1 é formado pela junção do bloco E_1 com o bloco D_1 formado acima.

O bloco N_1 é submetido a uma nova rodada conforme descrito acima e obtemos N_2, N_3 até N_{16}.

Após as 16 rodadas, é realizada uma troca de lados em N_{16} entre os blocos E_{16} e D_{16}.

Chamemos essa troca de *T*. Assim, $T(E_{16}) = D'_{16}$ e $T(D_{16}) = E'_{16}$ e, temos um novo bloco $T(N_{16}) = N'_{16}$.

Por fim, a inversa da função permutação I, ou seja, I^{-1} é aplicada em N'_{16} e este é o bloco encriptado, que chamaremos de C. Assim, $I^{-1}(N'_{16}) = C$.

Simplificado, temos a seguinte composta:

$$I(M) = N_0 = E_0D_0 \rightarrow X \circ I(M) = E_0X(D_0) \rightarrow \circ$$

$$K_i \circ X \circ I(M) = E_0 [X(D_0) + K_1] = E_0 [B_1B_2B_3B_4B_5B_6B_7B_8] \rightarrow$$

$$S \circ K_1 \circ X \circ I(M) = E_0 [S_1(B_1) S_2(B_2) S_3(B_3) \ldots S_7(B_7) S_8(B_8)]$$

$$S \circ K_1 \circ X \circ I(M) = E_0 [B'_1B'_2B'_3B'_4B'_5B'_6B'_7B'_8] \rightarrow S \circ K_1 \circ X \circ I(M) = E_0S$$

$$\rightarrow P \circ S \circ K_1 \circ X \circ I(M) = E_0P(S) \rightarrow E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = [E_0 + P(S)] \rightarrow$$

$$D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = D_0[E_0 + P(S)] \rightarrow D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = D_0D_1$$

$$\rightarrow D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = E_1D_1 \rightarrow D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = N_1$$

Chamando $D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X = Z_1$. Logo,

$$Z_1 \circ I(M) = N_1.$$

Aplicando 16 rodadas, temos:

$$Z_{16} \circ \ldots \circ Z_1 \circ I(M) = N_{16} \rightarrow T \circ Z_{16} \circ \ldots \circ Z_1 \circ I(M) = N'_{16} \rightarrow$$

$$I^{-1} \circ T \circ Z_{16} \circ \ldots \circ Z_1 \circ I(M) = C$$

Chamando $I^{-1} \circ T \circ Z_{16} \circ \ldots \circ Z_1 \circ I(M) = DES$, temos

$$DES(M) = C.$$

Como o algoritmo é simétrico, para decifrar C, basta aplicá-lo novamente, ou seja

$$DES(C) = M.$$

Sigamos ao exemplo prático:

Seja a mensagem PROFMAT_RJ. Suponhamos que o emissor A, queira enviar essa mensagem ao receptor B usando a Criptografia DES. Assim o emissor A associa a mensagem aos números correspondentes na **TABELA 1**, obtendo a sequência de números:

25 27 24 15 22 10 29 36 27 19,

que, respectivamente, na base binária são:

011001 011011 011000 001111 010110 000010 011101 100100 011011 010011

Agrupando a sequência de bits em blocos de 64 bits temos:

M = 0110010110110110000011110101100000100111011001000110110100110000. (1)

Notemos que tinhamos apenas 60 bits. Os bits que ficaram faltando para completar um bloco de 64 bits foram obtidos acrescentando-se 4 zeros ao final da sequência.

Logo, para o início do processo de **<u>ciframento</u>**, a mensagem passa pela primeira fase que é a função permutação I, a partir da **TABELA 2**, no qual é obtida pela sequência a seguir:

$$I(M)=N_0= 1111001100000010100010100110100101010101011101110001011001001100 \quad (2)$$

O *n*-ésimo bit de (2) é o *m*-ésimo bit de (1), sendo que *m* e *n* estão relacionados de acordo com a entrada m_n da **TABELA 2**. Por exemplo, se $n = 1$, a **TABELA 2** fornece $m = 59$, $n = 2$, a **TABELA 2** fornece $m = 51$.

Logo, o 1º bit de (2) é o 59º bit de (1), o 2º bit de (2) é o 51º bit de (1) e assim por diante.

Separando (2) em blocos de 32 bits, obtemos dois blocos. Chamaremos os primeiros 32 bits de bloco da "esquerda" e denotaremos por "E_0" e os outros 32 bits restantes de bloco da "direita" e denotaremos por "D_0". Assim,

$$E_0 = 11110011000000101000101001101001$$
$$D_0 = 01010101011101110001011001001100 \quad (3)$$

Para o bloco D_0 faremos uma expansão usando a **TABELA 4**. Assim, essa sequência de 32 bits será transformada em uma nova sequência com 48 bits, dada por:

$$X\,(D_0) = 110000010110100110001110000110010111010110110111 \quad (4)$$

O *n*-ésimo bit de (4) é o *m*-ésimo de (3), sendo que *m* e *n* estão relacionados de acordo com a entrada da **TABELA 4**. Por exemplo, se $n = 1$, a **TABELA 4** fornece $m = 15$. Logo, o 1º bit de (4) é o 15º bit de (3) e assim, por diante.

Consideremos uma sequência binária de 48 bits, que será a chave (que deve ser mantida em sigilo pelos comunicantes):

$$K_1 = 111101101010010010100011000110010110100111010001$$

Fazendo a soma binária, dígito a dígito, dos 48 bits do bloco $X\,(D_0)$ com a chave K_1, temos a nova sequência:

$$X(D_0) + K_1 = 001101111100110100101101000000000001110001100110.$$

Usaremos agora, as Caixas *S* **TABELA 6** para comprimir a sequência acima de 48 bits para 32 bits binários. Primeiramente, dividiremos a sequência anterior em blocos de 6 bits obtendo: B_1 o primeiro bloco, B_2 o segundo bloco até o oitavo bloco:

$$\underbrace{001101}_{B_1}\ \underbrace{111100}_{B_2}\ \underbrace{110100}_{B_3}\ \underbrace{101101}_{B_4}\ \underbrace{000000}_{B_5}\ \underbrace{000001}_{B_6}\ \underbrace{110001}_{B_7}\ \underbrace{100110}_{B_8}$$

Os blocos B, serão reduzidos a quatro bits cada utilizando-se as Caixas S_i do seguinte modo:

O primeiro e último dígito de B_i formam, em decimal, um número x de 0 a 3, que corresponde a uma das quatro linhas de S_i. Os quatro dígitos intermediários de B_i formam, em decimal, um número y de 0 a 15, que corresponde a uma das 16 colunas de S_i. Assim, localizamos o número $s_{x,y}$ na tabela S_i. O número s é um número de 0 a 15, que em binário, corresponde a uma sequência B'_i de quatro dígitos que será colocada no lugar de B_i.

Por exemplo, no primeiro bloco

$$B_1 = 001101,$$

temos que o primeiro e o último dígitos, 0 e 1, formam o número binário 01, que em decimal é o número 1, ou seja, temos a segunda linha de S_1. Os quatro dígitos do meio de B_1 formam o número binário 0110, que em decimal é o número 6, que corresponde a sétima coluna de S_1. Logo, localizamos $s_{x,y} = 11_{1,6}$, ou seja, s = 11, que em binário é 1011. Assim $B_1 = 001101$ é substituído por $B'_1 = 1011$.

De modo analógo para o restante dos blocos vamos obter:

$B'_2 = 1001$, $B'_3 = 1101$, $B'_4 = 1110$, $B'_5 = 0110$, $B'_6 = 0010$, $B'_7 = 0101$, $B'_8 = 1101$.

Juntando todos os blocos B'_i, para $i = 1, 2, 3, ...8$, em uma só sequência obtemos:

$$S = 10111001110111100110001001011101$$

Usando a **TABELA 5**, fazemos uma nova permutação da sequência acima à semelhança da que fizemos na sequência (1) a qual chamaremos de P(S):

$$P(S) = 01010011111000111110111101001100$$

Fazendo a soma binária de $E_0 + P(S)$ temos:

$$D_1 = E_0 + P(S) = 10100000111000010110010100100101$$

Juntando, respectivamente, as sequências D_0 e D_1 temos:

$$N_1 = 01010101011101110001011001001100101000001110000101100101001001 01$$

Aplicando a troca T dos blocos de 32 dígitos dos lados esquerdo e direito temos:

$$T(N_1) = N'_1 = 10100000111000010110010100100101010101010101110111000101100100 1100$$

Para finalizar a criptografia vamos utilizar a **TABELA 3** e aplicar a permutação I^{-1} na sequência anterior:

$$C = I^{-1}(N'_1) = 11010101000001100101111100001000000001111111010010011101101000 00$$

Logo essa sequência, é a mensagem criptografada. Assim o emissor A envia essa mensagem para o receptor B.

Para o **deciframento**, a sequência recebida o receptor B deverá proceder de modo analógo ao processo de ciframento.

O receptor B aplicará a função I a partir da **TABELA 2**, que é a primeira fase, e obterá a sequência a seguir:

$$I(C) = 10100000111000010110010100100101010101010101110111000101100100 1100$$

Separando a sequência anterior em blocos de 32 bits, obtemos dois blocos. Chamaremos os 32 bits de bloco da “esquerda”, que denotaremos por “E_0” e os outros 32 bits restantes de bloco da “direita”, que será denotado por “D_0”:

$$E_0 = 10100000111000010110010100100101$$
$$D_0 = 01010101011101110001011001001100$$

Para o bloco D_0 faremos a expansão usando a **TABELA 4**. Assim, a sequência de 32 bits será transformada em uma nova sequência com 48 bits:

$$X(C) = 110000010110100110001110000110010111010110110111$$

Usando a mesma chave K_1 de 48 bits que usamos para cifrar a mensagem, dada a seguir:

$$K_1 = 111101101010010010100011000110010110100111010001$$

Fazemos a soma binária desses 48 bits com o bloco X(C) e obtemos uma nova sequência:

$$X(C) + K_1 = 001101111100110100101101000000000001110001100110$$

Utilizando a **TABELA 6**, das Caixas S, e fazendo os mesmos procedimentos adotados no ciframento, separemos a sequência em blocos de 6 bits:

$$\underbrace{001101}_{B_1}\ \underbrace{111100}_{B_2}\ \underbrace{110100}_{B_3}\ \underbrace{101101}_{B_4}\ \underbrace{000000}_{B_5}\ \underbrace{000001}_{B_6}\ \underbrace{110001}_{B_7}\ \underbrace{100110}_{B_8}$$

Teremos a seguinte redução de 6 bits para 4 bits dada a seguir:

$$B'_1 = 1011,\ B'_2 = 1001,\ B'_3 = 1101,\ B'_4 = 1110,\ B'_5 = 0110,\ B'_6 = 0010,\ B'_7 = 0101,\ B'_8 = 1101$$

Juntando todos os blocos B'_i, para $i = 1, 2, ...8$, em uma só sequência obtemos:

$$S = 10111001110111100110001001011101$$

Usando a **TABELA 5**, da função permutação, na sequência acima obtemos a sequência a seguir no qual chamaremos de P(S):

$$P(S) = 01010011111000111110111101001100$$

Fazendo a soma binária de $E_0 + P(S)$ temos:

$$D_1 = E_0 + P(S) = 11110011000000101000101001101001$$

Juntando, respectivamente, as sequências D_0 e D_1 temos:

$$N_1 = 01010101011101110001011001001100111100110000001010001010011010 01$$

Aplicando T:

$$T(N_1) = N'_1 = 11110011000000101000101001101001010101010111011100010110010011 00$$

Para finalizar o deciframento vamos utilizar a **TABELA 3** e aplicar a função I^{-1} na sequência anterior chegando em:

$$M = I^{-1}(N'_1) = 01100101101101100000111101011000001001110110010001101101001100 00$$

Logo, essa sequência, é a mensagem decifrada. Ou seja, separando essa sequência em blocos de 6 bits e passando para a base decimal, obtemos os números:

25 27 24 15 22 10 29 36 27 19

que corresponde a mensagem original PROFMAT_RJ.

Nesse exemplo, para simplificar, usamos uma única rodada, mas isso é inseguro. Para oferecer maior segurança e resistência à criptoanálise o ideal é que se realizem várias rodadas, no caso 16 rodadas é o tamanho típico para a criptografia DES.

3.5 – Advanced Encryption Standard (Padrao de Encriptacao Avancada) ou AES

Segundo Stallings (2015), o AES foi publicado pelo National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia), ou NIST, em 2001, que foi

escolhido através de um concurso que desenvolvesse um algoritmo de chave simétrica para proteger informações, os vencedores foram os belgas Vincent Rijmen e Joan Daemen. A definição do AES conforme Stallingsn(2015): "é uma cifra de bloco e foi adotado como método padrão pelo governo dos Estados Unidos pela eficiência demonstrada". Após 2006, o AES tornou-se um dos algoritmos mais populares, usado para Criptografia de chave simétrica, e se concretizou como o substituto do DES. Comparada as cifras de chave pública como a RSA, a estrutura do AES e a maioria das cifras simétricas são bastante complexas e não explicadas tão facilmente quanto outras cifras criptográficas.

O tamanho de bloco fixo do AES e da chave são de 128 bits, além desse valor, a chave também pode ser de 192 ou 256 bits, o AES não é complexo de executar e precisa de pouca memória, possui software e hardware rápidos.

Capitulo 4
Criptografia ou encriptação Assimétrica

Por mais de dois mil anos, desde a época da cifra de César até a década de 70, a comunicação cifrada exigia que as duas partes comunicantes compartilhassem um segredo em comum, a chave simétrica usada para cifrar e decifrar. Uma dificuldade dessa abordagem é que as duas partes têm que escolher, conjuntamente e de alguma maneira, qual é a chave.
Mas, para isso, é preciso comunicação segura. Uma alternativa seria um encontro entre as partes para que escolhessem, pessoalmente, a chave. Porém, no atual mundo em rede, o mais provável é que as partes comunicantes nunca possam se encontrar. No intuito de resolver este problema, vários cientistas na década de 70 voltaram suas pesquisas para a busca de uma solução que desse fim a este impasse. Porém, em 1976, Diffie e Hellman apresentaram um algoritmo conhecido como Diffie Hellman Key Exchange, que tornou possível a comunicação por criptografia sem a necessidade de compartilhamento antecipado de uma chave secreta comum. Uma abordagem da comunicação segura radicalmente diferente e de uma elegância que levou ao desenvolvimento dos atuais sistemas de criptografia de chaves públicas.

4.1 – Criptografia de chave pública

Stallings (2015) explica que a maior e talvez a única revolução verdadeira em toda a história da criptografia foi o progresso da criptografia de chave pública. De seu surgimento até os dias atuais é possível verificar que as ferramentas elementares da substituiçãp e permutação são os mais usados nos sistemas criptográficos. Depois de muitos anos surgiu a máquina de encriptação/decriptação de rotor, a qual foi de fundamental importância no avanço da criptografia simétrica, este progresso reduziu de forma significativa o trabalho que seriam calculados à mão. A máquina de encriptação/decriptação de rotor possibilitou o surgimento de cifras cada vez mais complexas. Com a utilização dos computadores, muitos sistemas foram surgindo, e dentre estes tivemos como ponto forte o Data Encryption Standard (DES), que foi desenvolvido pela Lucifer na IBM. Mesmo com todo o desenvolvimento tanto das máquinas de rotor quanto do DES ainda não foi possível deixar de usar muitas das ferramentas básicas de substituição e permutação.

Houve uma mudança significativa no cenário da criptografia com o surgimento da criptografia de chave pública. Temos de um lado, os algoritmos que são baseados em funções

matemáticas chamados de chave pública que usavam substituição e permutação. Outro ponto significativo é que a criptografia de chave pública é assimétrica, que necessita do uso de duas chaves separadas, ao contrário da criptografia simétrica, que utiliza apenas uma chave. A importância de usar duas chaves é que haverá consequêcnias significativas nas áreas de confidencialidade, distribuição de chave e autenticação.

Conforme explica Stallings (2015), existem muitas produções erradas com relação à criptografia de chave pública. A primeira delas é dizer que a criptografia de chave pública é mais segura contra a criptoanálise do que a criptografia simétrica. O que acontece realmente, é que o tamanho da chave e o trabalho computacional envolvido para quebrar uma cifra é o que necessita qualquer esquema de criptografia para sua segurança. Não há nada em princípio sobre a criptografia simétrica ou de chave pública que torne uma superior à outra, do ponto de vista de resistência à criptoanálise.

O segundo erro é afirmar que a criptografia simétrica se tornou inadequada devido ao uso da criptografia de chave pública. De outro modo, por conta do *overhead* computacional dos esquemas de criptografia de chave pública atuais, parece não haver probabilidade previsível de que a criptografia simétrica será abandonada.

E finalmente, ainda existe um desconforto na distribuição de chave quando se usa a criptografia de chave pública, pois afirmam ser trivial, em comparação com o tratamento um tanto desajeitado que é envolvido com os centros de distribuição de chave para a criptografia simétrica. O que realmente acontece, é que existe a necessidade de alguma forma de protocolo, geralmente abrangendo um agente central, e os procedimentos envolvidos não são mais simples nem mais eficientes do que aqueles exigidos para a criptografia simétrica.

Para Stallings (2015), a evolução do conceito de criptografia de chave pública se deve ao fato da tentativa de atacar dois dos problemas mais difíceis associados à encriptação simétrica. O primeiro é o da distribuição de chaves.

"A encriptação simétrica requer (1) que dois comunicantes já compartilhem uma chave, que de alguma forma foi distribuída a eles; ou (2) o uso de um centro de distribuição de chaves. Whitfield Diffie, um dos descobridores da encriptação de chave pública (com Martin Hellman, ambos da Stanford University, na época), raciocinou que esse segundo requisito anulava a essência da criptografia: a capacidade de manter sigilo total sobre a sua própria comunicação. Conforme foi dito por Diffie: “afinal, qual seria a vantagem de desenvolver criptossistemas impenetráveis, se seus usuários fossem forçados a compartilhar suas chaves

com um CDC que poderia ser comprometido por roubo ou suborno?""(Stallings, 2015)

O segundo problema sobre o qual Diffie ponderou, e que estava aparentemente não relacionado com o primeiro, foi o de *assinaturas digitais*. Se o uso da criptografia tivesse que se tornar comum, não apenas nas situações militares, mas para fins comerciais e particulares, então as mensagens e documentos eletrônicos precisariam do equivalente das assinaturas usadas nos documentos em papel. Ou seja, poderia ser criado um método para estipular, para a satisfação de todas as partes, que uma mensagem digital foi enviada por determinada pessoa?

Diffie e Hellman fizeram uma descoberta incrível em 1976, surgindo com um método que resolvia os dois problemas e que era radicalmente diferente de todas as técnicas anteriores de criptografia, quatro milênios atrás.[8]

4.2 – Modelo de Cifra Assimétrica

Stallings (2015) explica que os algoritmos assimétricos precisam de duas chaves: uma para codificação e outra diferente, mas que seja usada para a decodificação. Segue algumas das principais características:

- É praticamente difícil determinar computacionalmente a chave de decodificação conhecemdo apenas o algoritmo de criptografia e da chave de codificação.
- Qualquer chave pode ser escolhida para ser usada para codificação com a outra para decodificação.

Segue abaixo um esquema de encriptação de chave pública com cinco itens, conforme mostra Stallings (2015):

- **Texto claro:** mensagem ou dados originais onde é possível a compreensão e que servem como entrada do algoritmo de encriptação.
- **Algoritmo de encriptação:** é o que realiza as diversas substituições e transformações no texto claro.

8 "Diffi e e Hellman apresentaram *publicamente* os conceitos da criptografia de chave pública em 1976. Hellman dá crédito a Merkle com a descoberta independente e simultânea do conceito, embora Merkle não o tenha publicado antes de 1978. De fato, o primeiro documento não confidencial descrevendo a distribuição de chave pública e a criptografia foi uma proposta de projeto de 1974 por Merkle (<http://
merkle.com/1974>). Porém, esse não foi o verdadeiro início. O almirante Bobby Inman, como diretor da National Security Agency (NSA), reivindicou que a criptografia de chave pública tinha sido descoberta na NSA em meados da década de 1960. A primeira apresentação *documentada* desses conceitos veio em 1970, do Communications-Electronics Security Group, o equivalente britânico da NSA, em um relatório confidencial de James Ellis. Ellis referia-se à técnica como *criptografia não secreta*." (Stallings, 2015)

- **Chaves pública e privada:** São as chaves usadas no algoritmo, sendo uma usada para a codificação, e a outra para codificação. As transformações exatas realizadas pelo algoritmo dependem da chave pública ou privada que é fornecida como entrada.
- **Texto cifrado:** é a mensagem embaralhada produzida como saída. Ela depende do texto claro e da chave. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes.
- **Algoritmo de decriptação:** é o algoritmo que recebe o texto inelegível e a chave produz o texto original.

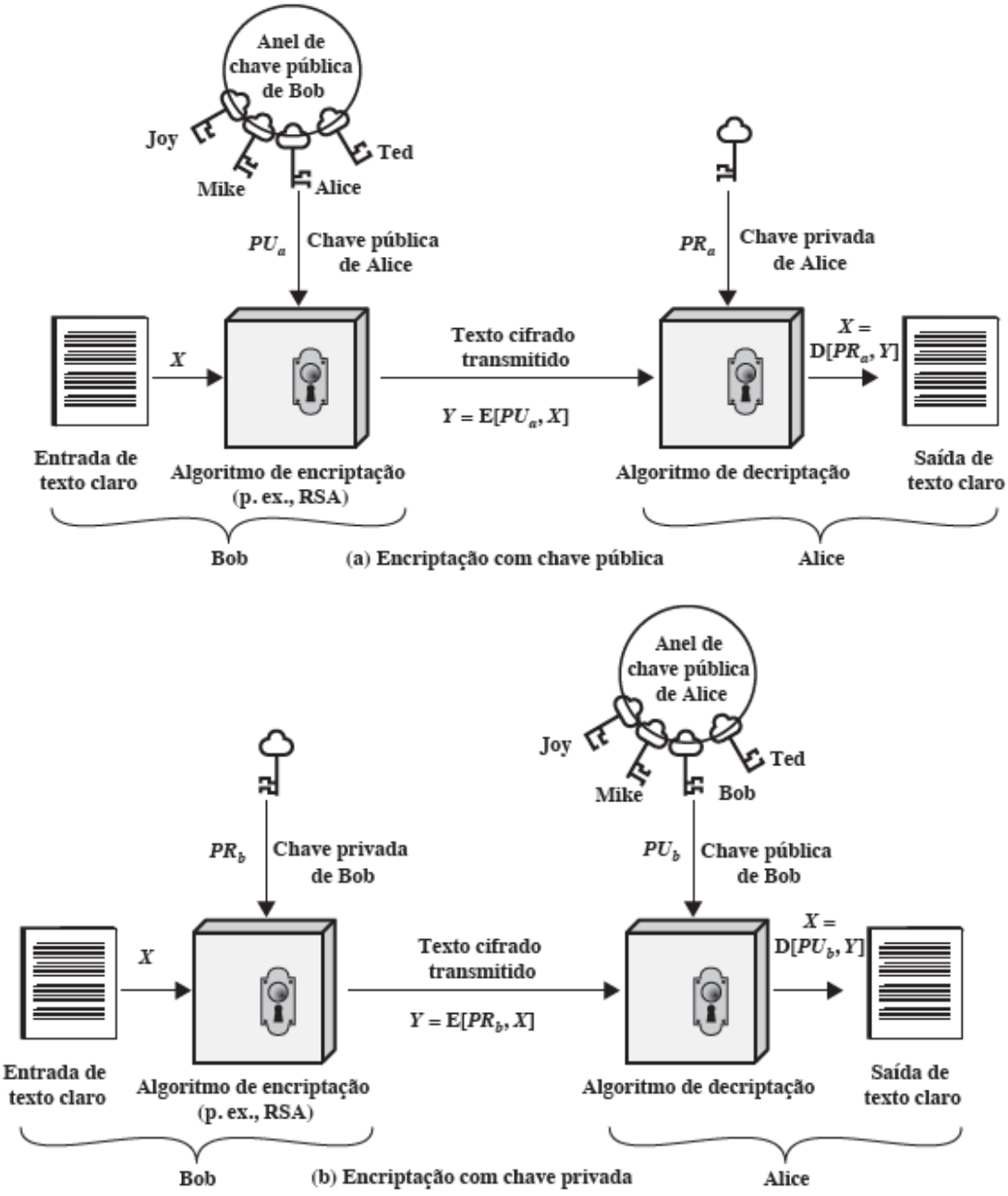


Figura 21: Criptografia de chave pública
(Fonte: Stallings, 2015, p. 202)

Segue as etapas essenciais segundo Stallings (2015):

1. Cada usuário gera um par de chaves a ser usado para a encriptação e a decriptação das mensagens.
2. Cada usuário coloca uma das duas chaves em um registrador público ou em outro arquivo acessível. Essa é a chave pública. A chave acompanhante permanece privada. Como a Figura 21.1a sugere, cada usuário mantém uma coleção de chaves públicas obtidas de outros.
3. Se Bob deseja enviar uma mensagem confidencial para Alice, ele a encripta usando a chave pública de Alice.
4. Quando Alice recebe a mensagem, ela a decripta usando sua chave privada. Nenhum outro destinatário pode decriptar a mensagem, pois somente Alice conhece a chave privada de Alice.

Observe que as chaves públicas ficam disponíveis para todos os participantes, cada participante produz localmente as chaves privadas e, portanto, nunca necessitam serem distribuídas. A comunicação recebida estará protegida sempre que a chave privada de um usuário permanecer protegida e secreta. Uma questão importante e eficaz é que em qualquer momento um sistema pode alterar sua chave privada e publicar uma chave pública correspondente para substituir sua antiga.

4.3 – Criptoanálise de chave pública

Stallings (2015) explica que tanto um sistema de codificação simétrico quanto o de chave pública estam suscetíveis a um ataque de força bruta. A contramedida é a mesma: use chaves grandes. Ainda assim, existe um dilema a ser considerado. Uma função matemática reversível para uso é do que depende os sistemas de chave pública. A dificuldade de executar os cálculos dessas funções pode não crescer de froma constante com o número de bits na chave, mas sim mais rapidamente do que isso. Concluir-se com isto que o ataque por força bruta se torna impraticável se o tamanho da chave for consideravelmente grande, porém pequeno pequeno para que a encriptação e a decriptação sejam viáveis. Mas o que acontece na prática? Acontece que o usuário ganha de um lado com um impraticável ataque por força bruta devido ao grande tamanho da chave, mas por outro lado perde em velocidade de encriptação/decriptação, pois ficou muito lenta para uso geral. De outro modo, a encriptação

de chave pública atualmente é confinada a aplicações de gerenciamento de chave e assinatura.

Um outro modo de atacar um sistema de chave pública é achar alguma forma de calcular a chave privada dada a chave pública. Até agora, a matemática não mostrou que essa forma de ataque é inviável para determinado algoritmo de chave pública. Com isto, o RSA e qualquer outro algoritmo utilizado são suspeitos. Um problema que parece insolúvel de um ponto de vista pode ter uma solução se for visto de uma maneira inteiramente diferente, isto é o que mostra a história da criptoanálise.

Por fim, há outra forma de ataque que é singular aos sistemas de chave pública. É um ataque de mensagem provável. Suponha, por exemplo, que uma mensagem tivesse que ser enviada contendo exclusivamente uma chave DES de 56 bits. Um invasor conseguiria encriptar todas as chaves DES possíveis de 56 bits usando a chave pública e descobrir a chave encriptada testando com o texto cifrado transmitido.

Portanto, para o esquema de chave pública o tamanho da chave não importa, pois o ataque é reduzido a um por força bruta em uma chave de 56 bits. Se adicionarmos alguns bits aleatórios a mensagens simples podemos impedri esse tipo de ataque.

4.4 – Algoritmo RSA

Stallings (2015) explica que a introdução de uma npva técnica para criptografia foi feito através de um artigo pioneiro de Diffie e Hellman e, de fato, causou alvoroço entre os criptologistas, pois desafiou os mesmos a encontrarem um algoritmo criptográfico que atendesse os requisitos para os sistemas de chave pública. Muitos algoritmos foram propostos. Alguns deles, embora inicialmente promissores, provaram ser falhos.

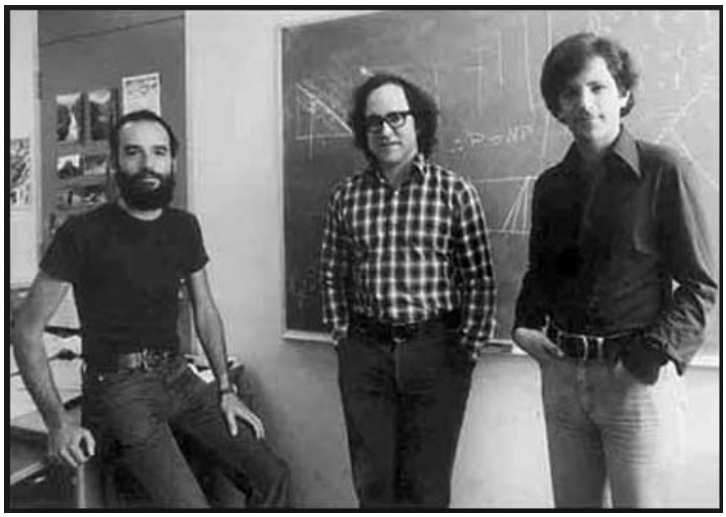


Figura 22: Ron Rivest, Adi Shamir e Leonard Adleman
(Fonte: brilliant.org)

Só em 1977 que surgiu uma das primeiras respostas ao desafio, desenvolvida por Ron Rivest, Adi Shamir e Len Adleman, no MIT, e publicada em 1978. O esquema Rivest-Shamir-Adleman (RSA), desde essa época, tem reinado soberano como a técnica de uso geral mais aceita e implementada para a encriptação de chave pública.

Uma cifra de bloco em que o texto claro e o cifrado são inteiros entre 0 e $n - 1$, para algum n é a definição do esquema RSA. Um tamanho típico para n é 1024 bits, ou 309 dígitos decimais. Ou seja, n é menor que 2^{1024}.

4.4.1 – Descrição matemática do algoritmo

Coutinho (2000) explica que para criptografar uma mensagem M, usando uma chave pública (e, n), onde e e n são inteiros positivos, façamos o seguinte:

- Represente a mensagem como um inteiro entre 0 e $n - 1$. (Se a mensagem for longa, quebre-a em blocos de modo que isso possa ser feito).
- Criptografe a mensagem elevando cada bloco M à "e-ésima" potência módulo n.

  Então, o resultado criptografado C é o resto da divisão de M^e por n:

$$C \equiv M^e \bmod n.$$

- Para decifrar a mensagem criptografada, eleve-a a uma outra potência d e calcule o resto da divisão de C^d por n. Assim,

$$M \equiv \mathrm{C^d} \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n.$$

Tanto o emissor quanto o receptor precisam conhecer o valor de n. O emissor conhece o valor de e, e somente o receptor sabe do valor de d. Assim, esse é um algoritmo de encriptação de chave pública com um chave pública $PU = (e, n)$ e uma chave privada $PR = (d, n)$. Para que esse algoritmo seja satisfatório à encriptação de chave pública, os seguintes requisitos precisam ser atendidos:

1. É possível encontrar valores de e, d e n, tais que $M^{ed} \bmod n = M$ para todo $M < n$.
2. É relativamente fácil calcular $M^e \bmod n$ e $C^d \bmod n$ para todos os valores de $M < n$.
3. Conhecendo e e n, é inviável determinar d.

Precisamos encontrar um relacionamento na forma

$$M^{ed} \bmod n = M$$

O relacionamento mostrado se mantém se e e d forem inversos multiplicativos módulo $\varphi(n)$, onde $\varphi(n)$ é a função totiente de Euler. O capítulo 2 mostrou que, para p, q primos, $\varphi(pq)$

$= (p - 1)(q - 1)$. O relacionamento entre e e d pode ser expresso como

$$ed \bmod \varphi(n) = 1$$

Isso é equivalente a dizer

$$ed = 1 \bmod \varphi(n)$$

$$d = e^{-1} \bmod \varphi(n)$$

Ou seja, e e d são inversos multiplicativos mod $\varphi(n)$. Observe que, de acordo com as regras da aritmética modular, isso é verdadeiro somente se d (e, portanto, e) for relativamente primo de $\varphi(n)$. de modo equivalente, $mdc(\varphi(n), d) = 1$.

Agora estamos prontos para formular o esquema RSA. Os ingredientes são os seguintes:

p, q, dois números primos	(privados, escolhidos)
$n = pq$	(público, calculado)
e, com $mdc(\varphi(n), e) = 1$, $1 < e < \varphi(n)$	(público, escolhido)
$d = e^{-1} \pmod{\varphi(n)}$	(privado, calculado)

A chave privada consiste em (d, n), e a chave pública, em (e, n). Suponha que o usuário A tenha publicado sua chave pública e que o usuário B queira enviar a mensagem M para A. Então, B calcula $C = M^e \bmod n$ e transnite C. Ao receber esse texto cifrado, o usuário A decripta calculando $M = C^d \bmod n$.

4.4.2 – Exemplo do RSA

Para usarmos o método *RSA*, devemos converter uma mensagem em uma sequência de números. Chamaremos essa etapa de *pré-codificação*.

Para efeito de exemplificação, tomemos a seguinte tabela de conversão na pré-codificação:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	_	0	1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

O espaço entre palavras será substituído pelo nº. 36. Por exemplo, a frase “PROFMAT_RJ”, é

convertida no número

$$25272415221029362719$$

A vantagem de se utilizar 2 dígitos para representar uma letra reside no fato de que tal procedimento evita a ocorrência de ambiguidades. Por exemplo, se *a* fosse convertido em 1 e *b* em 2*;* teríamos que *ab* seria 12*;* mas *l* também seria 12*:* Logo, não poderíamos concluir se 12 seria *ab* ou *l.*

Precisamos determinar 2 primos distintos, que denotaremos por p e q, que são denominados *parâmetros RSA*. Seja

$$n = pq,$$

que é chamado de *módulo RSA*.

A última etapa da pré-codificação consiste em separar o número acima em blocos cujos valores sejam menores que n.

A mensagem cuja conversão foi feita acima pode ser separada nos seguintes blocos:

$$25 \;\; 27 \;\; 24 \;\; 15 \;\; 22 \;\; 10 \;\; 29 \;\; 36 \;\; 27 \;\; 19$$

A maneira de escolher os blocos não é única e não precisa ser homogênea (todos os blocos com o mesmo número de dígitos), mas devemos tomar alguns cuidados como, por exemplo, não começar um bloco com zero, pois isto traria problemas na hora de montar a sequência recebida (o zero no início do bloco não pode aparecer!).

Passemos ao processo de codificação. Temos $n = pq$ com p e q primos.

Tomemos

$$\varphi(n) = (p - 1)\,(q - 1).$$

Seja $e < \varphi(n)$ inteiro positivo inversível módulo $\varphi(n)$, ou seja,

$$\text{mdc}\,(e, \varphi(n)) = 1.$$

Esse número e é chamado de *expoente de enciframento.*

O par (n, e) é denominado *chave pública de codificação do sistema RSA.*

Agora, codifiquemos cada bloco obtido na pré-codificação. Após a codificação, os blocos não poderão ser reunidos de modo que não possamos distinguí-los, pois isto tornaria impossível a decodificação da mensagem.

A codificação de um bloco b será denotada por $C(b)$. Temos que $C(b)$ é o resto da divisão de b^e por n, isto é,

$$\text{C(b)} \equiv b^e \pmod{n}.$$

Por exemplo, se $p = 29$ e $q = 67$, então $n = 1943$. Logo, $\varphi(n) = 1848$, pois $n = 1943 = 29 \times 67$.

Tomemos $e = 701$ (observe que mdc (701, 1848) = 1). Assim, o último bloco, 19, da mensagem anterior é codificado como o resto da divisão de 19^{701} por 1943. Calculando:

$$19^5 \equiv 717 \pmod{1953}$$
$$19^{10} \equiv 1137 \pmod{1943}$$
$$19^{20} \equiv 674 \pmod{1943}$$
$$19^{40} \equiv 1557 \pmod{1943}$$
$$19^{80} \equiv 1328 \pmod{1943}$$
$$19^{100} \equiv 1292 \pmod{1943}$$
$$19^{300} \equiv 1834 \pmod{1943}$$
$$19^{600} \equiv 223 \pmod{1943}$$
$$19^{700} \equiv 552 \pmod{1943}$$
$$19^{701} \equiv 773 \pmod{1943}$$

Fazendo o mesmo para os outro blocos,

Bloco 25: $25^{701} \equiv 895 \pmod{1943}$

Bloco 27: $27^{701} \equiv 259 \pmod{1943}$

Bloco 24: $24^{701} \equiv 198 \pmod{1943}$

Bloco 15: $15^{701} \equiv 595 \pmod{1943}$

Bloco 22: $22^{701} \equiv 1849 \pmod{1943}$

Bloco 10: $10^{701} \equiv 155 \pmod{1943}$

Bloco 29: $29^{701} \equiv 841 \pmod{1943}$

Bloco 36: $36^{701} \equiv 384 \pmod{1943}$

Codificando toda a mensagem, obtemos a seguinte sequência de blocos:

$$895 - 259 - 198 - 595 - 1849 - 155 - 841 - 384 - 259 - 773$$

Para decodificar uma mensagem codificada, precisamos de n e do inverso de e módulo $\varphi(n)$, que chamaremos de d, ou seja

$$ed \equiv 1 \pmod{\varphi(n)}.$$

O par (n, d) é denominado *chave privada de decodificação do sistema RSA*.

Seja $a = C(b)$ um bloco da mensagem codificada, então $D(a)$ será o resultado da decodificação. Temos que $D(a)$ é o resto da divisão de a^d por n, isto é,

$$D(a) \equiv a^d \pmod{n}.$$

Para calcular d, sendo conhecidos e e $\varphi(n)$, basta aplicar o algoritmo euclidiano

estendido, pois $1 = ed - k\,\varphi(n)$. Esperamos que, decodificando os blocos da mensagem codificada, possamos encontrar a mensagem original, ou seja, $D(C(b)) = b$. Para decodificarmos, não é necessário conhecermos p e q, basta conhecer n e d.

No exemplo que estamos acompanhando, temos que $n = 1943$ e $e = 701$.

Usando o algoritmo euclediano estendido para descobrir d, temos:

$$1848 = 2.701 + 446$$
$$701 = 1.446 + 255$$
$$446 = 1.255 + 191$$
$$255 = 1.191 + 64$$
$$191 = 3.64 - 1$$

Assim, temos:

$$1 = 3.64 - 191$$
$$1 = 3.(255 - 1.191) - 1.191$$
$$1 = 3.255 - 4.191$$
$$1 = 3.255 - 4.(446 - 1.255)$$
$$1 = 7.255 - 4.446$$
$$1 = 7.(701 - 1.446) - 4.446$$
$$1 = 7.701 - 11.446$$
$$1 = 7.701 - 11.(1848 - 2.701)$$
$$1 = 29.701 - 11.1848$$

Logo, concluímos que $d = 29$.

Assim, para decodificar o bloco 773 recebido, devemos calcular o resto da divisão de 773^{29} por 1943, ou seja, 19:

$$19 \equiv 773^{29} \pmod{1943}$$

Logo, a sequência decodificada será

$$25\ \ 27\ \ 24\ \ 15\ \ 22\ \ 10\ \ 29\ \ 36\ \ 27\ \ 19$$

que corresponde, via tabela de conversão, à expressão “PROFMAT_RJ”

Considerações finais

Embora este trabalho não tenha foco na aplicabilidade da criptografia no ensino básico, é possível verificar que muitas das cifras utilizadas ao longo do texto pode ser desenvolvida e ter como ponto de referência do processo de ensino e aprendizagem a abordagem de assuntos de interesse do estudante, tornando a Matemática interessante e motivadora. A criptografia pode ser utilizada como um gerador de situações desafiadoras que permitem o aprofundamento dos assuntos desenvolvidos no ensino básico, possibilitando dessa forma ao estudante perceber a utilização do conhecimento em situações práticas.

Um exemplo simples e sem muito custo de utilização de uma cifra em sala de aula, seria a cifra de Cesár, nessa cifra pode ser utilizado o conceito de permutação e combinação, assunto este que pode ser abordado de forma lúdica e que os estudantes aprendam de forma significativa.

Os materiais necessários são apenas papel e lápis e/ou caneta. Passos a serem desenvolvidos na aplicação da atividade:

1º passo: O professor levará várias frases codificadas, todas preparadas antes da aula, o interessante é usar várias variações da cifra, ou seja, andar duas, três, quatro, cinco casas e não apenas três como na cifra original.

2º passo: O professor dissertará um pouco sobre a cifra e sua utilização explicando como descobrir as frases usando as várias variações no alfabeto.

3º passo: Com as frases já descorbertas, o professor questionará os estudantes numa discussão onde seja levado em consideração pontos importantes da cifra, tais como: senha única, permutação, combinação e dificuldade na decifragem.

Outro exemplo seria a construção e utilização de um bastão de Licurgo, essa cifra é uma das quais pode ser usada em sala de aula de forma significativa. Materiais necessários:

- Garrafas pets de vários tamanho;
- Cola;
- Papel; e
- Lápis e/ou caneta.

Passos a serem seguindos:

1º passo: A preparação de todo material a ser utilizado será feito antes de sua aplicabilidade em sala de aula, devido a isto, o professor levará as garrafas com diâmetros diferentes e as

tiras de papel já com as frases prontas.

2º passo: O professor comentará um pouco dessa cifra com os estudantes e sua importância na história.

3º passo: Logo em seguida, distribuirá as garrafas com diâmetros diferentes e as várias tiras de papel e verificará se os estudantes serão capazaes de descobrirem as frases.

4º passo: Possivelmente os estudantes conseguiram desvendar as frases, pois no 2º passo o professor já explicou como a cifra era utilizada.

5º passo: Questionamentos e discussões sobre o tema estudado, principlamente em relação a noção de senha única, ou seja, o professor entrará com o conceito de criptografia simétrica (neste caso será a senha usada para cifrar que será a mesma para decifrar).

Observe que o importante nessa atividade não é a descorberta das frases, mas sim o conceito de senha única utilizada para descobrir as frases, neste caso a senha utilizada foi o diâmetro da garrafa, pois as frases só seram descorbertas nas garrafas corretas.

Referências Bibliográficas:

AVALIAÇÃO à distância: Criptografia. Centro de Educação à Distância do Estado do Rio de Janeiro. Rio de Janeiro: Fundação CECIERJ, 2017.

Coutinho, S. C. *Números inteiros e Criptografia RSA*, 2ª ed., vol. 2 de S*érie de Computação e Matemática.* Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2000.

C. L. Barczark. *A Indecifrável Enigma*. São Paulo. Clube de Autores. 2014.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret*. E.U.A.. Editora Scribner Book Company, 1996.

Schneeberger, Carlos Alberto. *História Geral: teoria e prática*. São Paulo. Editora Rideel, 2006.

Singh, Simon. *O livro dos códigos*. Rio de Janeiro. Editora Record, 2007.

Stallings, William. *Criptografia e segurança de redes: princípios e práticas*/William Stallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi Messeder Barreto, Rafael Misoczki. - 6. ed. - São Paulo: Pearson Education do Brasil, 2015.

Wazlawick, Raul Sidnei. *História da Computação*. Rio de Janeiro. Editora Elsevier, 2016.