

CRIPTOGRAFIA DE DADOS



Premissa:

... informação é poder ...

Deus

usou a matemática

para construir o

Universo ...

Criptografia:

cryptos = **secreto**

grafia = **escrita**

- técnica mais elaborada;
- processos sistematizados de transformação da mensagem original em uma mensagem ininteligível;
- a mensagem, não pode ser entendida a não ser pelas pessoas que sabem como recuperá-la;
- a mensagem, mesmo sendo interceptada em seu trânsito, resiste à decifragem;
- dois conceitos importantes estão na base da criptografia: os conceitos de algoritmo (cifra ou código) e o de chave.

Ex:

Chave:

- língua do p; **ex: pvoupaopcipnepma**

- Código de César;

- Máquina Enigma;

- Algoritmo:

- DES;

- 3DES;

- MD5;

- Blowfish;

- Certificação digital;

Transposição

- Troca de posição das letras na mensagem;
- Embaralhamento das letras segundo uma chave pré- definida.

03 letras assumem 6 formas diferentes ($3!=6$)

Ex: a palavra SOL -> sol, slo, osl, ols, Iso e los

- Texto com 35 palavras ficaria:

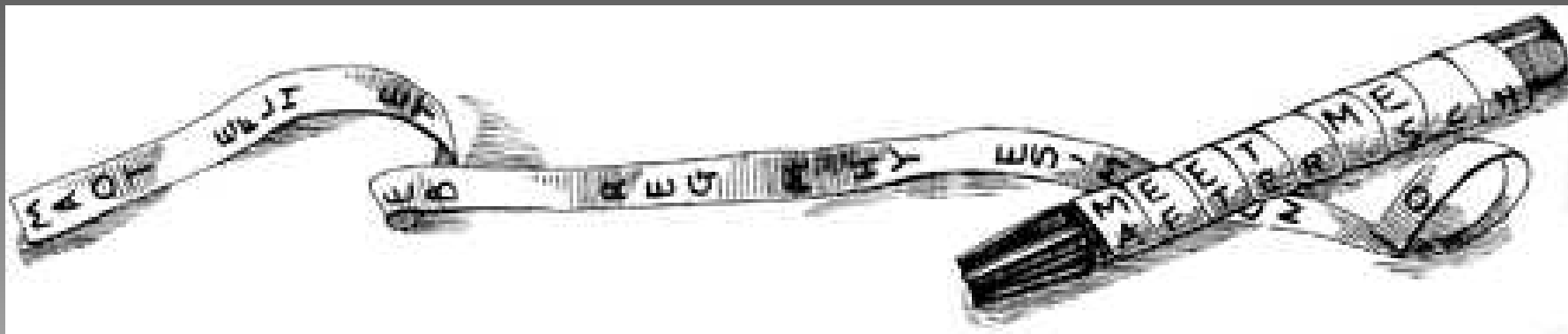
$35!=10.333.147.966.386.144.929.666.651.337.523.200.000.000$

Problema ???

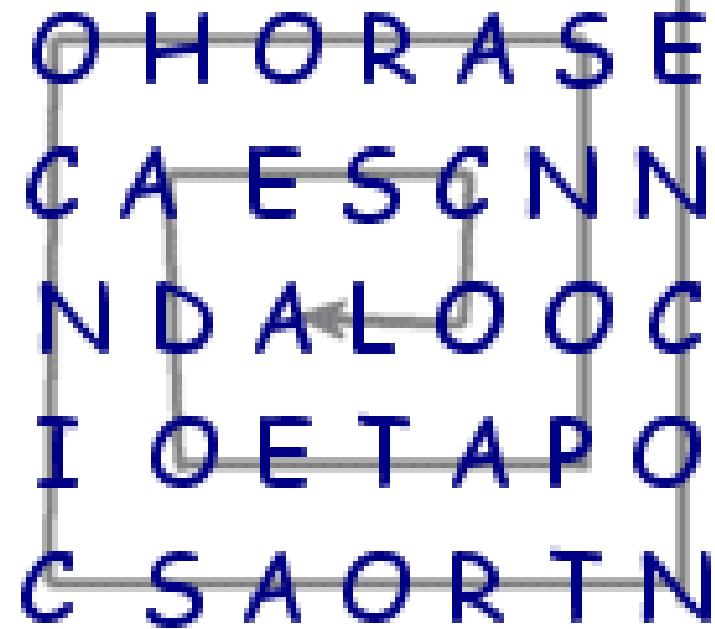
Ex:

- bastão de Licurgo (Sytale Spartano);
- grelha indefinida (Luigi Sacco durante a I Guerra Mundial);
- tabela Espartana.

Bastão de Licurgo (Scytale Spartano)



Grelha indefinida



A 5x5 grid of letters is shown. The letters are arranged as follows:

O	H	O	R	A	S	E
C	A	E	S	C	N	N
N	D	A	L	O	O	C
I	O	E	T	A	P	O
C	S	A	O	R	T	N

A path of letters is highlighted in blue: O, H, O, R, A, S, E, C, A, E, S, C, N, N, N, D, A, L, O, O, C, I, O, E, T, A, P, O, C, S, A, O, R, T, N. A blue arrow points from the 'L' in the third row, fourth column to the 'O' in the third row, fifth column.

Tabela Espartana

- Tabela comum de linhas e colunas (mXn);
- chave é dada pelas dimensões da tabela.

Ex:

- texto = **ataquem o inimigo pelo desfiladeiro**
- chave = 7 x 5

A	T	A	Q	U
E	M	O	I	N
I	M	I	G	O
P	E	L	O	D
E	S	F	I	L
A	D	E	I	R
O	A	B	C	D

- texto criptografado =

A E I P E A O T M M E S D A A O I L F E B Q I G O I I C U N O D L R D

Criptoanálise

cryptos = secreto

analysis = decomposição

- guerra eterna entre criptografia e criptoanálise;

Ex: criptoanálise da tabela espartana

Texto a decifrar:

**ODHX ROCAETARONGADAMTAFES AESEZANCE
IHB**

- fragilidade: matriz $m \times n$

- $N = m \times n$

- logo m e n são divisores de N ;

- Resolvido pelo método da força bruta – tentativa:

- experimentar todas as possibilidades de chave na tentativa de produzir a decifragem (força bruta).

- funciona para códigos fracos ou quando o espaço de chaves é muito restrito.

N (texto a decifrar) = 36

- Temos que:

1 x 36 = 36

2 x 18 = 36

3 x 12 = 36

4 x 9 = 36

6 x 6 = 36

- testando todas as possibilidades baseados na exclusão, chegamos a conclusão de que a chave é 6x6, portanto:

O	C	O	M	A	N
D	A	N	T	E	C
H	E	G	A	S	E
X	T	A	F	E	I
R	A	D	E	Z	H
O	R	A	S	A	B

- A frase decifrada é: O comandante chega sexta feira dez horas

Substituição

- troca dos símbolos que constituem a mensagem por outros;
- existem 3 tipos de substituição:
 - simples (ou monoalfabética): um por outro;
 - homofônica: um por vários;
 - polialfabético: usa várias cifras de substituição simples.

Ex:

- Código de César;
- Cifra de Vigenère.

Substituição simples (ou monoalfabética)

- troca de um símbolo por outro;
- não necessita respeitar as letras do alfabeto e pode usar símbolos arbitrários.
- pode-se sofisticar utilizando-se palavra-chave;

Ex:

Código de César

- 100 a 44 A. C.;
- correspondência militar;
- chave de substituição simples;
- Código de César original: chave = 3;

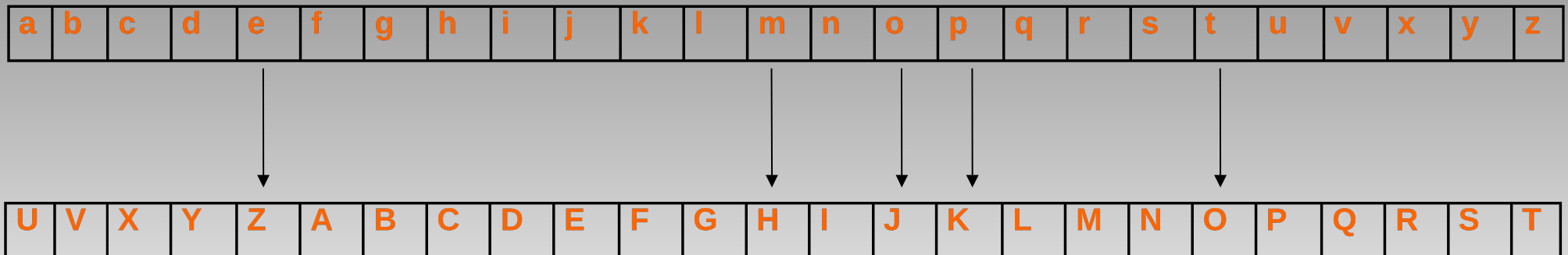
Código de César:

- substituição de cada letra do alfabeto por uma letra transladada algumas posições à frente;
- emissor e o destinatário antecipadamente combinam trocar mensagens com este algoritmo;
- escolher uma chave, que deve ser um número entre 1 e 24 (ou o tamanho do alfabeto -1);
- possibilidade = $25 ! - 1$

Ex:

chave escolhida = 5

texto a ser codificado = tempo



texto codificado:

O Z H K J

Código de César com palavra-chave

- Sofisticação posterior do Código de César;
- palavra-chave geralmente é constituída por uma ou duas palavras sugestivas para o contexto;
- não se usa repetição de símbolo na palavra-chave;
- escrevem-se as letras na seqüência do alfabeto, pulando aquelas já utilizadas na palavra-chave.

Ex:

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

- texto a ser cifrado: c o r a g e m
- palavra-chave = V I T O R I A
- texto cifrado: T K N V B R H

Criptoanálise do Código de César

- método da análise de frequências;
- ocorreu durante o século IX;
- criado pelo matemático árabe Al-Kindy;
- derrubou totalmente a criptografia baseada em substituição monoalfabética;
- obrigou os cientistas ligados à criptografia a buscarem novas formas de cifrar dados.

Análise de freqüências

- periodicidade de ocorrência de cada letra é distinta;
- em qualquer texto:

$$NT = Na + Nb + Nc + \dots + Nx + Ny + Nz$$

- e sua freqüência é dada por:

$$Fa = NL / NT$$

- na língua portuguesa a freqüência média aproximada de ocorrência de cada letra em textos longo é:

a	e	o	p, r, s	i, n	d, m, t	u, c, l	b, f, g, h, j, v, x, z
14,5%	13%	11,5%	8%	6%	5%	4,5%	menor que 3%

Texto para decifrar pela análise de frequência

EXCJLOHLNFLJLZ MCXJNCTNTXJMCXHXFZLT
NNCILINTNEOFZNAOTNTNEOFZNOFUNFRONM
CXIOTNMCXLJNFLJFNLHINDXEENOJMCXNELI
MCXJLFZLJMCXUQLIXJFNMCXQNJ NITXJUNV
CXOINJ NJLEPINTNJPNFNFXOINJTXPNOBLTL
JQNINFSNOJRLELJNLPXQLJLJ TONJTTLTXJGL
FHNITN XBOJHXFRONIXJGOINNNQENOF LRXF
RONRLELGXIUCEXJ NUQLILENIXQNV LJXIXFL
LRXCCEENFHLNDCQNTLLECFTLCEJLFZLTLCI
NTLNAOTN CEZOFLTX NELIMCXNCILINJMCXJL
QMCXAOTNMCX FLOHXJTXEXQLTONFNM CXQN
TLRX NQXVIONFNM CXQXOFVXFCLULQVNILRX
CPLITNTLTX XJHIXQNJN HXIINTXNILENJ RZX
ONNJ LFTNJ PXOSNFTLNNIXONXNQCNPXOSN
FTLLENIRNJOEOILT XNPIXC

Solução:

- contar o total de letras: 503

- efetuar a análise da frequência das repetições de cada letra:

Símbolos	N	L	X	J	F	I	T	O
Frequências	16,5%	11,3%	11,1%	7,3%	6,5%	6,5%	6,5%	6,1%

- comparar com a frequência do alfabeto em questão:

a	e	o	p, r, s	i, n	d, m, t	u, c, l	b, f, g, h, j, v, x, z
14,5%	13%	11,5%	8%	6%	5%	4,5%	menor que 3%

- Comparativo das duas tabelas acima:

Cifras	N	X, L	J, F, I, T, O
Letras	a	e, o	r, s, i, n, d, m, t, p

- resolver a dúvida entre as letras X e L;

- uma solução é buscar no texto seqüência que cifra a palavra “que” (muito comum na língua portuguesa);

EXCJLOHLNFLJLZ **MCX**JNCTNTXJ**MCX**HXFZLTNNCILINTN
EOFZNAOTNTNEOFZNOFUNFRON**MCX**IOTN**MCX**LJNFLJF
NLHINDXEENOJ**MCX**NELI **MCX**JLFZLJ**MCX**UQLIXJFN**MCX**
QNJ NITXJUNVCXOINJ NJLEPINTNJPNFNFXOINJTXPNOB
LTLJQNINFSNOJRLELJNLPXQLJ LJ TONJTTLTXJGLFHNTN
XBOJHXFRONIXJGOINNNQENOF LRXF RONRLELGXIUCE
XJ NUQLILENIXQNV LJXIXFLLRXCC EENFHLNDCQNTLLEC
FTLCEJLFZLTL CINTLNAOTN CEZOFLTX NELI**MCX**NCILINJ
MCXJLQ**MCX**AOTN**MCX**FLOHXJTXEXQLTONFN**MCX**QNTL
RX NQXVIONFN**MCX**QXOFVXFCLULQVNILRXCP LITNTLT X
XJHIXQNJN HXIINTXNILENJ RZXONNJ LFTNJ PXOSNFTL
N NIXONXNQCNPXOSNFTLLENIRNJOE OILT XNPIXC

- **MCX** aparece 14 vezes, logo é forte crermos que substitui o “que”, e que portanto “X” corresponde a “e”, e que que “M” e “C” estão cifrando, respectivamente, as letras “q” e ”u” ;

- Logo podemos repensar melhor nossa tabela comparativa da seguinte forma:

Cifras	N	X	L	C	M	J, F, I, T, O
Letras	a	e	o	u	Q	r, s, i, n, d, m, t, p

- a seguir podemos tentar definir as letras “a”, “e”, “o”, portanto buscaremos os dígrafos “nha” e “nho”:

EXCJLOHLNFLJLZ MCXJNCTNTXJMCXHX **FZL** TNNCILINTN
EO **FZN** AOTNTNEO **FZN** OFUNFRONMCXIOTNMCXLJNFLJF
NLHINDXEENOJMCXNELI MCXJL **FZL** JMCXUQLIXJFNM CX
QNJ NITXJUNVCXOINJ NJLEPINTNJPNFNF XOINJTXPNOB
LTLJQNINFSNOJRLELJNLPXQLJ LJ TONJTTLTXJGLFHNITN
XBOJHXFRONIXJGOINNNQENOF LRXFRONRLELGXIUCE
XJ NUQLILENIXQNV LJXIXFLLRXCC EENFHLNDCQNTLLEC
FTLCEJL **FZL** TLCINTLNAOTN CEZOFLTX NELIMCXNCILINJ
MCXJLQMCXAOTNMCX FLOHXJTXEXQLTONFNM CXQNTL
RX NQXVIONFNM CXQXOFVXFCLULQVNILRX CPLITNTLTX
XJHIXQNJN HXIINTXNILENJ RZXONNJ LFTNJ PXOSNFTL
N NIXONXNQCNPXOSNFTLLENIRNJOE OILT XNPIXC

- A busca revela na mensagem cifrada duas vezes FZN e três vezes FZL;
- logo, possivelmente temos que “nha” e “nho” têm como cifra, respectivamente, FZN e FZL;
- Portanto é possível avançar um pouco mais e melhorar a Tabela, ficando assim:

Cifras	N	X	L	M	C	F	Z	J, I, T, O
Letras	a	e	o	q	u	n	h	r, s, i, d, m, t, p

- agora vamos buscar cifras para os blocos “as”, “os” e “es” que formam a maior parte dos plurais;
- Percebemos que uma das cifras entre J, I, T, O deve representar a letra “s”;

- Olhando novamente o texto vamos encontrar a ocorrência de NJ e XJ, cada um com 12 e 11 vezes, respectivamente, e LJ com 9 vezes;
- isto fortalece que J deve estar cifrando a letra “s”;
- Conseguimos portanto decifrar 8 letras: a, e, o, q, u, n, h, s
- este conjunto de letras representa, com forte indício, a cifragem de mais de 40% das letras do alfabeto;
- o trabalho agora é substituir no texto cifrado as cifras N, X, L, M, C, F, Z, J, pelas letras a, e, o, q, u, n, h, s;
- em seguida, tentar dar sentido ao texto remanescente que permanece cifrado, isto não é fácil, mas ao final teremos:

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

- seguindo a tabela e decifrando o texto, teremos:

Meus Oito Anos (*)

**Oh! Que saudades que tenho
Da aurora da minha vida, da minha infância querida
Que os anos não trazem mais!
Que amor, que sonhos, que flores,
Naquelas tardes fagueiras
À sombra das bananeiras,
Debaixo dos laranjais!
Como são belos os dias
Do despontar da existência!
Respira a alma inocência
Como perfumes a flor;
O mar é lago sereno,
O céu um manto azulado,
O mundo um sonho dourado,
A vida um hino d'amor!
Que auroras, que sol, que vida,
Que noites de melodia
Naquela doce alegria,
Naquele ingênuo folgar!
O céu bordado d'estrelas,
A terra de aromas cheia,
As ondas beijando a areia
E a lua beijando o mar!**

Casimiro de Abreu

Código de substituição homofônica

- tentativa de reação à análise de frequências;
- associar a cada consoante um símbolo;
- para cada vogal quatro ou cinco símbolos distintos;
- para dificultar a decifragem, introduziu-se símbolos que nada significavam;

b	c	d	f	g	h	j	k	l	m	n	p	q	r	s	t	v	x	y	z
U	X	T	H	\$	N	∅	A	V	∅	Π	E	λ	P	L	Q	Σ	S	Y	I
Letras	a				e			i			o			u		nulos			
Cifras	R	D	&	#	@	Ω	B	F	⊕	M	\$	∇	Z	⊥	O	C	Δ	J, ∪, α, β	

- cifragem: `enviem tanques hoje` ⇒ `@ΠJΣFΩ∅αQRΠλOB LNV$∅@`

- apesar de várias cifragens, as fragilidades persistiam com os códigos homofônicos.

Pergunta???

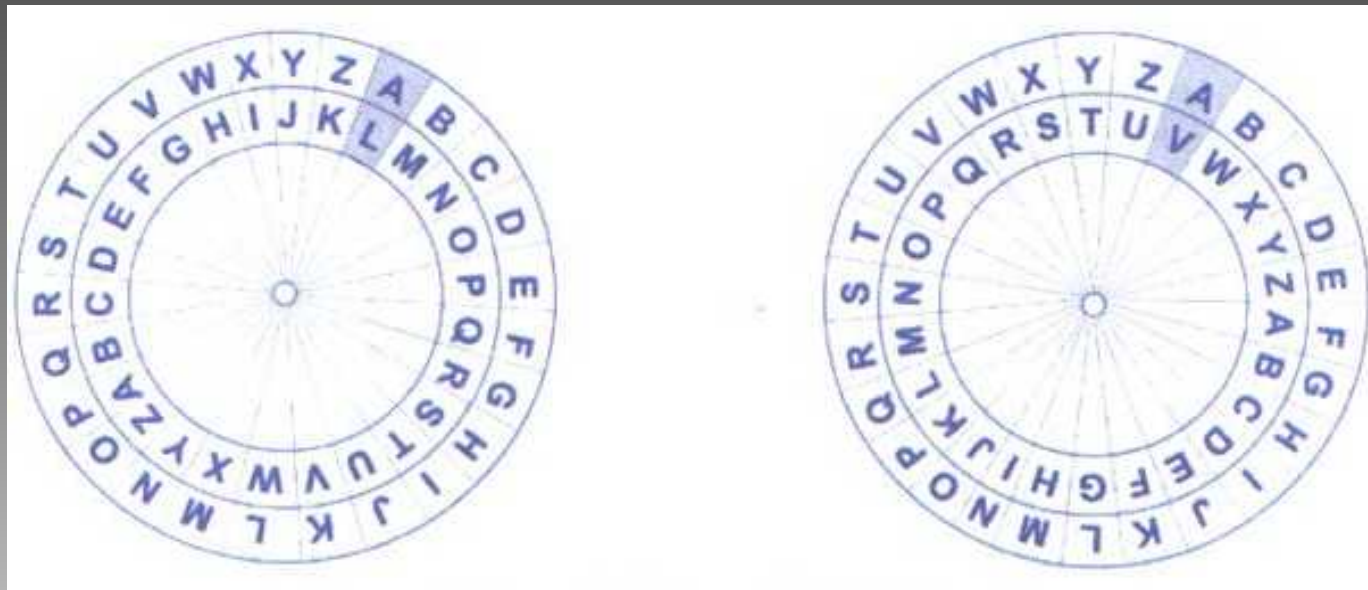
por que não associar de uma vez várias cifras distintas a cada letra?

Resposta:

- seria a solução evidente para uma fuga consistente da análise de frequências;**
- a chave que permite a cifragem e a decifragem deve também atender ao quesito usabilidade;**
- a criptografia, até o início do século XX, era usado essencialmente a serviço do comércio e principalmente militar, na trincheria durante a baltalha, com necessidade de decifrar rapidamente uma mensagem vital, o código teria de apresentar uma interface amigável.**

Código de substituição polialfabético

- alternativa a cifra monoalfabética;
- criado por Leon Battista Alberti, em 1470;
- primeira cifra polialfabética;
- pela primeira vez foi utilizado um processo mecânico;
- processo foi conhecido por “discos de Alberti”:



- o número de discos depende do tamanho da palavra-chave;
- as letras de ordem ímpar do texto original são cifradas usando A - > L;
- as letras de ordem par do texto original são cifradas usando A - > V;

Cifra de Vigenère

- criado para fugir à análise de frequências;
- criado por Blaise de Vigenère, em 1586;
- Foi chamada de “a cifra indecifrável”;
- durou aproximadamente 286 anos;

Cifra de Vigerère:

- sistema polialfabético ou de substituição múltipla;
- estrutura é definida por uma tabela;
- constituída por uma matriz quadrada de 26 linhas e 26 colunas.

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

Chave para a Cifra de Vigenère

- a chave pode ser qualquer palavra:
 - uma frase;
 - ou um conjunto arbitrário de letras;
 - não há impedimento para o comprimento da chave (número de letras distintas).

Ex:

- texto a ser cifrado: **armada submarina entrando no porto sábado**
- palavra-chave: **SEGREDO**

Mensagem original	a	r	m	a	d	a	s	u	b	m	a	r	i	n	a	e	n	t
Palavra chave	S	E	G	R	D	O	S	E	G	R	D	O	S	E	G	R	D	O
Mensagem cifrada	S	V	S	R	G	O	L	Z	H	E	D	G	B	R	G	V	Q	I
Mensagem original	r	a	n	d	o	n	o	p	o	r	t	o	s	a	b	a	d	o
Palavra chave	S	E	G	R	D	O	S	E	G	R	D	O	S	E	G	R	D	O
Mensagem cifrada	K	E	T	U	R	C	H	T	U	J	X	D	L	E	H	R	G	D

S V S R G O L Z H E D G B R G V Q I K E T U R C H T U J X D L E H R G D

A principal inovação do método de Vigenère:

- várias cifras para a vogal a;
- esta letra que aparece oito vezes na mensagem original;
- ela é cifrada de acordo com a ordem de aparecimento da letra, respectivamente, pelos códigos de César definidos pelas letras S, R, O, D, G, E, E, R;
- portanto, apesar da mensagem ser curta, usamos 6 códigos distintos para cifrar a letra de maior frequência de nosso alfabeto;
- O mesmo se aplica a todas as outras letras do alfabeto, todos tendo portanto vários códigos, praticamente impossibilitando humanamente a sua análise de frequências;
- **PROBLEMA**: por ser muito difícil cifrar e decifrar pelo Código de Vigenère, ele ficou quase 200 anos em desuso.

Criptanálise : O ataque de Babage à Cifra de Vigenère

- criado, em 1856, pelo matemático Inglês Charles Babage;
- foi uma das figuras científicas mais enigmáticas do século XIX;
- trabalhou no desenvolvimento de máquinas que hoje são reconhecidas como precursoras dos modernos computadores;
- assim como a análise de frequências, ao quebrar a cifra dita indecifrável, Babbage coloca de novo em xeque à criptografia;

Solução:

- identificar o tamanho da palavra-chave;
- utilizar, baseado no tamanho da palavra-chave, a análise de frequências;

Ou seja:

- 1º) identificar o comprimento m da palavra-chave que identifica o número de letras, sem repetição da palavra-chave;
- 2º) dividir a mensagem criptografada em m textos disjuntos e aplicar a cada um a análise de frequências.

Outros tipos de Códigos de criptografia

Cifra Playfair:

- substituir cada par de letras da mensagem original por outro par de letras (as cifras;
- uso de palavra-chave.

Cifra ADFGVX

- mais famosa cifra usada na Primeira Guerra Mundial;
- foi quebrada em situação dramática por Pavin, com o exército alemão nos calcanhares de Paris;
- exemplo clássico de código que mistura as duas grandes técnicas da criptografia clássica: substituição e transposição;
- chave simétrica que permite a cifragem e a decifragem também é híbrida, constando de duas partes, uma para cada processo.

Cifra ADFGVX

A estrutura da cifra é definida por uma tabela quadrada (7x7), com quarenta e nove entradas. Na primeira linha e primeira coluna a partir da segunda posição, aparecem, sequencialmente, as letras A, D, F, G, V, X que dão nome à cifra.

A posição correspondente à primeira linha e primeira coluna fica vazia.

As outras trinta e seis posições são preenchidas pelas vinte e seis letras do alfabeto e mais dez dígitos.

Note que como observado no início do Texto 1, para a cifra ADFGVX o alfabeto é o inglês com as letras.

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

Cifra ADFGVX

As posições para as letras e para os dígitos, dentro da tabela, são escolhidas de modo aleatório e constituem a parte da chave do código para a etapa caracterizada por substituição.

Atabela e preenchida pelos 26 caracteres do alfabeto e pelos 10 algarismos numericos.

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

Cifra ADFGVX

Exemplo:

Considerando a Tabela anterior que define parte da chave correspondente à etapa de substituição de um código ADFGVX. Usando a palavra GATO como parte da chave para a etapa de transposição, cifre a mensagem:

sigam a rota 29

Cifra ADFGVX

Fase de substituição

Nesta fase, cada letra ou dígito da mensagem original é substituída por um par de letras.

Cada letra ou dígito da mensagem original é substituída por um par da tabela.

Assim a mensagem:

sigam a rota 29

Fica assim:

FA AG DD AA FG AA GV AV XX AA FX GG

Esta fase corresponde a uma substituição monoalfabética, que pode ser quebrada por análise de frequência. Com o objetivo de tornar mais robusta a cifragem vem a segunda fase da cifragem.

Cifra ADFGVX

Fase de Transposição

Esta etapa corresponde a uma transposição orientada por uma palavra-chave.

Nesta etapa, partindo da mensagem já cifrada pela primeira fase promove-se um embaralhamento – uma transposição – das letras, com auxílio da segunda parte da chave que é a palavra GATO.

Cifra ADFGVX

Fase de Transposição

A regra para efetuar a transposição consiste em usar duas novas tabelas.

No topo da primeira tabela é escrita a palavra-chave GATO.

Em seguida, o texto cifrado é escrito em linhas nesta primeira tabela.

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

Cifra ADFGVX

Fase de Transposição

A primeira tabela tem suas colunas reorganizadas de modo que a palavra-chave continue no topo, mas as letras são escritas na ordem alfabética.

A	G	O	T
A	F	G	A
D	D	A	A
G	F	A	A
V	G	V	A
X	X	A	A
X	F	G	G

Cifra ADFGVX

Fase de Transposição

Finalmente, a mensagem cifrada corresponde ao texto que pode ser lido sucessivamente nas colunas da tabela anterior.

Logo teremos a mensagem “sigam a rota 29” finalmente codificada como:

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

Cifra ADFGVX

Cirptoanalise da Cifra ADFGVX

A primeira fase da cifragem corresponde a uma substituição monoalfabética, que pode ser quebrada por análise de frequência.

A segunda etapa refere-se a uma transposição, usando métodos que podem ser comparados aos da tabela Espartana que foi estudado anteriormente, portanto suscetível a quebra via análise fatorial.

A máquina Enigma e a II Guerra Mundial

- durante a II Guerra Mundial, a criptografia experimenta notável efervescência;
- grande parte motivada pela entrada em cena da máquina de cifras alemã denominada Enigma;
- os alemães apostaram fortemente sobre a eficiência do equipamento para vencer a guerra;

Criptoanálise do Enigma

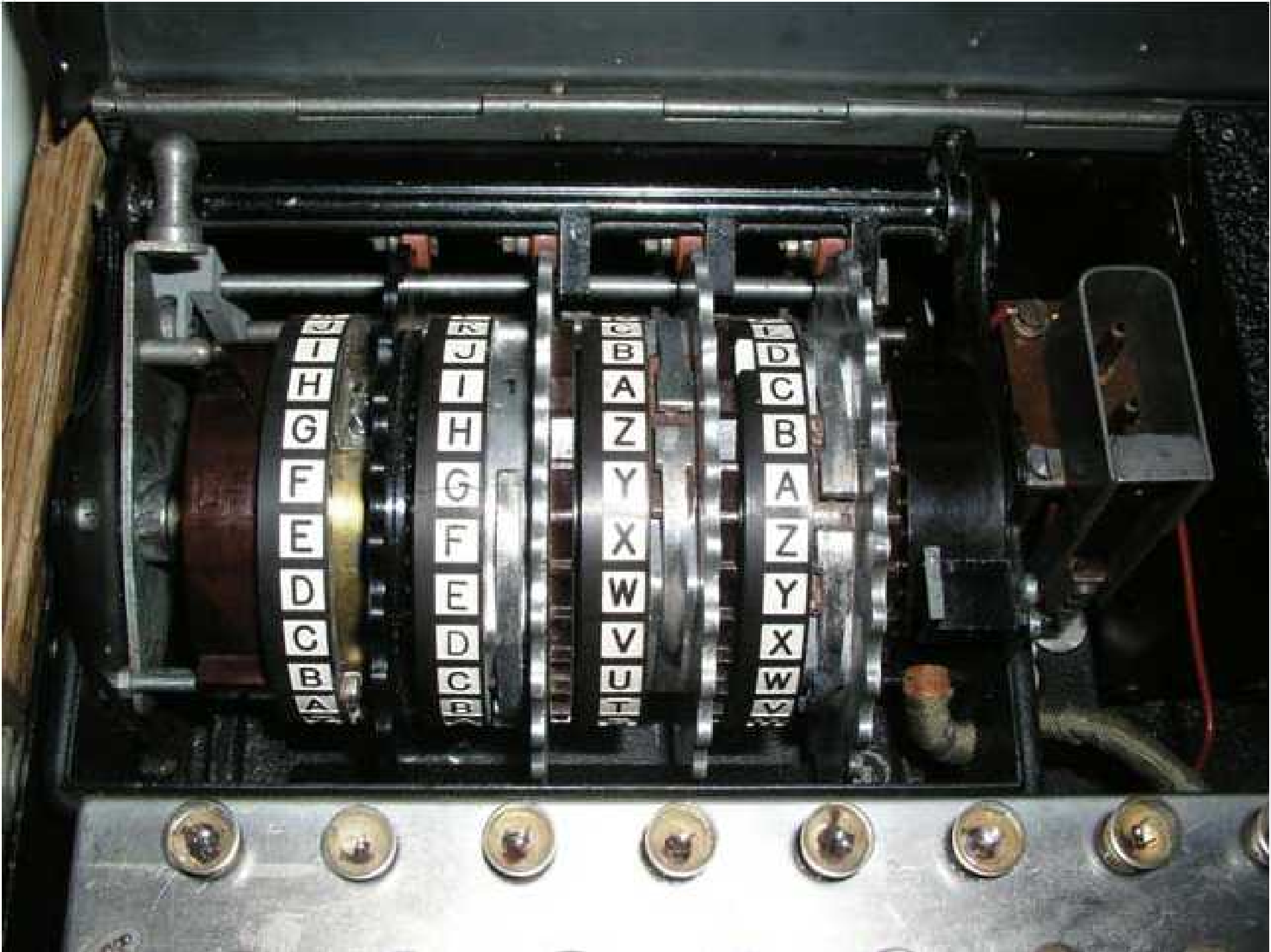
- envolveu poloneses e franceses em uma primeira fase e, finalmente, a parte significativa do trabalho foi realizada pelos ingleses;
- só foi possível porque os aliados conseguiram roubar uma máquina enigma e o seu livro de códigos; [U 571](#)
- Liderados por Alan Turing, construiu-se os primeiros computadores eletro-mecânicos Bomba e Colossus (programável e precursor dos computadores eletrônicos) (ENIAC). [ENIGMA](#)

Dificuldades na criptoanálise

- os alemães mudavam constantemente as configurações do ENIGMA;
- as chaves tinham validade mensal;
- a máquina ENIGMA era constantemente melhorada;
- acréscimo de mais dois misturadores, incrementando, de modo impressionante, o número de chaves possíveis;
- representa um divisor de águas entre a criptografia clássica e a moderna – a criptografia antes e depois da existência do computador;
- representou o estágio mais avançado a que se pode chegar com as máquinas de cifrar, com base exclusivamente mecânica e com a utilização de corrente elétrica;
- inspirado nos discos de Alberti;
- Os discos são o princípio básico dos misturadores, que são o coração do enigma;







Estrutura

- teclado;
- painel luminoso;
- câmara com misturadores;
- refletor;
- painel frontal com cabos elétricos;

Combinações de cifragens

- três misturadores e com 26 posições:

$$26 \times 26 \times 26 = 17.576$$

- são 6 posições distintas para os 3 misturadores:

$$6 \times 17.576 = 105.456$$

- possibilidade de realizar um máximo de 13 conexões entre o teclado e os misturadores através do painel frontal:

+ de 1.000.000.000 de combinações possíveis

1000 Enigmas -> 4 chaves/m -> 24 h/dia - não conseguiriam verificar todas as chaves possíveis nem em 900 milhões de anos

Criptografia clássica:

- necessita do conceito de chave simétrica ou chave secreta;
- a chave usada para cifrar uma mensagem é a mesma usada para decifrar;
- nesse aspecto reside a grande fragilidade do método;
- é necessária uma troca prévia da chave entre emissor e receptor antes do início do fluxo de mensagens;
- o risco de interceptação da chave é grande;
- esta pode ser lida durante a transmissão, sem que os agentes que promovem a troca tomem conhecimento;
- em 1977, surge o conceito de chave assimétrica ou chave pública;
- dividiu a criptografia em antes e depois deste evento.

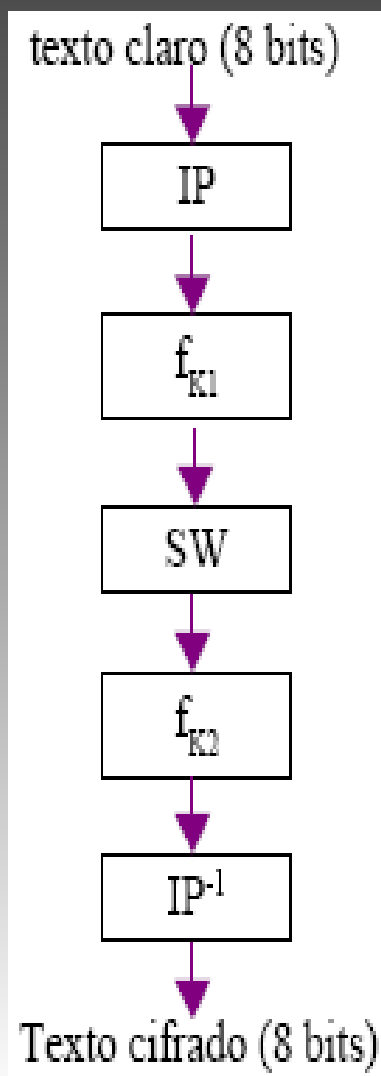
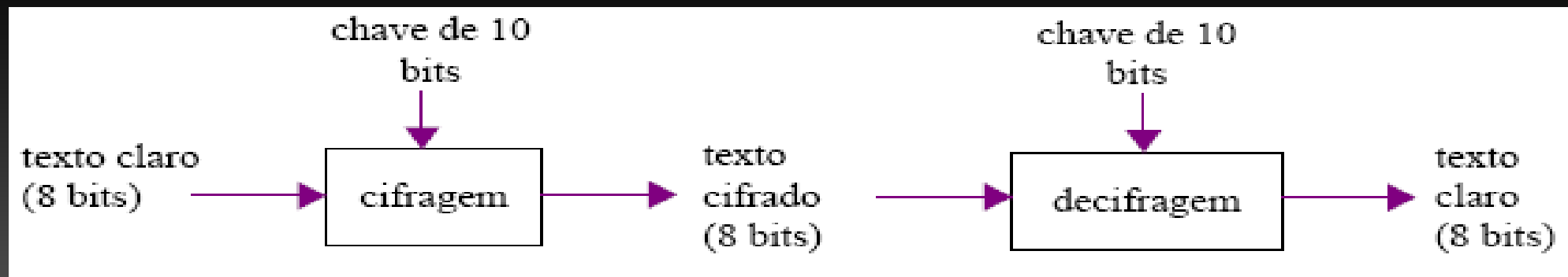
Criptografia moderna

- era digital;
- baseado em algoritmos;

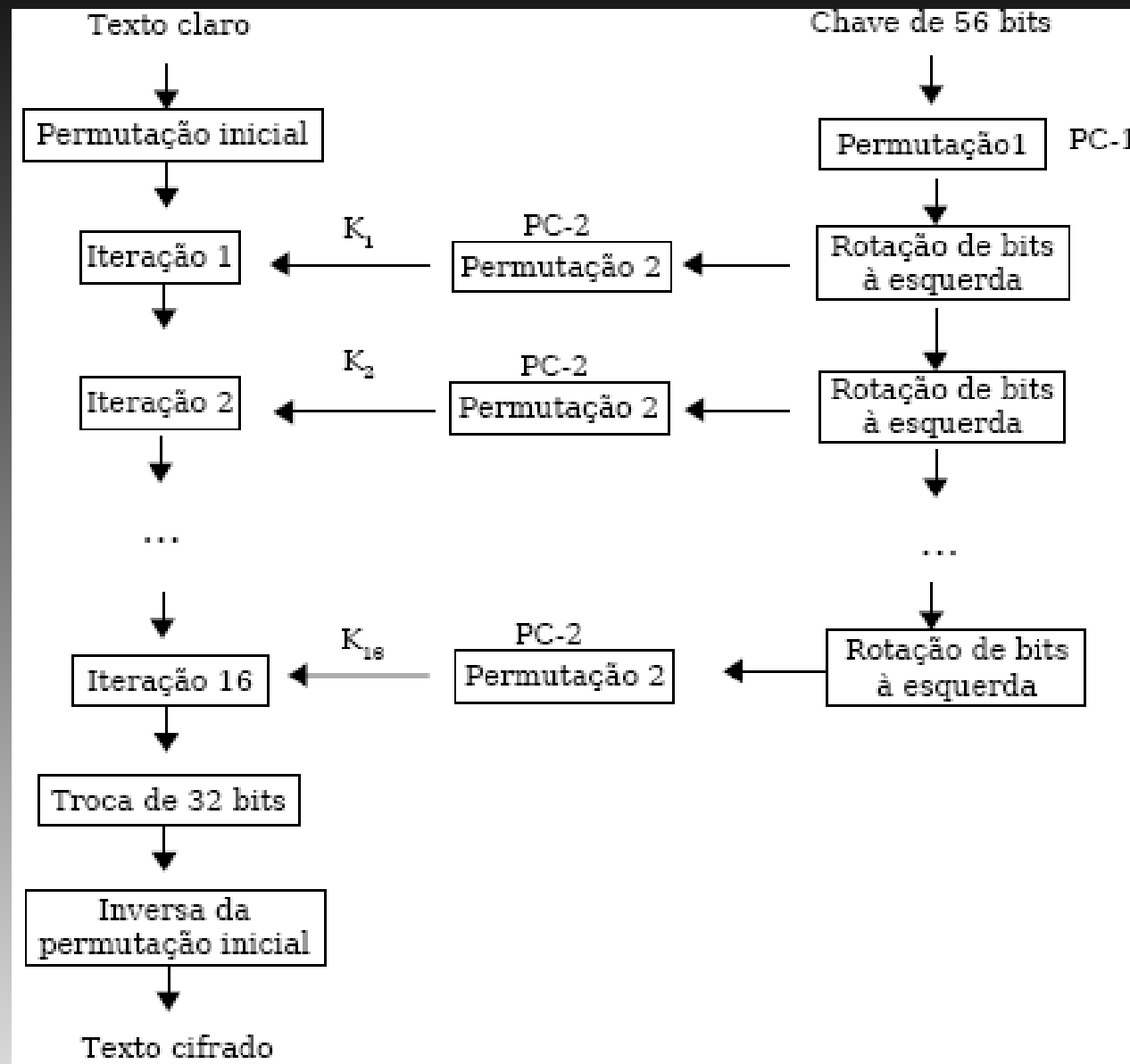
Algoritmo DES

- IBM, 1974 (1960);
- foi adotado como padrão nos Estados Unidos pela NSA;
- A NSA (National Security Agency) diminuiu o a dimensão da chave;
- apesar das restrições da NSA, o DES pode alcançar 2^{56} chaves distintas;
- É o algoritmo criptográfico mais usado no mundo (incluindo suas variações, como o 2DES e 3DES);

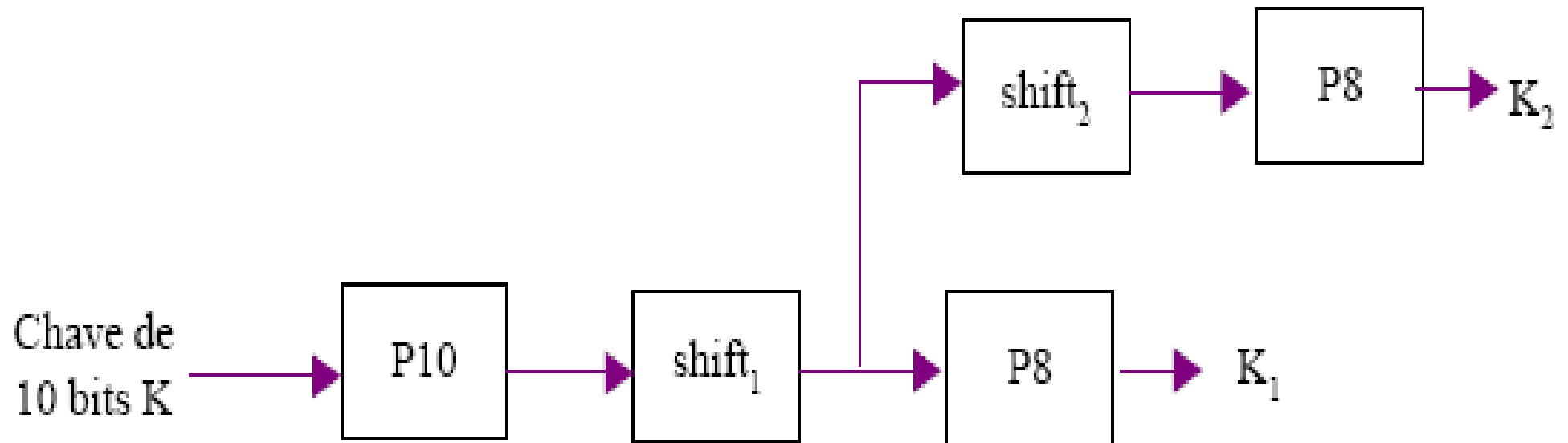
Algoritmo DES simplificado (S-DES)



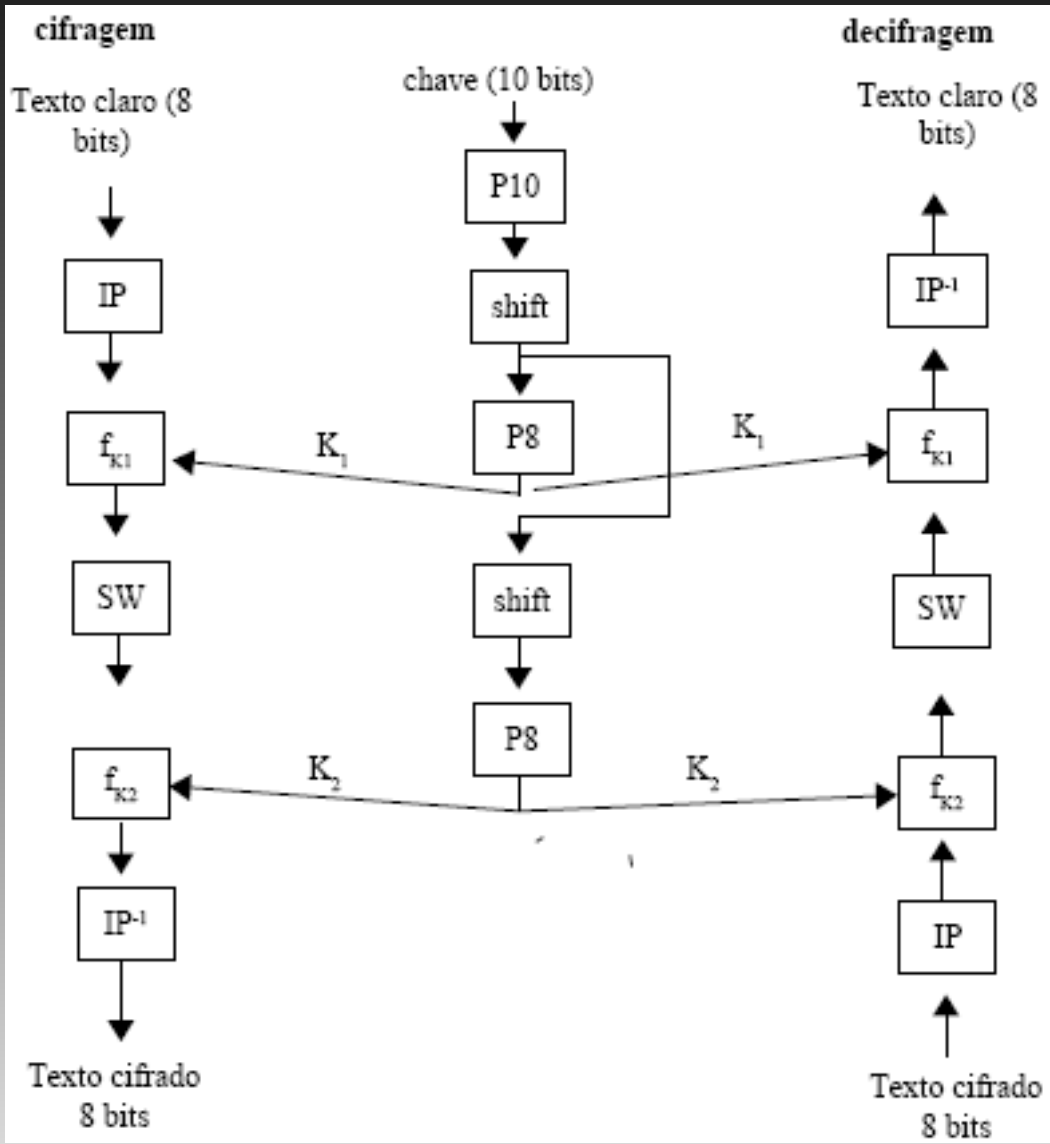
Algoritmo DES simplificado (S-DES)



Geração de chaves no S-DES



Decifragem de chaves no S-DES



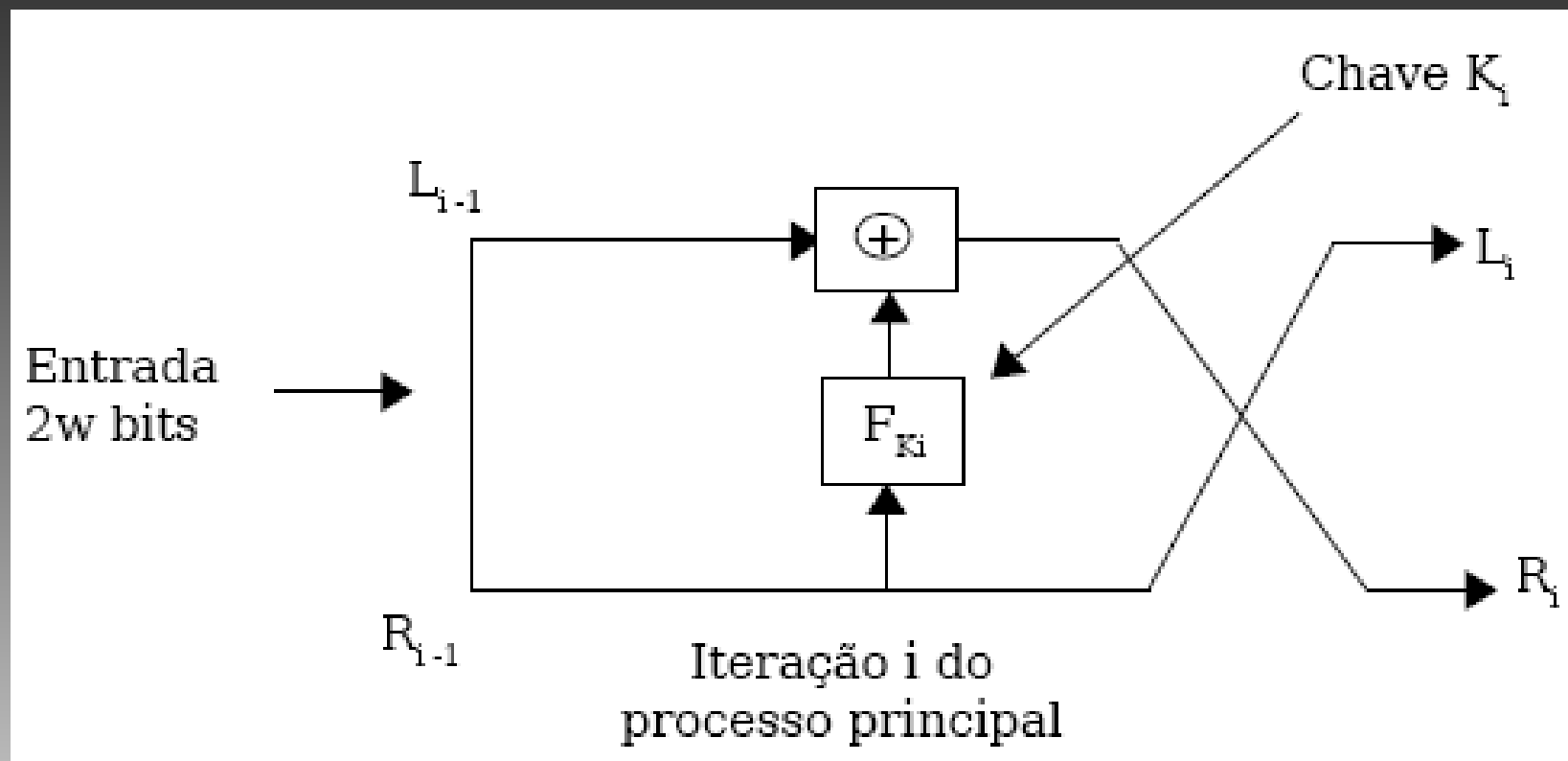
Quebra do algoritmo DES

- em 1977, um pesquisador chamado Wilner projetou uma máquina que custaria cerca de US\$ 100.000,00, na época, e levaria cerca de 6 horas para encontrar a chave correta para um texto criptografado com o DES;
- em 1998, a equipe de John Gilmore, no EFF (Electronic Frontier Foundation) construiu uma máquina projetada para analisar o espaço de chaves do DES;
- em junho de 1998 eles anunciaram ter quebrado um código DES, com esta máquina somente, em 46 horas;
- a máquina é chamada DES Key Search Machine e é capaz de testar 90 bilhões de chaves por segundo;
- neste ponto ficou provado que o DES não era mais seguro e que algoritmos mais fortes deveriam substituí-lo como padrão. O feito da EFF derrubou de vez o DES que, mesmo com sua chave de apenas 56 bits, reinou por 2 décadas como padrão de criptografia simétrica.



DES Key Search Machine

Algoritmo Cifra de Feistel



Criptografia Assimétrica

- após a quebra do DES em poucas horas, viu-se a necessidade de novo suspiro para a criptografia;
- criou-se então o conceito de chave pública, que seria uma nova era na criptografia;
- foi criado por Whitfield Diffie em 1975;
- idéia:
 - um par de chaves, uma delas deve ser divulgada (a chave pública) enquanto que a outra que deve ser mantida em sigilo (a chave privada);
 - A chave pública é utilizada para criptografar a mensagem;
 - enquanto que a chave privada é utilizada para decifrar a mensagem.

Ex:

- inicia-se o processo quando ambos geram um par de chaves.
- Alice gera seu par:
 - CA = Chave pública de Alice
 - DA = Chave secreta de Alice
- enquanto Bob gera seu par:
 - CB = Chave pública de Bob
 - DB = Chave secreta de Bob
- a chave pública é divulgada um para o outro, ou para quem quiser;
- A chave privada são mantidas em segredo.

Processo:

- para enviar uma mensagem P a Alice, Bob usa a chave CA , produzindo o texto cifrado $CA(P)$;
- este é enviado por qualquer meio;
- Alice recebe a mensagem $CA(P)$ e usa sua chave secreta DA , obtendo

$$DA(CA(P))=P$$

- isto é, recupera a mensagem inicial.
- Não importa que o texto seja interceptado em trânsito, porque somente Alice conhece a chave secreta DA e pode decifrá-lo.

Esquema:

Alice	Bob
Gera par de chaves D_A, C_A . Divulga C_A	Quer enviar mensagem P para Alice.
	Usa chave pública de Alice e gera mensagem cifrada $C_A(P)$
Recebe $C_A(P)$	Transmite $C_A(P)$
Usa chave secreta D_A e recupera mensagem inicial. $P = D_A(C_A(P))$	

- caso algum hacker conseguisse interceptar toda a comunicações entre Alice e Bob saberia apenas a chave publica C_A e a mensagem cifrada $C_A(P)$, não poderia decifrar a mensagem pois não conhece D_A e o conhecimento de C_A não permite deduzir D_A .



F I M

Jiyan Yari

jeandems@gmail.com

