Criptografia II

Criptografia

António Santos

ISTEC

Tópicos

Cifra ADFGVX

	A	D	F	G	V	X
A	0	Q	9	Z	7	C
D	M	U	1	H	F	2
F	4	8	W	N	R	G
G	L	6	V	T	P	A
V	Y	3	D	5	E	K
X	J	S	I	O	B	X

Cifra ADFGVX

Mensagem: "Enviem tropas"
Mensagem criptografada:
VVFGGFXFVVFGDAGGFVXGGVGXVG

W	H	I	S	K	Y
V	V	F	G	G	F
X	F	V	V	F	G
D	A	G	G	F	V
X	G	G	V	G	X
V	G	A	A	A	A

Cifra ADFGVX

Mensagem: "Enviem tropas"
Mensagem criptografada:
VVFGGFXFVVFGDAGGFVXGGVGXVG

H	I	K	S	W	Y
V	F	G	G	V	F
F	V	F	V	X	G
A	G	F	G	D	V
G	G	G	V	X	X
G	A	A	A	V	A

Texto criptografado:
"VFAGGFVFVGGAGFFGAGVGVAVXDXVFGVXA"

Cifra de Vernam

$$c_i = p_i \oplus k_i$$

onde
p_i = digito binário na posição i do texto claro
k_i = digito binário na posição i da chave
c_i = digito binário na posição i do texto cifrado
$\oplus$ = operação ou - exclusivo (XOR)

Cifra de Vernam

chave: pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
texto claro: mr mustard with the candlestick in the hall
texto cifrado:
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Cifra de Vernam

chave: mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
texto claro: miss scarlet with the knife in the library
texto cifrado:
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Cifra de Vernam

Dificuldades fundamentais:

- Criar grandes quantidades de chaves aleatórias representa um problema prático. Qualquer sistema bastante utilizado poderia exigir milhões de caracteres aleatórios regularmente. O fornecimento de caracteres de fato aleatórios nesse volume é uma tarefa significativa.
- Ainda mais assustador é o problema da distribuição e proteção da chave. A cada mensagem a ser enviada, uma chave de mesmo tamanho é necessária para uso do emissor e do receptor. Assim, existe um problema gigantesco de distribuição de chave.

Técnicas de transposição

Mensagem: "meet me after the toga party"

m	e	m	a	t	r	h	t	g	p	r	y
e	t	e	f	e	t	e	o	a	a	t	

Mensagem encriptada: "MEMATRHTGPRYETEFETEOAAT"

Técnicas de transposição

Mensagem: attack postponed until two am x y z

Chave:	4	3	1	2	5	6	7
Texto claro:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Texto cifrado: "TTNAAPTMTSUOAODWCOIXKNLYPETZ".

Técnicas de transposição

Chave:	4	3	1	2	5	6	7
Entrada:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

SaÃda: "NSCYAUOPTTWLTMDNAOIEPAXTTOKZ"

Técnicas de transposição

01	02	03	04	05	06	07	08	09	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28

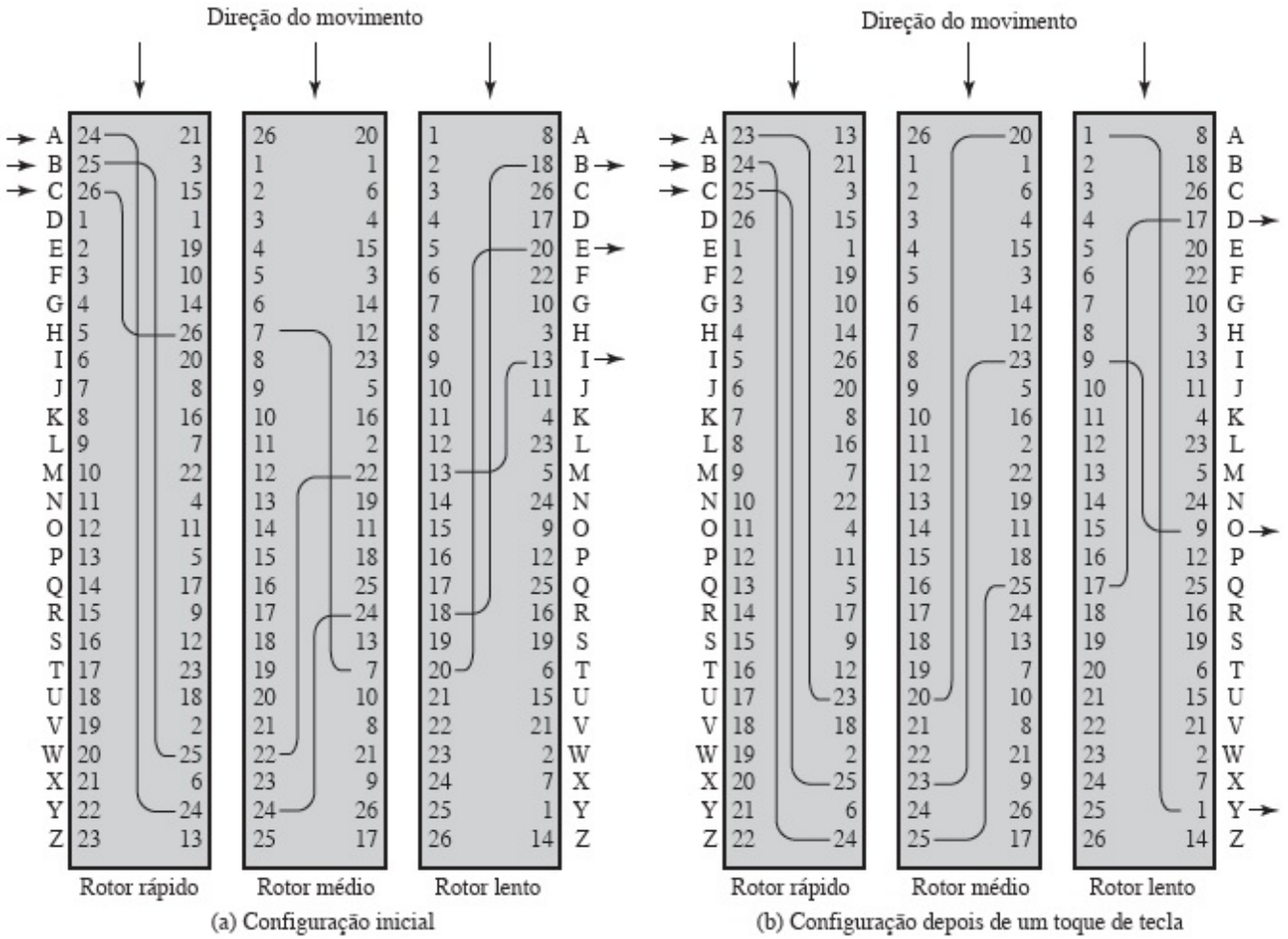
Técnicas de transposição

03	10	17	24	04	11	18	25	02	09	16	23	01	08
15	22	05	12	19	26	06	13	20	27	07	14	21	28

Técnicas de transposição

17	09	05	27	24	16	12	07	10	02	22	20	03	25
15	13	04	23	19	14	11	01	26	21	18	08	06	28

Máquinas de Rotor



Cifra de Hill

$$M(M^{-1}) = M^{-1}M = I$$

Cifra de Hill

$$A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$A^{-1} mod(26) = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

Cifra de Hill

$$AA^{-1} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} =$$

$$\begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix} =$$

$$\begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} mod(26) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Cifra de Hill

Texto claro: "paymoremoney"

Chave: $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Cifra de Hill

Pay:
$(15\ 0\ 24)K = (303\ 303\ 531)mod26 = (17\ 17\ 11) = RRL$
Texto Cirfrado: "RRLMWBKASPDH"