# Aula 2

# Criptografia Convencional

## *Técnicas Clássicas*

# Cifrador Playfair

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

***2 em 2 letras***

***Regras***

A senha não pode ter letra repetida
Letras repetidas usa-se caracter preenchedor. Ex: x
Letras na mesma linha trocadas pela seguinte
Letras na mesma coluna trocadas pela seguinte
Para o restante, usa-se a coluna do outro

Exemplo

```
departamento de informáticax
HAQLTUBKSOUN HA KOHMXRSQPISB
```

# Cifrador de HILL

Matemático Leslir Hill
em 1929

**de *m* em *m* letras**

$$m=3 \begin{cases} C_1=(k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26 \\ C_2=(k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26 \\ C_3=(k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26 \end{cases}$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

**C=KP**

- Texto Original
- Chave
- Texto Cifrado

Decriptografar
**$P = K^{-1}C$**

# Exemplo do Crifrador de Hill

```
p - L
a - N
y - S
m - H
o - D
r - L
e - E
m - W
o - M
n - T
e - R
y - W
```

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

$$K(15\ 0\ 24)^T = (375\ 819\ 486)^T \bmod 26 = (11\ 13\ 18)^T$$

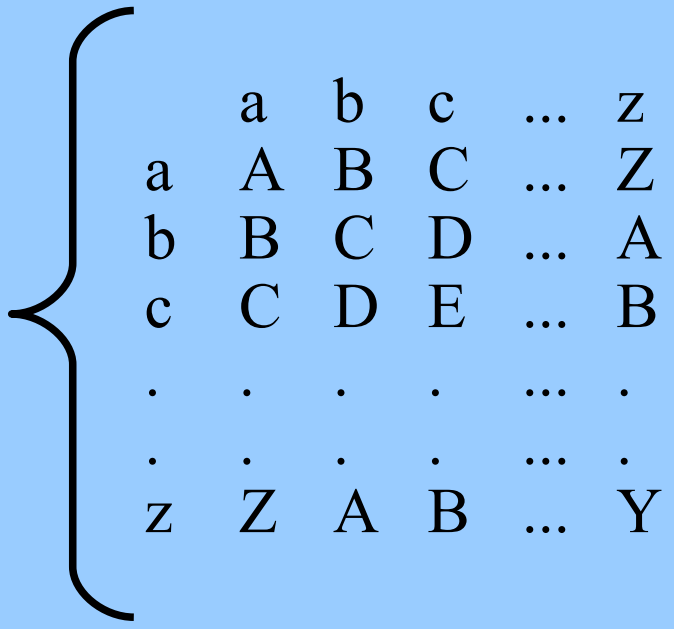
**p a y** → **L N S**

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \bmod 26$$

# Cifradores Polialfabéticos

Vigenère - **Auto Chave**
Vernam - xor

Joseph Mauborgne - **one-time pad**



| | a | b | c | ... | z |
|---|---|---|---|---|---|
| a | A | B | C | ... | Z |
| b | B | C | D | ... | A |
| c | C | D | E | ... | B |
| . | . | . | . | ... | . |
| . | . | . | . | ... | . |
| z | Z | A | B | ... | Y |

$c_i = p_i \oplus K_i$

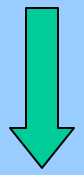
$p_i = c_i \oplus K_i$

Exemplo:

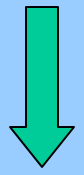
```
deceptivedeceptivedeceptive
wearediscoveredsaveyourself
ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

# Técnicas de Transposição - 1

**troqueascaixasapossinomeiodia**



**t o u a c i a a o s n m i d a**
**r q e s a x s p s i o e o i**



**touaciaaosnmidarqesaxspsioeoi**

# Técnicas de Transposição - 2

Chave: 4 3 1 2 5 6 7

Texto Original:

```
p e g u e a c
a i x a a z u
l a d a p e l
a m a n h a q
```

Texto Cifrado: GXDAUAANEIAMPALAEAPHAZEACULQ

# Técnicas de Transposição - 3

Chave: 4 3 1 2 5 6 7

Texto Original:

| | | | | | | |
|---|---|---|---|---|---|---|
| g | x | d | a | u | a | a |
| n | e | i | a | m | p | a |
| l | a | e | a | p | h | a |
| z | e | a | c | u | l | q |

Texto Cifrado: DIEAAAACXEAEGHLZUMPUAPHLAAAQ

# Análise da Transposição

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| p | e | g | u | e | a | c |
| a | i | x | a | a | z | u |
| l | a | d | a | p | e | l |
| a | m | a | n | h | a | q |

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| g | x | d | a | u | a | a |
| n | e | i | a | m | p | a |
| l | a | e | a | p | h | a |
| z | e | a | c | u | l | q |

*Pegue a caixa azulada pela manha q*

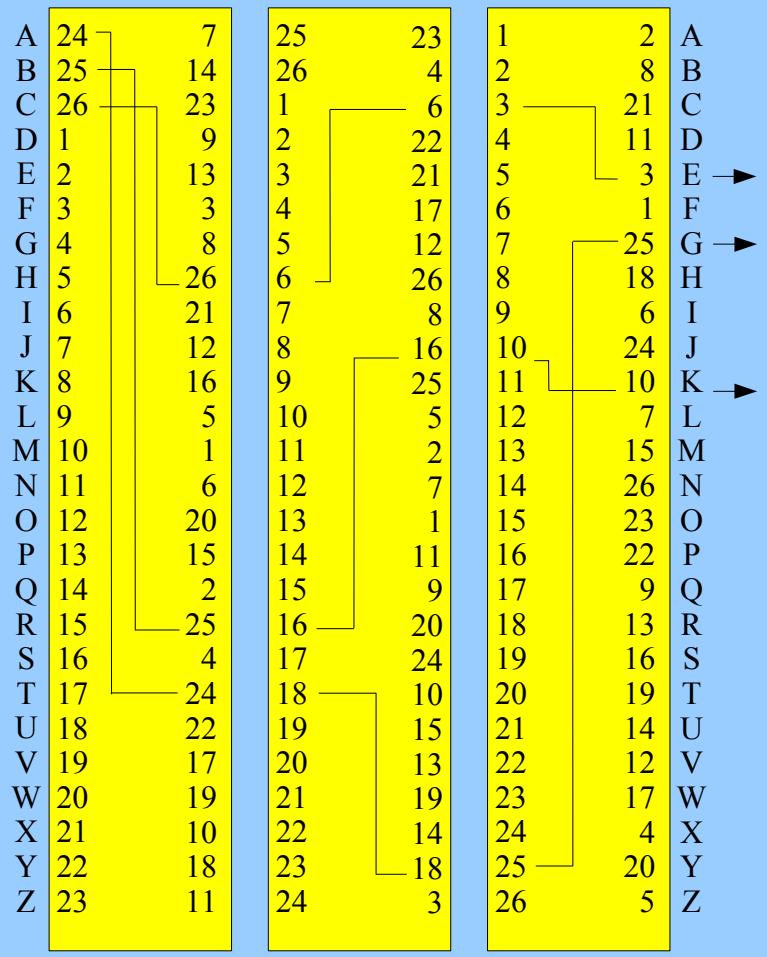
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

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

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

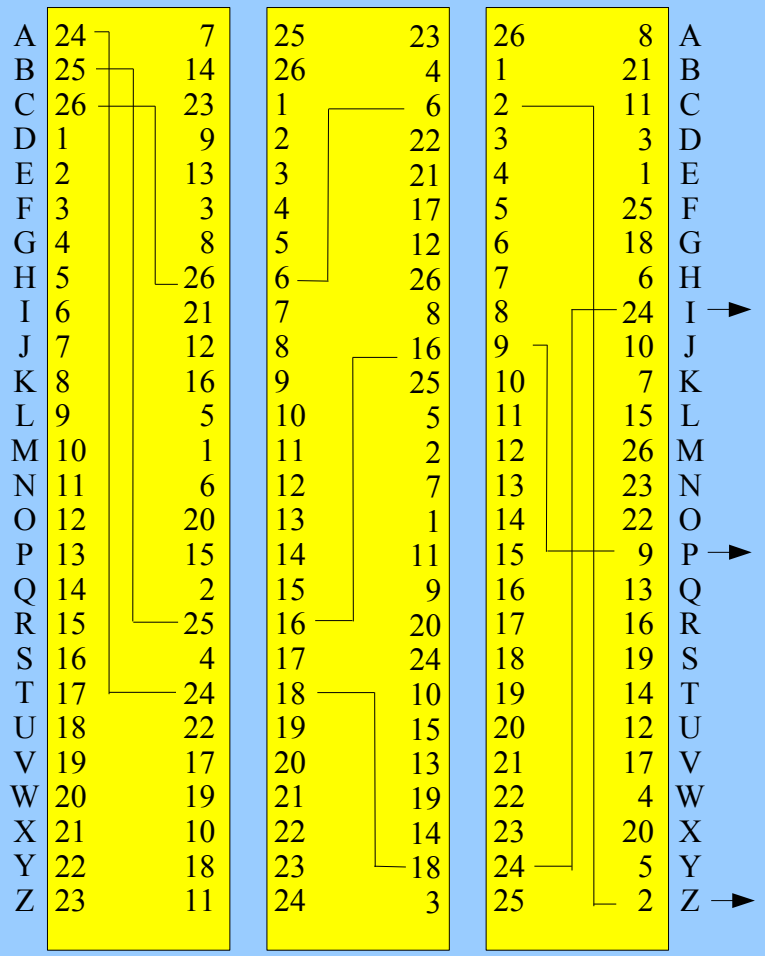
# Máquina de três rotores

A – I
B – P
C – Z




Configuração Inicial

A – G
B – K
C – E




Após uma letra selecionada

# Máquinas Rotoras

- 3 -> 26 x 26 x 26 = 17.576 diferentes alfabetos de substituição
- 4 -> 456.976
- 5 -> 11.881.376