# Criptografia Clássica

## Criptografia

António Santos

ISTEC

# Tópicos

# Estenografia

Trata-se do estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma de segurança por obscurantismo.

# Exemplos

- Escrita no crânio de um escravo.
- Mensagens engolidas.
- Escrita em ovos cozidos.
- Micro-perfuração.
- A "escrita simpática".
- Microponto.
- Grelhas de leitura.
- Variação de tipos impressos.

# Estenografia com imagens

| L | i | s | b | o | a |
|---|---|---|---|---|---|
| 01001100 | 01110011 | 01100111 | 01100010 | 01101111 | 0110( |

Se o bit menos significativo do primeiro pixel for 1, o valor é mantido, caso contrário é trocado para 1.

# Código Bacon para Textos

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | AAAAA | G | AABBA | N | ABBAA | T | BAABA |
| B | AAAAB | H | AABBB | O | ABBAB | U-V | BAABB |
| C | AAABA | I-J | ABAAA | P | ABBBA | W | BABAA |
| D | AAABB | K | ABAAB | Q | ABBBB | X | BABAB |
| E | AABAA | L | ABABA | R | BAAAA | Y | BABBA |
| F | AABAB | M | ABABB | S | BAAAB | Z | BABBB |

# Código Bacon para Textos

- Escreve-se o texto codificado
- Retira-se os espaços entre as palavras
- Escreve-se uma frase sem espaços com o mesmo tamanho
- Na frase escrita na posição onde tem os Bs na frase codificada coloca-se as letras a maiúscula
- Coloque os espaços na frase.

# Scitala Espartana

# Scitala Espartana

- 3 caracteres - $3 \times 2 = 6$
- 10 caracteres - $10! = 3628800$

# Cifra Kamasutra

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

# Cifra Kamasutra

Um alfabeto com $26$ caracteres
Número de possibilidades:
$26! = 403291461000000000000000000.$

# Quantas chaves são necessárias?

Dois utilizadores? - Uma chave.
Três? - Três chaves: AB, BC, AC.
Quatro? - Seis Chaves: AB BC CD AC AD BD.
n? - $\frac{n(n-1)}{2}$
População mundial de 6000 milhões de individuos.
Número:179999999997000000000.

# Cifra de Polibio

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

# Cifra de Polibio - numérica

| | 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 |

# Cifra de Cesar

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
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

# Cifra de Cesar

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 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 |

# Cifra de Cesar

Codificar: $C(X) = (X + 3)(mod 26)$
Descodificar: $C^{-1}(X) = (X - 3)(mod 26)$

# Cifra de Cesar - Geral

Codificar: $C(X) = (X + k)(modn)$
Descodificar: $C^{-1}(X) = (X - k)(modn)$

# Cifra de Cesar - Geral

$26! = 403291461126603635584000000$ alfabetos cifrados possíveis

# Cifra de Cesar - QWERTY

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

# Cifra de Cesar -ANTONIO

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

# Atbash Hebraico

| Alfabeto Original | a | b | c | d | e | f | g | h | i | j | k | l |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alfabeto Cifrada | Z | Y | X | W | V | U | T | S | R | Q | P | O |

# Atbash Hebraico

| Alfabeto Original | n | o | p | q | r | S | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alfabeto Cifrada | M | L | K | J | I | H | G | F | E | D | C | B | A |

# Al-Kindi

O sistema para resolver enigmas criptográficos:
Procurar caracteres mais frequentes tendo em atenção a frequência com que aparecem e a frequência da lingua.
Procurar palavras frequentes.

# Frequência

| Letra | P | Letra | P | Letra | P | Letra | P |
|---|---|---|---|---|---|---|---|
| A | 14.63% | H | 1.28% | O | 10.73% | V | 1.67% |
| B | 1.04% | I | 6.18% | P | 2.52% | W | 0.01% |
| C | 3.88% | J | 0.40% | Q | 1.20% | X | 0.21% |
| D | 4.99% | K | 0.02% | R | 6.53% | Y | 0.01% |
| E | 12.57% | L | 2.78% | S | 7.81% | Z | 0.47% |
| F | 1.02% | M | 4.74% | T | 4.34% | | |
| G | 1.30% | N | 5.05% | U | 4.63% | | |

**Tabela:** Frequências relativas das letras na lingua Portuguesa

# Frequência

- As vogais ocuparão cerca de $49\%$ do texto.
- Somente o "a"e "e"são identificados com relativa confiabilidade, porque se destacam muito dos demais. De fato, entre as duas vogais, elas ocupam $27,20\%$ da mensagem.
- As letras de alta frequência representam $63,50\%$ do total.
- As consoantes mais frequêntes: s, r, n, d (cerca de $24,38\%$).
- As seis letras menos frequentes: w, j, z, x, y e k (pouco mais de 1

# Cifras homofónicas

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

# cifras monoalfabéticas

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

# cifras polialfabéticas - Alberti

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Original | 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 |
| Cifrado 1 | F | R | J | O | Y | D | I | Q | T | Z | S | L | M | E | U | N | B | K | W | A | H | P | C | X | G | V |
| Cifrado 2 | H | T | R | V | Z | D | I | Q | J | Y | P | E | L | M | U | B | N | K | A | W | F | S | X | C | G | O |

# Palavra por código

Flandres $\leftarrow \oplus$
Rei de França $\leftarrow \otimes$
Rainha da Inglaterra $\leftarrow$
Rio Sena $\leftarrow \aleph$
Rainha da Escócia $\leftarrow \Phi$
Almirante $\leftarrow \upsilon$
Capturar $\leftarrow$ 13
Matar $\leftarrow$ 34
hoje $\leftarrow$ 45
manha $\leftarrow$ 56
atravessar $\leftarrow$ WD

# Palavra por código

"Capturar o rei da França e atravessar o Sena"
tranforma-se em
"13-⊗-WD-א"

# Tabela de Vigenére

| 0 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 |
| 2 | 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 |
| 3 | 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 |
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| 10 | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 11 | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| 12 | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 13 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 14 | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |

# Exemplo Vigenére com Chave

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Texto Original | O | E | X | E | R | C | I | T | O | E | S | T |
| Palavra-Chave | A | Z | U | L | A | Z | U | L | A | Z | U | L |
| Alfabeto Cifrada | O | D | R | P | R | B | C | X | O | F | M | X |

# A Cifra de Gronsfeld

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 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 |
| 1 | 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 |
| 2 | 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 |
| 3 | 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 |
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | 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 |

# Exemplo

| Mensagem | C | R | I | P | T | O | G | R | A | F | I | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Chave | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 |
| Mensagem Cifrada | F | W | P | A | G | F | Z | O | C | H | L | F |

# Cifra de Playfair

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

# Cifra de Playfair

1. Dividir em pares de letras ou digitos (anagramas).
2. As duas letras de todos os anagramas devem ser diferentes,
3. Inserir "x"adicional quando necessário para quebrar a igualdade ou para criar pares

# Cifra de Playfair

1. Mesma linha $(a_{i,j}, a_{i,k}) \longrightarrow (a_{i,j+1}, a_{i,k+1})$
2. Mesma coluna $(a_{i,k}, a_{j,k}) \longrightarrow (a_{i+1,j}, a_{j+1,k})$
3. Nenhuma das anteriores $(a_{k,i}, b_{j,s}) \longrightarrow (a_{k,s}, b_{j,i})$

# Exemplo

Codificar "ISTTU"com a chave CAIRO:

- Expressa-se a mensagem em diagramas: IS Tx TU;
- O "I"cifra-se como "E"(segunda regra);
- O "S"cifra-se como "X"(segunda regra);
- O "T"cifra-se como "S"(terceira regra);
- O "X"cifra-se como "Y"(terceira regra);
- O "T"cifra-se como "U"(primeira regra);
- O "U"cifra-se como "P"(primeira regra);

E a mensagem encriptada seria "EXSYUP".