

<http://www.Criptomuseum.com/Cripto/lorenz/sz40>

# CRIPTOGRAFIA

# Criptografia: terminologia (1/2)

2

- Criptografia
  - Arte ou ciência de escrever de forma escondida
    - do Grego *kryptós*, escondido + *graph*, radical de *graphein*, escrever
  - Foi inicialmente usada para tornar a informação confidencial
    - Compreensível apenas para alguns
- Esteganografia
  - Semelhante, mas tecnicamente diferente
    - do Grego *steganós*, escondido + *graph*, radical de *graphein*, escrever
  - É usado para referir a camuflagem de informação
- Criptanálise
  - Arte ou ciência de quebrar sistemas criptográficos ou de revelar informação criptografada

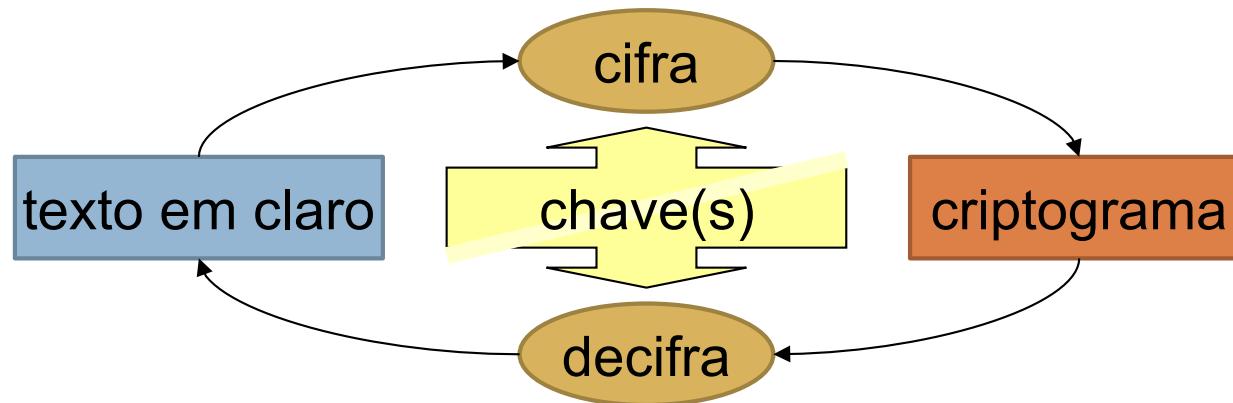
# Criptografia: terminologia (2/2)

3

- Cifra
  - Técnica criptográfica concreta
  - Transformação criptográfica de informação
- Operação de uma cifra
  - cifra (ou cifragem): texto em claro → criptograma
  - decifra (ou decifragem): criptograma → texto em claro
- Algoritmo: forma pela qual a informação é transformada
- Chave: parâmetro do algoritmo

# Criptografia: terminologia (2/2)

4



# Cifras: evolução da tecnologia

5

- Manuais

- Algoritmos simples
- Transposição ou substituição de letras



# Cifras: evolução da tecnologia

6

## □ (Eletro)Mecânicas

- A partir do Séc. XIX
  - Enigma
  - M-209 Converter
  - Lorenz
- Algoritmos de substituição mais complexos



# Cifras: evolução da tecnologia

7

## □ Informáticas / computacionais

- Apareceram com os computadores
- Algoritmos de substituição muito complexos
- Algoritmos matemáticos



# Cifras de transposição

8

- Os símbolos originais são baralhados
  - Mas mantêm-se iguais
- O algoritmo fornece uma forma base de fazer e desfazer a baralhada
  - A chave define a operação completamente
- Atualmente já não se usam

# Cifras de substituição

9

- Substituição dos símbolos originais por outros
  - Dicionário de substituição

```
53##†305))6*;4826)4#. )4#);806*  
;48†8¶60))85;1‡(; :‡*8†83(88)5*  
†;46(;88*96*?;8)*‡(;485);5*†2:  
*‡(;4956*2(5*4)8¶8*;4069285);)  
6†8)4##;1(‡9;48081;8:8‡1;48†85  
;4)485†528806*81(‡9;48;(88;4(‡  
?34;48)4‡;161;:188;‡?;
```

A good glass in the bishop's hostел in  
the devil's seat fifty one degrees an  
d thirteen minutes northeast and by  
north main branch seventh limb east  
side shoot from the left eye of the de  
ath's head a bee line from the tree thr  
ough the shot forty feet out

Edgar Allan Poe, "The Gold Bug"

- O algoritmo e a chave definem o dicionário de substituição

# Cifras computacionais

10

- Algoritmos simétricas
  - Usam apenas uma chave para cifrar e decifrar
    - Aproximação clássica
- Algoritmos assimétricos
  - Usam pares de chaves para cifrar e decifrar
    - Uma aproximação introduzida na década de 1970
- Ambos fazem a substituição de bits
  - O símbolo base da informação em informática

# Cifras simétricas

11

## □ Contínuas

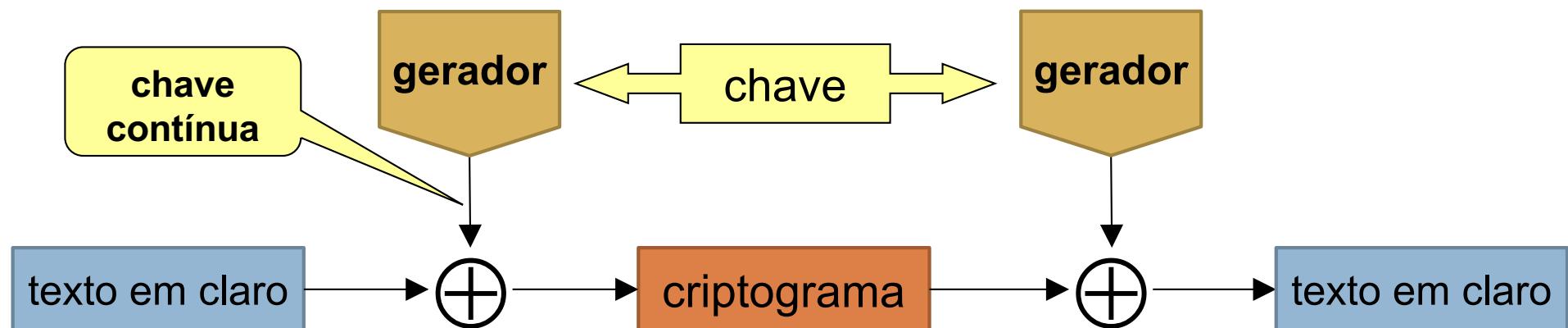
- A informação é uma sequência de bits
  - 1 ou mais
  - A posição dos bits é determinante para a sua substituição
- Normalmente usadas em comunicações rádio

## □ Por blocos

- A informação é uma sequência de blocos de bits
  - 64 ou mais
  - A posição dos blocos não altera a sua substituição
- Mais usadas em dados armazenados

# Cifras contínuas (*stream ciphers*)

12



- Mistura de uma chave contínua (*keystream*) com os dados a transformar

- Chave contínua é uma sequência pseudoaleatória
  - A sequência é produzida por um gerador
    - Parametrizado por uma chave
  - A mistura é feita (e desfeita) com a operação XOR

$$C = T \oplus ks$$

$$T = C \oplus ks$$

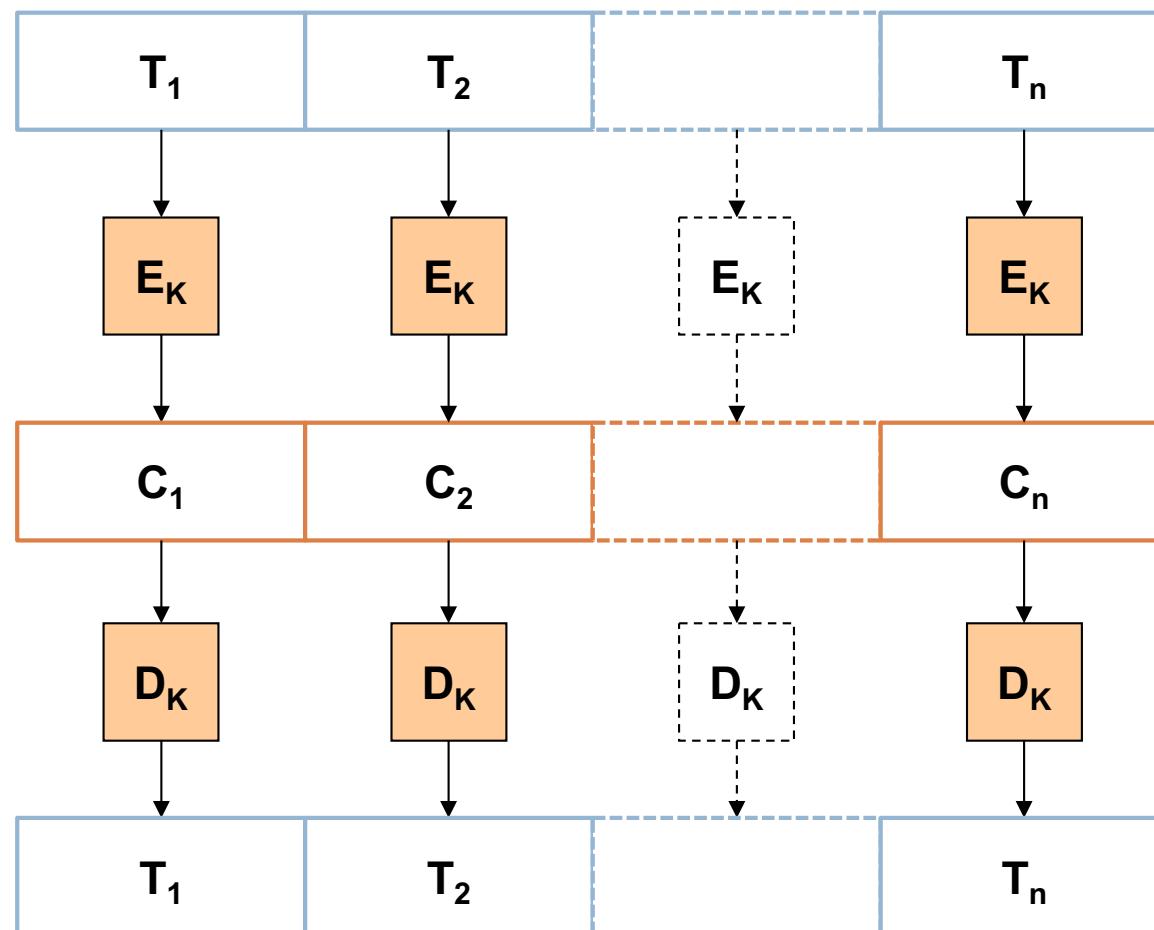
# Cifras por blocos

13

- Electronic Code Book (ECB)
  - É o modo mais simples de fazer cifra por blocos
  - O texto original é dividido em blocos contíguos de igual dimensão  $T_i$ 
    - Dimensão imposta pelo algoritmo
  - A cifra de cada  $T_i$  cria um bloco de criptograma  $C_i$ 
    - A sua sequência é o criptograma
  - Cada bloco é cifrado e decifrado independentemente

# Cifras por blocos

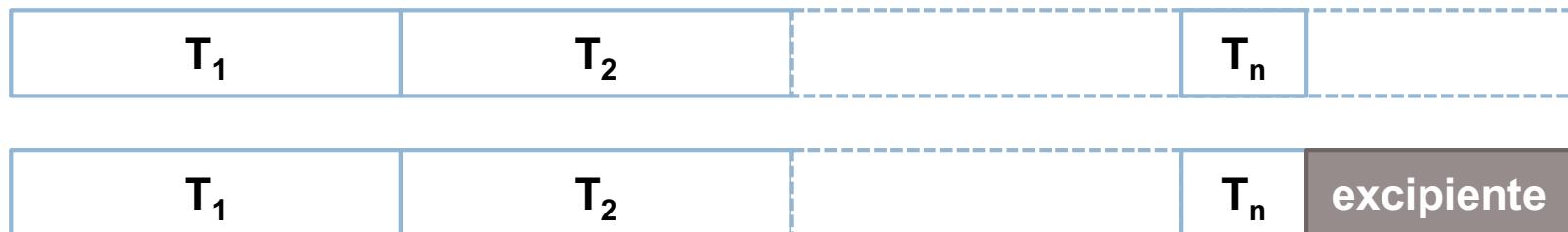
14



# Alinhamento (*padding*)

15

- O texto tem de ser alinhado
  - Não podem ser processados blocos incompletos
- Alinhamento com excipiente
  - Muitas maneiras de o fazer
  - É fundamental indicar a existência e comprimento do excipiente



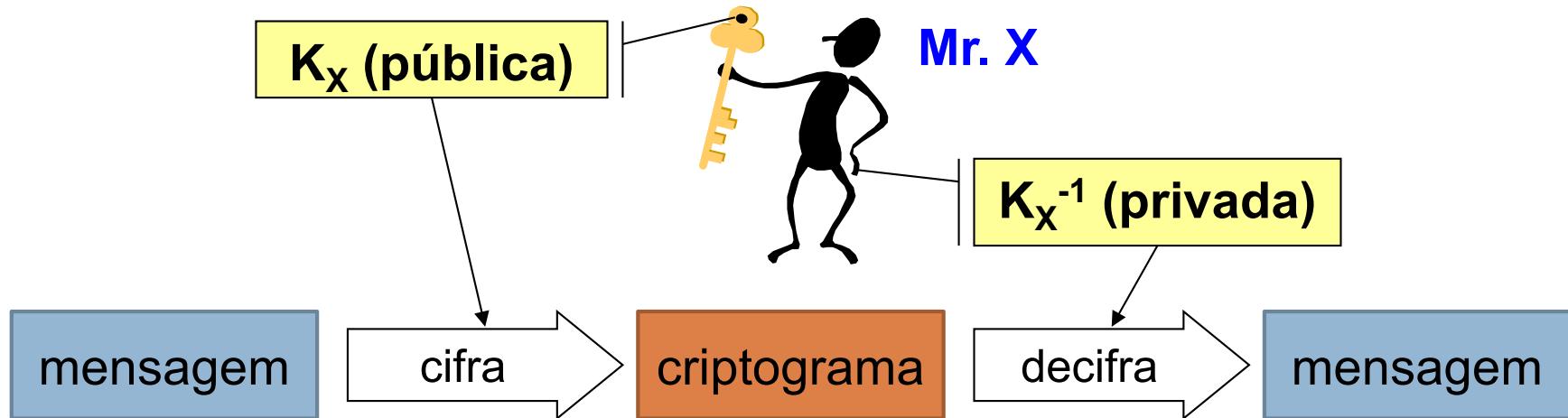
# Cifras assimétricas

16

- Cifras que usam **pares de chaves**
  - Chave **privada**
  - Chave **pública**
  - Da pública não é possível inferir a privada
- Cifras de chave pública
- Cada chave faz o inverso da outra
  - Cifra com pública, decifra com privada
  - Cifra com privada, decifra com pública
- São **cifras por blocos**

# Confidencialidade com cífras assimétricas

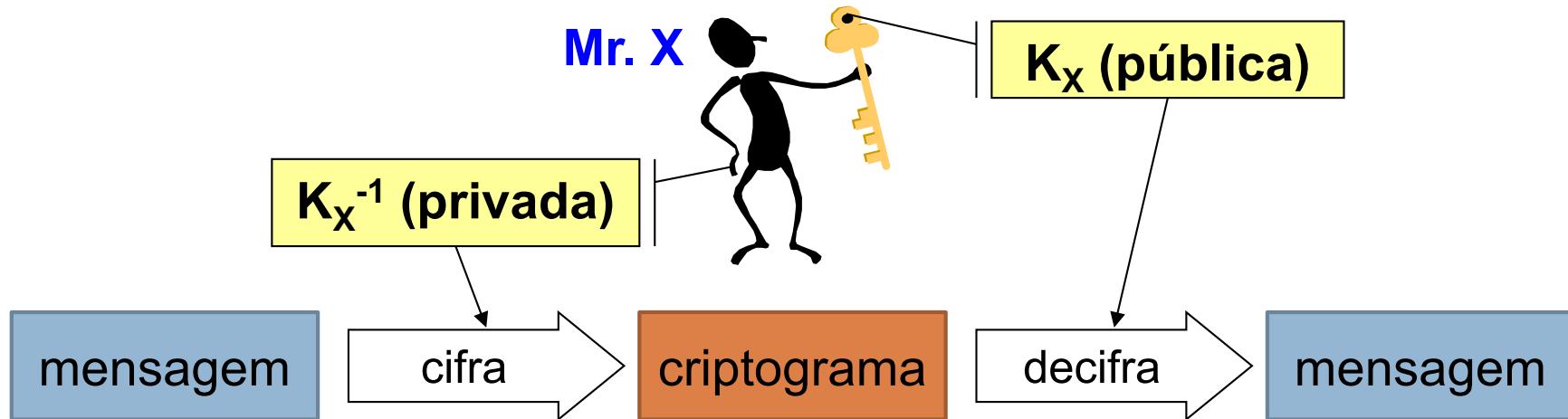
17



- Só se usa o par de chaves do receptor
  - Para enviar uma mensagem confidencial para X só é preciso conhecer a chave pública de X ( $K_x$ )
- Só X será capaz de decifrar o criptograma
  - Porque apenas X conhece a chave privada  $K_x^{-1}$

# Autenticação de conteúdos com cifras assimétricas

18



- Só se usa o par de chaves do emissor
  - Para validar a assinatura de X numa mensagem só é preciso conhecer a sua chave pública ( $K_x$ )
- Só X poderá ter produzido o criptograma
  - Porque apenas X conhece a chave privada  $K_x^{-1}$

# Funções de síntese (digest)

19

- Não são funções de cifra
  - Mas usam princípios criptográficos
- Produzem um valor de dimensão constante a partir de um volume arbitrário de bits
  - São funções de dispersão (*hashing*)
  - Mas têm propriedades especiais
- Utilidade
  - Detetar alterações em dados
  - Agilizar assinaturas digitais
  - Fazer transformações de dados unidirecionais

# Tecnologia atual

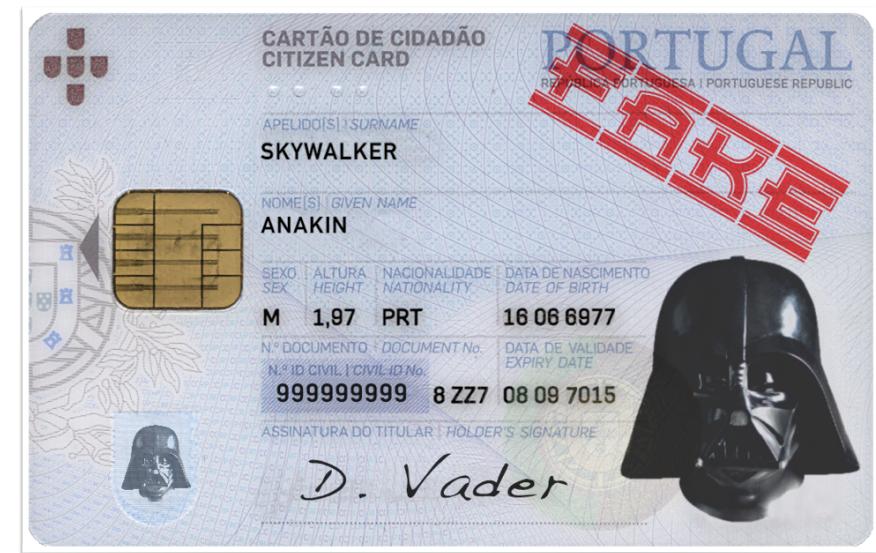
20

- Cifras contínuas
  - RC4, A5
  - Geradores baseados em cifras por blocos
- Cifras por blocos
  - DES, IDEA, Blowfish
  - AES
- Cifras assimétricas
  - RSA, ElGamal
  - Curvas Elíticas
- Alinhamento
  - PKCS #7 (bytes)
  - RFC 1321 (bits)
- Funções de síntese
  - MD5 (a evitar)
  - SHA-1
  - SHA-256
  - SHA-512

# Utilização: CC

21

- Chaves Assimétricas
- Chave privada gera assinaturas
  - Nunca sai do cartão
- Chave pública para distribuição
- Certificado emitido pelo estado



# Utilização: Distribuição de aplicações

22

- Gestor assina pacotes
  - Garante que não são alterados
- Clientes verificam assinaturas antes de instalarem

```
[user@cloud:~$ sudo apt-key list
/etc/apt/trusted.gpg
-----
pub    1024D/437D05B5 2004-09-12
      Ubuntu Archive Automatic Signing Key <ftpmaster@ubuntu.com>
uid
sub    2048g/79164387 2004-09-12

pub    1024D/FBB75451 2004-12-30
      Ubuntu CD Image Automatic Signing Key <cdimage@ubuntu.com>
```

# Utilização: Distribuição de aplicações

23

```
user@cloud:~$ apt-cache show python
```

Package: python

Source: python-defaults

Version: 2.7.8-3

Installed-Size: 680

Maintainer: Matthias Klose <doko@debian.org>

...

Description-md5: d1ea97f755d8153fe116080f2352859b

...

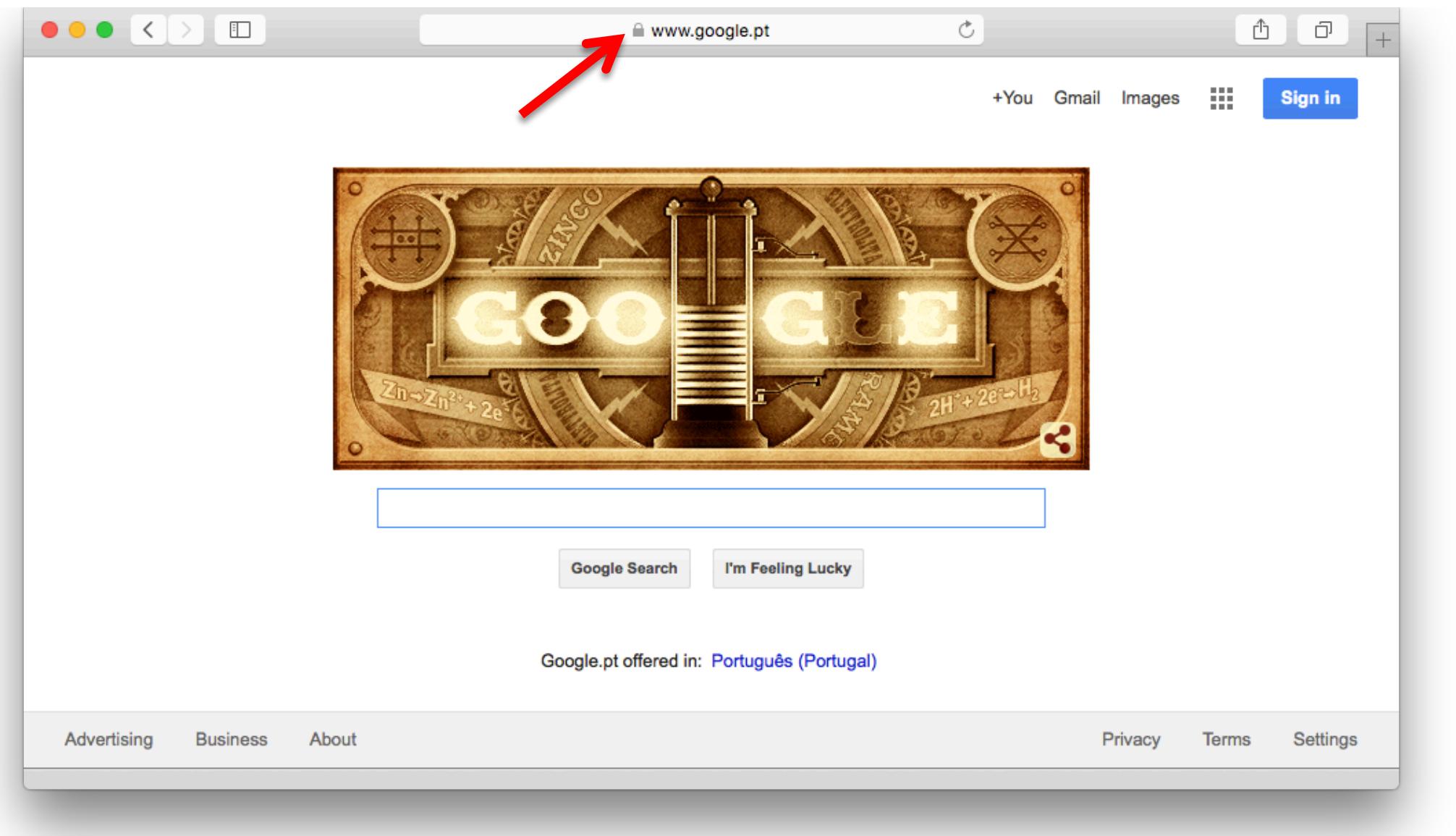
MD5sum: 209fc82bed11aeafdf55bf4ac2b248232

SHA1: 171427cf618679073017acb28ad894a5cbb1ebd5

SHA256: 73a05a2747674b247a2ee2d3c0ff39e903d742daa7c3641f9c6ff121863865f1

# Utilização: Navegação (HTTPS)

24



# Utilização: outros

25

- Redes de Telemóvel
  - Cifrar chamadas, autenticar utilizadores
- Sistemas de pagamento
- Consolas de Jogos
  - proteção contra cópias
- Distribuição de TV
- Etc...

# Para Aprofundar

26

- André Zúquete, Segurança em Redes Informáticas (4.<sup>a</sup> Ed. Aumentada), FCA