

# CRIPTOGRAFIA E CERTIFICAÇÃO DIGITAL

Júnio César da Silva MSc.



- Agenda

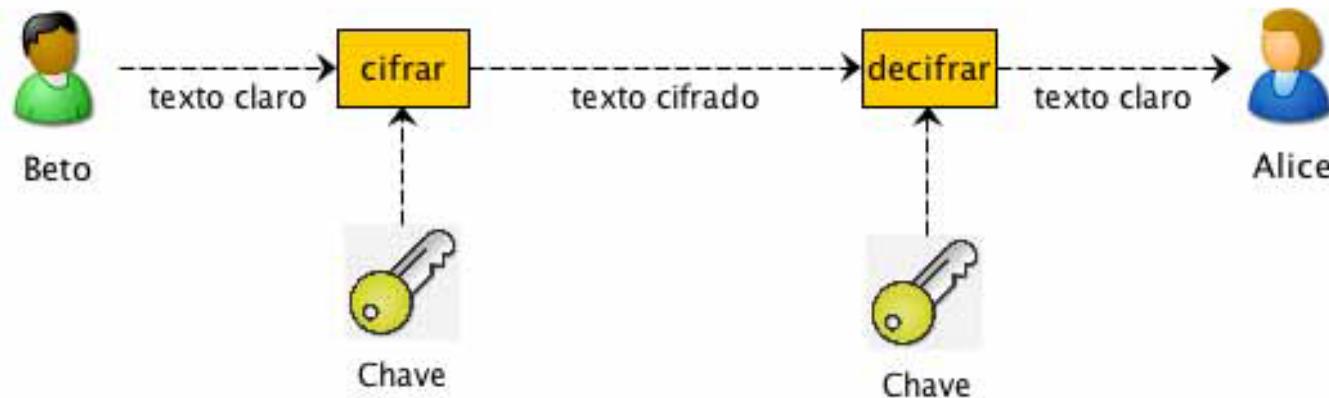
- Criptografia
- Assinatura Digital
- Infra Estrutura de Chaves Públicas



# Criptografia

- Kryptós: Escondido
- Gráphein: Escrita
- Princípios e técnicas para transformar uma mensagem de sua forma original para outra ilegível.





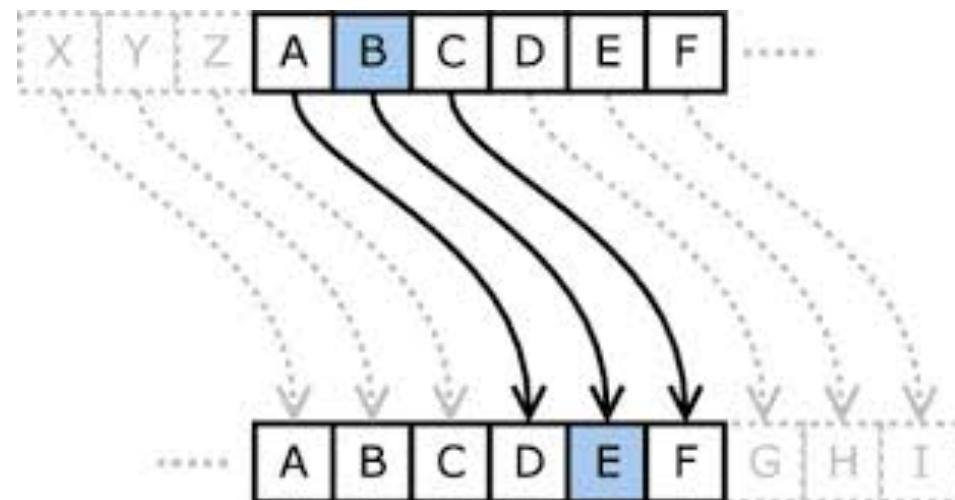
- ✓ **Texto claro:** Texto original
- ✓ **Texto cifrado:** Texto ilegível
- ✓ **Cifrar:** Processo de transformação do texto claro em texto cifrado
- ✓ **Decifrar:** Processo de transformação do texto cifrado em texto claro
- ✓ **Chave:** Conjunto de dados utilizados para cifrar e decifrar.



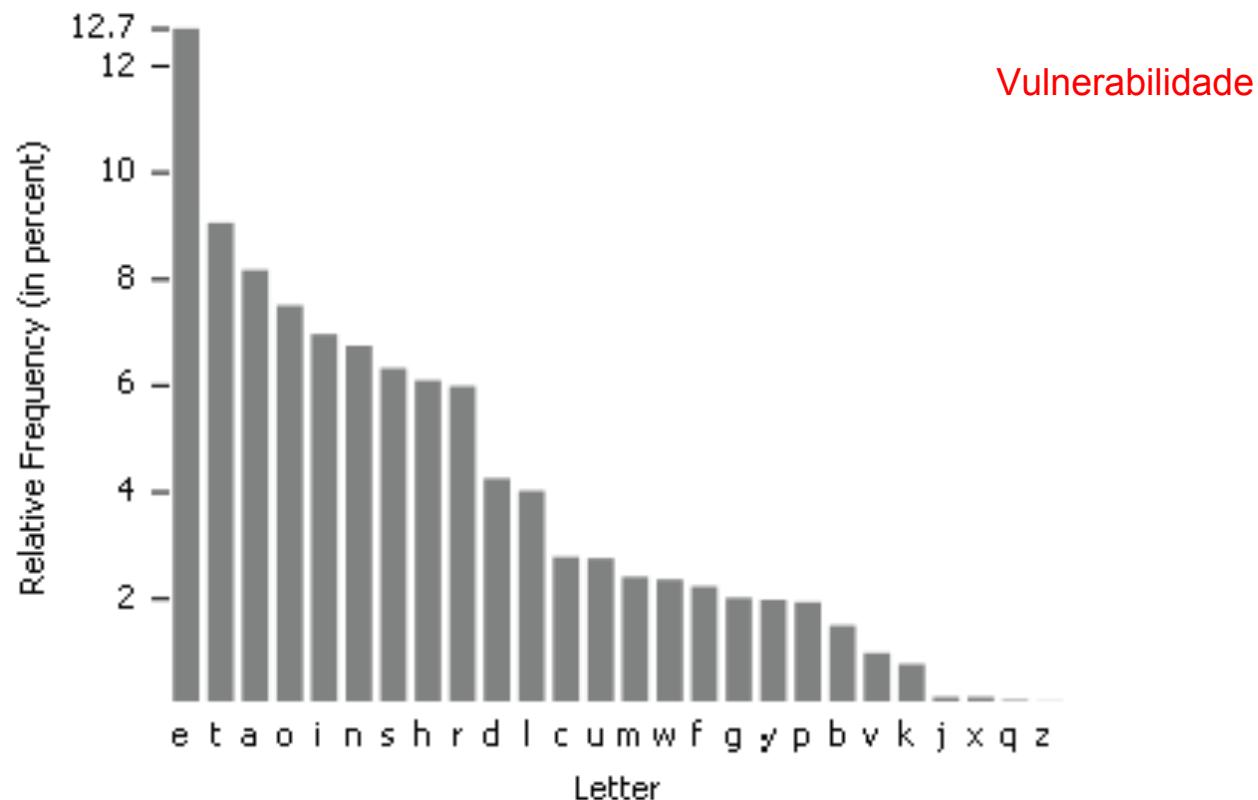
# Criptografia Clássica



# Cifrador de César



# Análise de frequência



Vulnerabilidade



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

# Cifrador polialfabético

## Cifrador de Vigenere

Mensagem: universo

Chave: xpto

Resultado: rcbjbgc



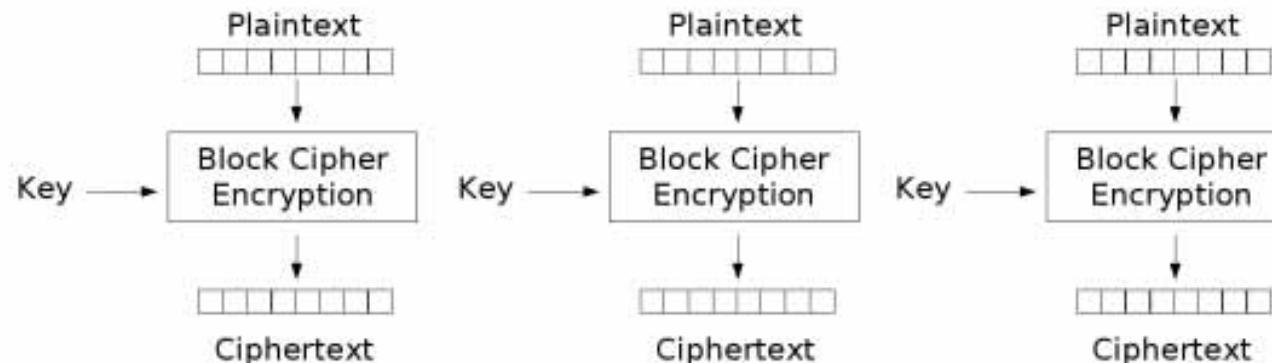
# Criptografia Moderna



1949: Claude Shannon e Warren Weaver publicam o artigo “Communication Theory of Secrecy Systems”



# Cifradores de Bloco



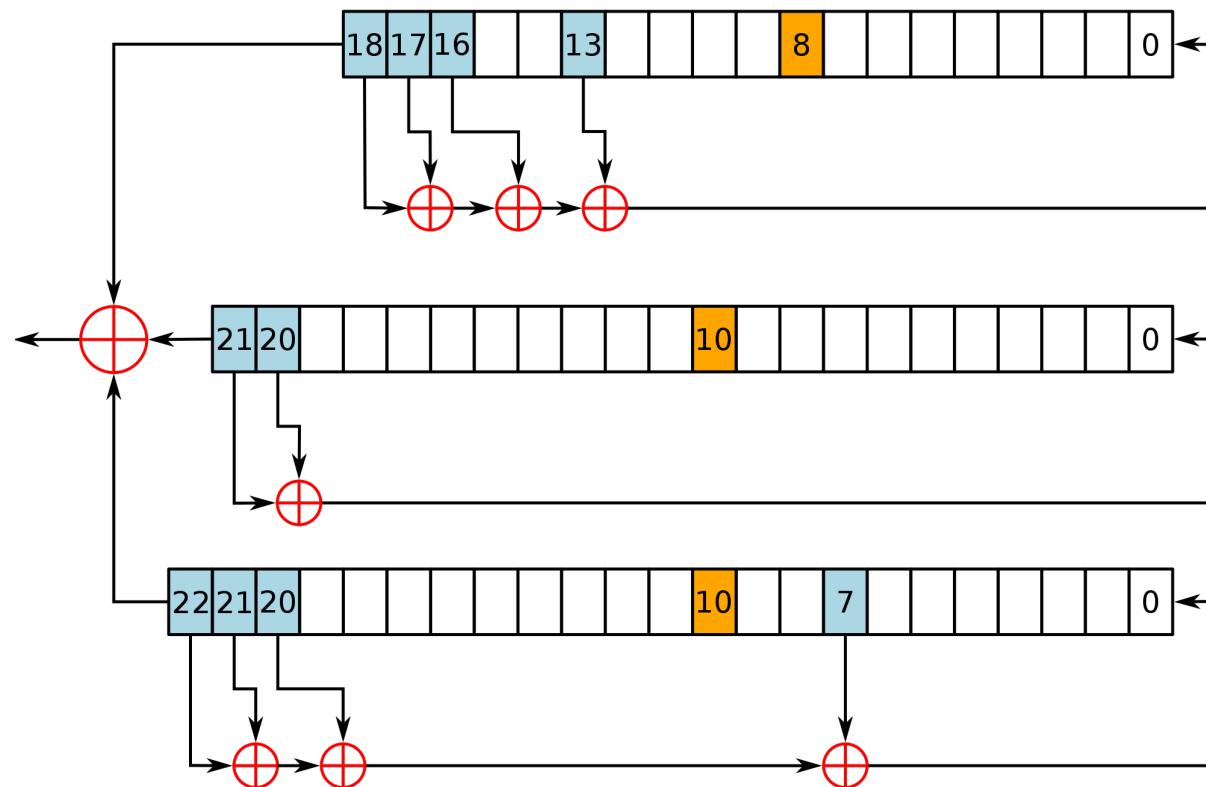
Electronic Codebook (ECB) mode encryption

1976 o governo americano publica o DES (Data Encryption Standard)



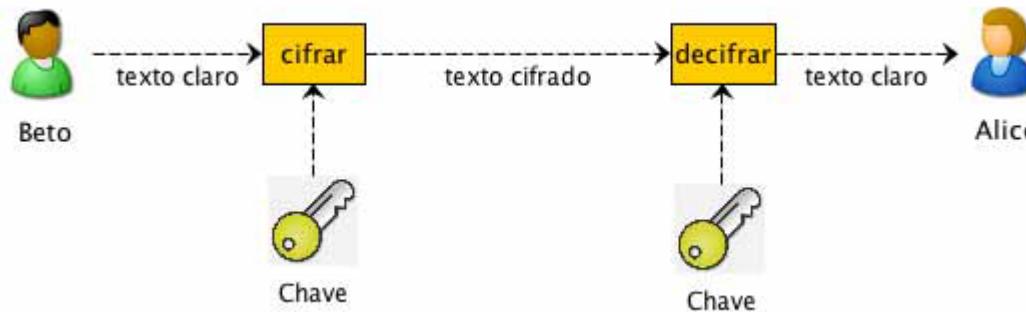
# Cifradores de Fluxo

RC4 é o mais conhecido atualmente



# Criptografia simétrica

- Mesma chave para cifrar e decifrar uma mensagem.
- Questões:
  - Como distribuir as chaves de maneira segura?
  - É possível verificar se a mensagem foi alterada?
  - É possível verificar o emissor da mensagem?



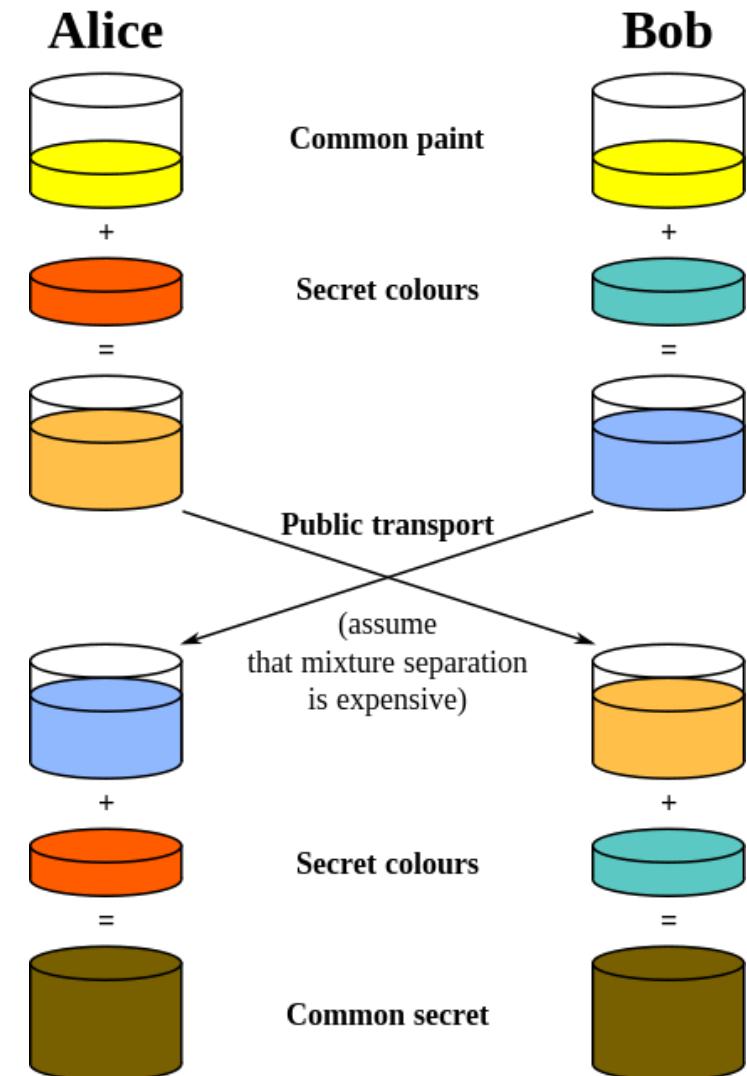
# Algoritmos simétricos

- DES e 3DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)



# Troca de Chaves

O Conceito de troca de chaves em um meio inseguro foi publicado em 1976 por Diffie- Hellman



# Matematicamente falando

1. Alice and Bob agree to use a prime number  $p = 23$  and base  $g = 5$  (which is a primitive root modulo 23).
2. Alice chooses a secret integer  $a = 6$ , then sends Bob  $A = g^a \bmod p$ 
  - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer  $b = 15$ , then sends Alice  $B = g^b \bmod p$ 
  - $B = 5^{15} \bmod 23 = 19$
4. Alice computes  $s = B^a \bmod p$ 
  - $s = 19^6 \bmod 23 = 2$
5. Bob computes  $s = A^b \bmod p$ 
  - $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret (the number 2).



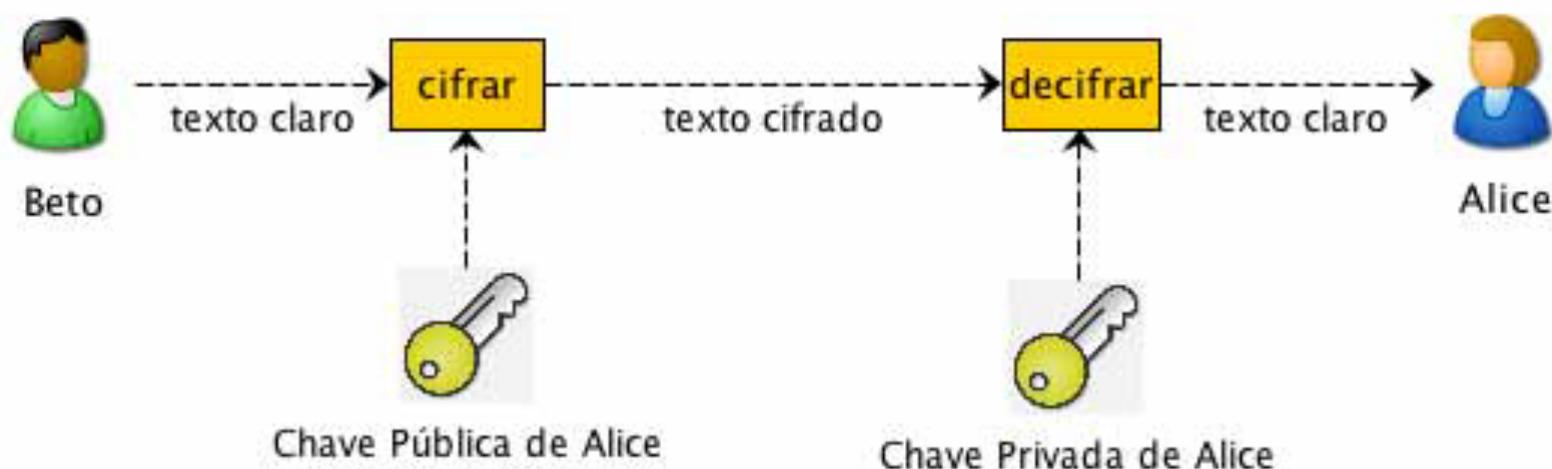
Alice		Bob		Eve	
knows	doesn't know	knows	doesn't know	knows	doesn't know
$p = 23$	$b = ?$	$p = 23$	$a = ?$	$p = 23$	$a = ?$
base $g = 5$		base $g = 5$		base $g = 5$	$b = ?$
$a = 6$		$b = 15$			$s = ?$
$A = 5^a \text{ mod } 23$		$B = 5^b \text{ mod } 23$		$A = 8$	
$A = 5^6 \text{ mod } 23 = 8$		$B = 5^{15} \text{ mod } 23 = 19$		$B = 19$	
$B = 19$		$A = 8$		$s = 19^a \text{ mod } 23 = 8^b \text{ mod } 23$	
$s = B^a \text{ mod } 23$		$s = A^b \text{ mod } 23$			
$s = 19^6 \text{ mod } 23 = 2$		$s = 8^{15} \text{ mod } 23 = 2$			
$s = 2$		$s = 2$			

- Para valores de  $p$  com 300 dígitos e valores de  $a$  e  $b$  com pelo menos 100 dígitos, a computação necessária para se descobrir  $a$  e  $b$  não é viável.



# Criptografia Assimétrica

- Utiliza um par de chaves
  - Chave pública (cifrar)
  - Chave privada (decifrar)

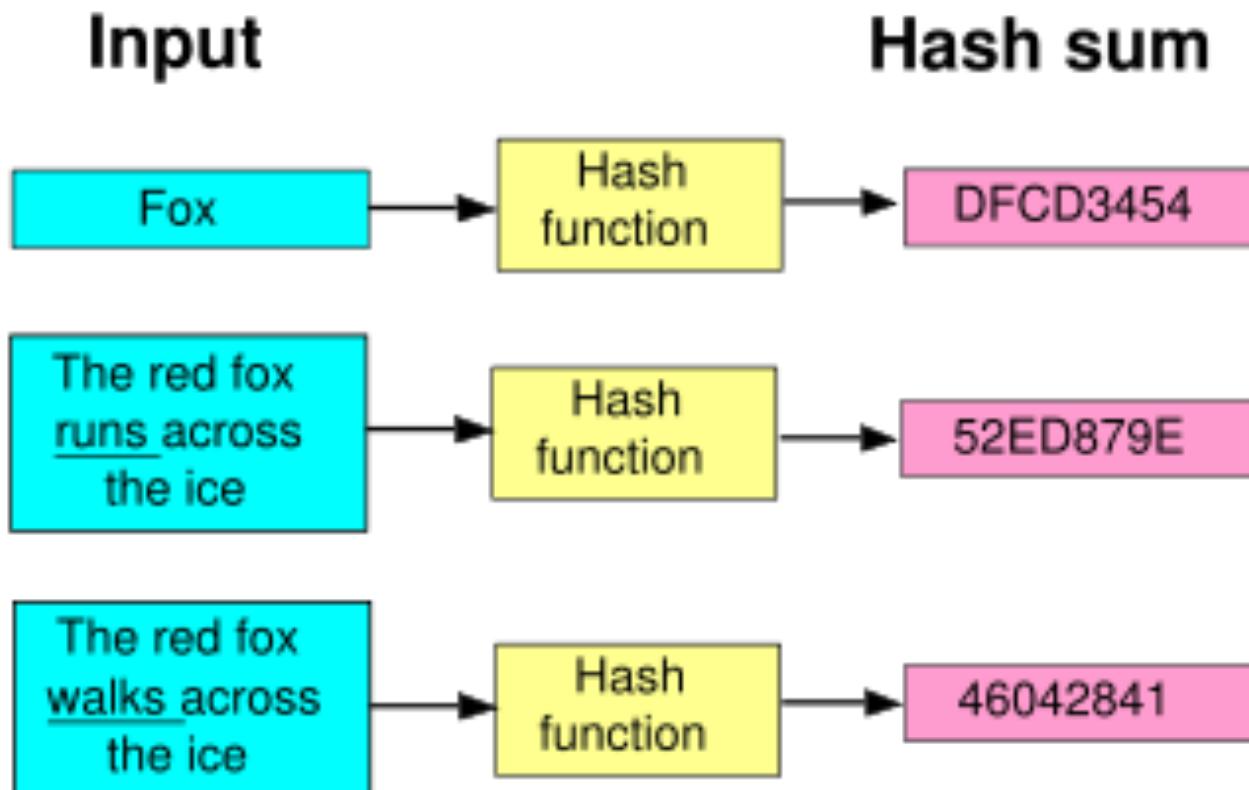


# Algoritmos de Hash

- Processam uma mensagem de entrada, gerando um conjunto de bits de saída de tamanho fixo, independente do tamanho da mensagem de entrada.
- Este conjunto de bits pode ser entendido como a “impressão digital” da mensagem.
- Exemplos:
  - Message Digest 5 – MD5
  - Secure Hash Algorithm 1 – SHA1

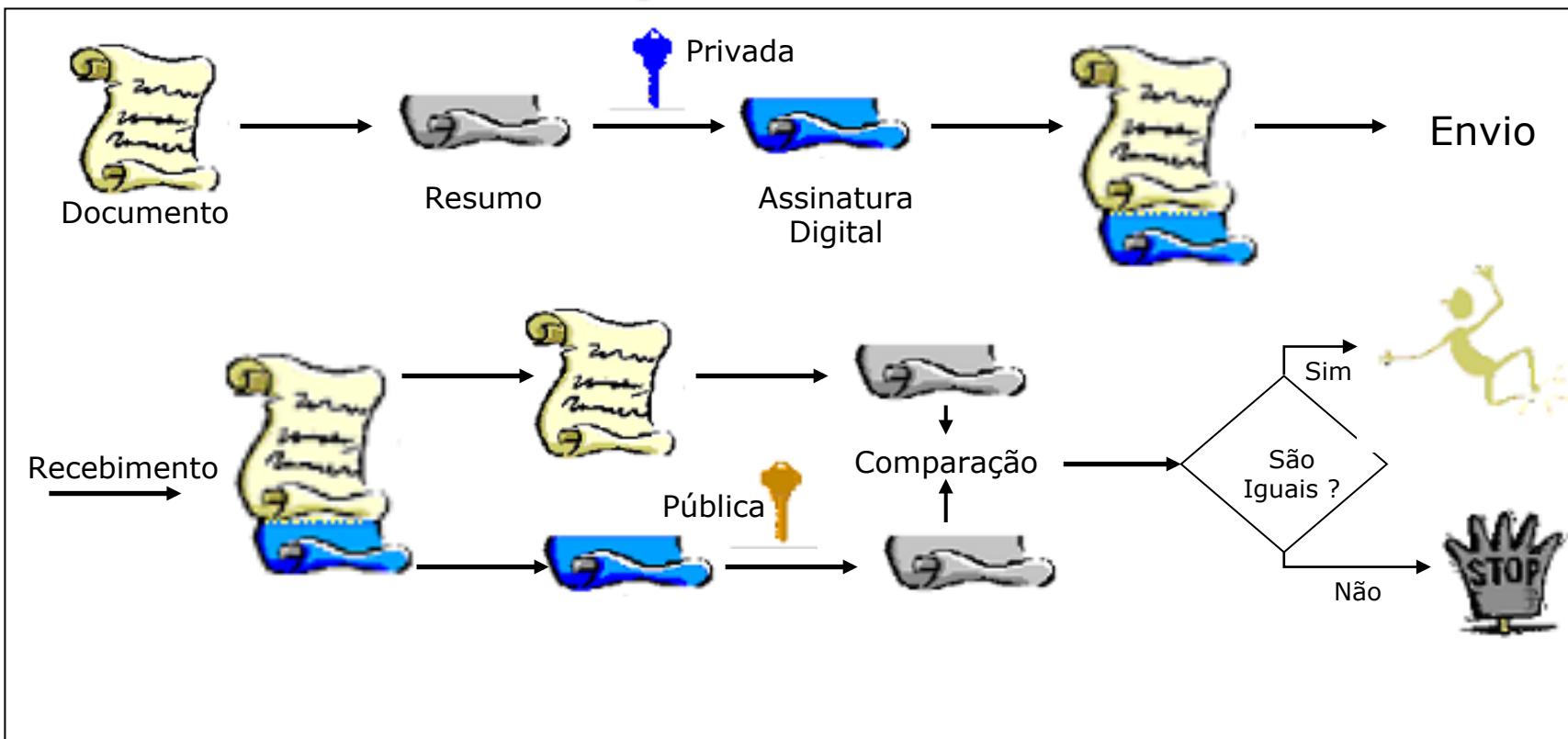


# Algoritmos de Hash

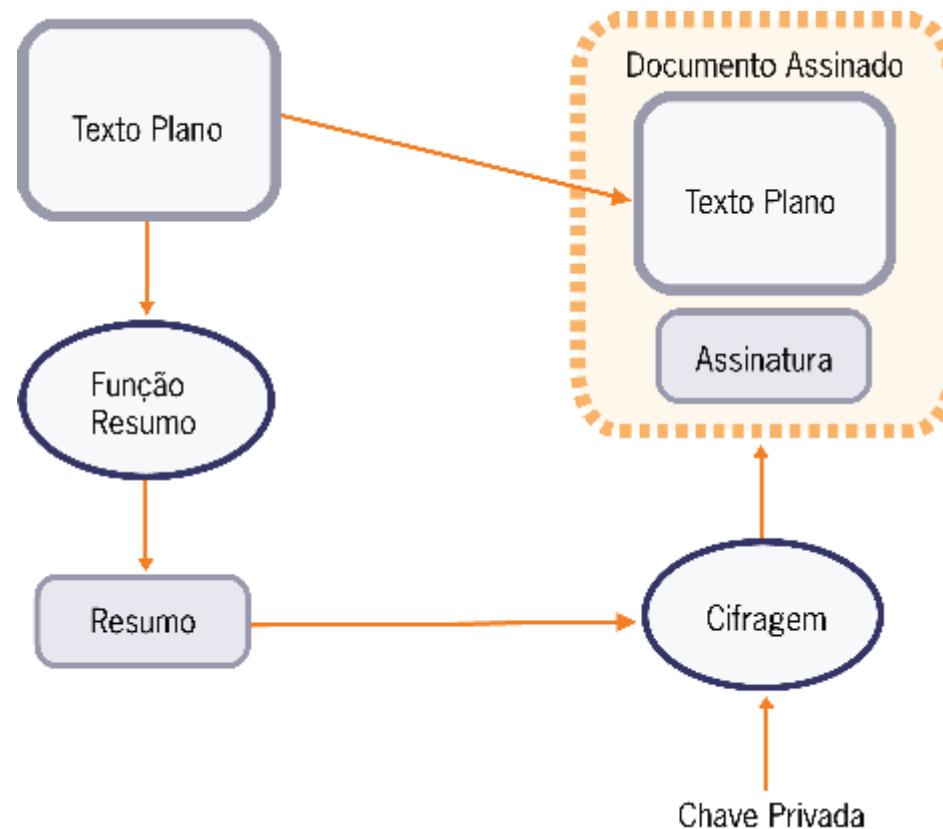


# Assinatura Digital

Documento assinado digitalmente:



# Assinatura Digital



# Assinatura Digital

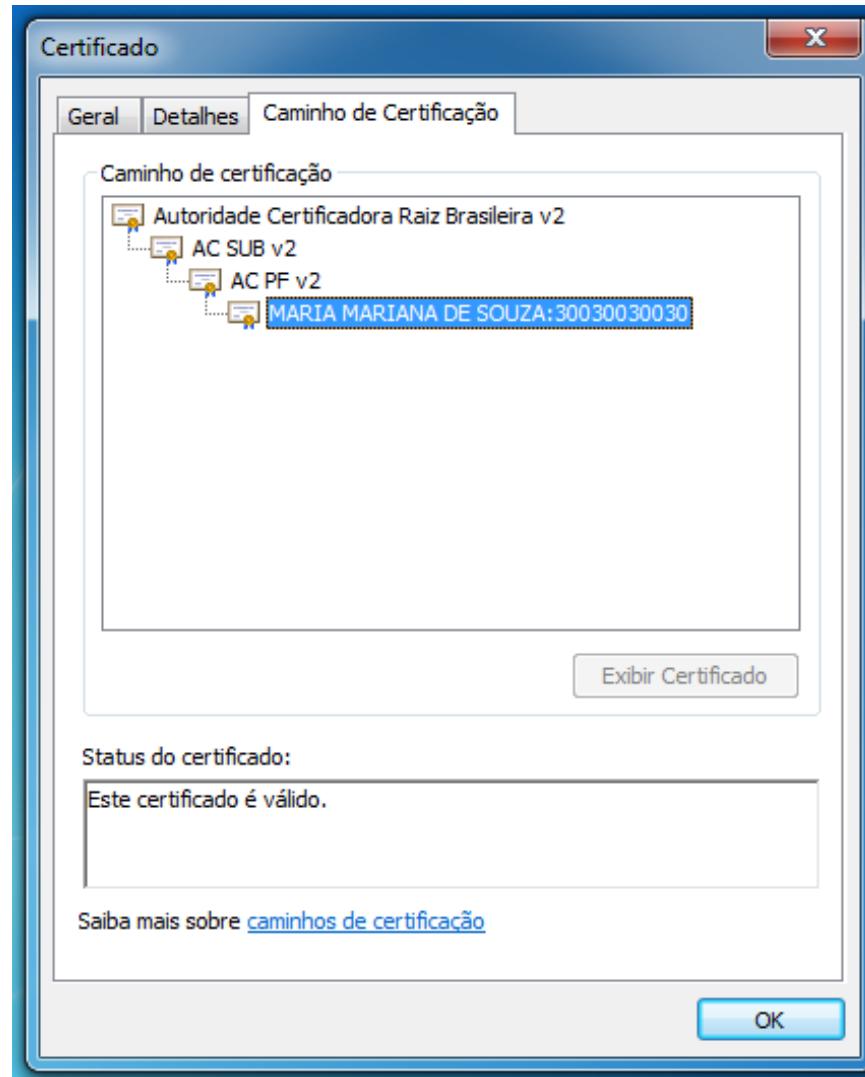
- Autenticidade
  - Busca garantir que a mensagem é autêntica, o autor da mensagem é realmente quem diz ser.
- Integridade
  - Permite verificar se a mensagem enviada é igual à mensagem recebida ou se sofreu alguma alteração.
- Irretratabilidade
  - O emissor não pode negar a autenticidade da mensagem.



# Certificado Digital

- ▶ É um arquivo, gerado por uma Autoridade Certificadora, em observância à recomendação internacional I-TUT X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia pública e uma pessoa física, jurídica, máquina ou aplicação.



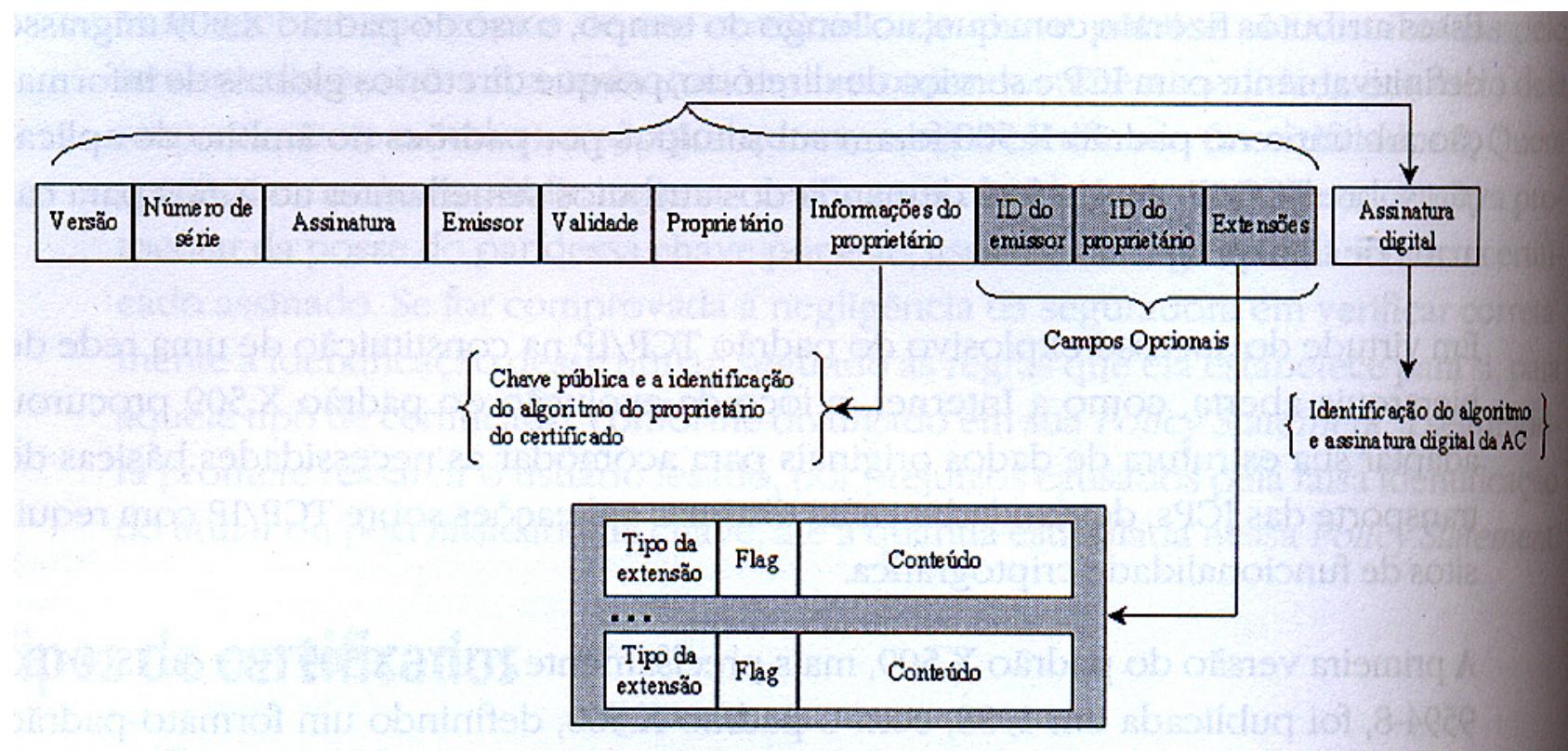


# Estrutura certificado

- A infra-estrutura de chaves públicas Brasileira – ICP-Brasil utiliza certificados no padrão ITU-T X.509 (X.509v3).

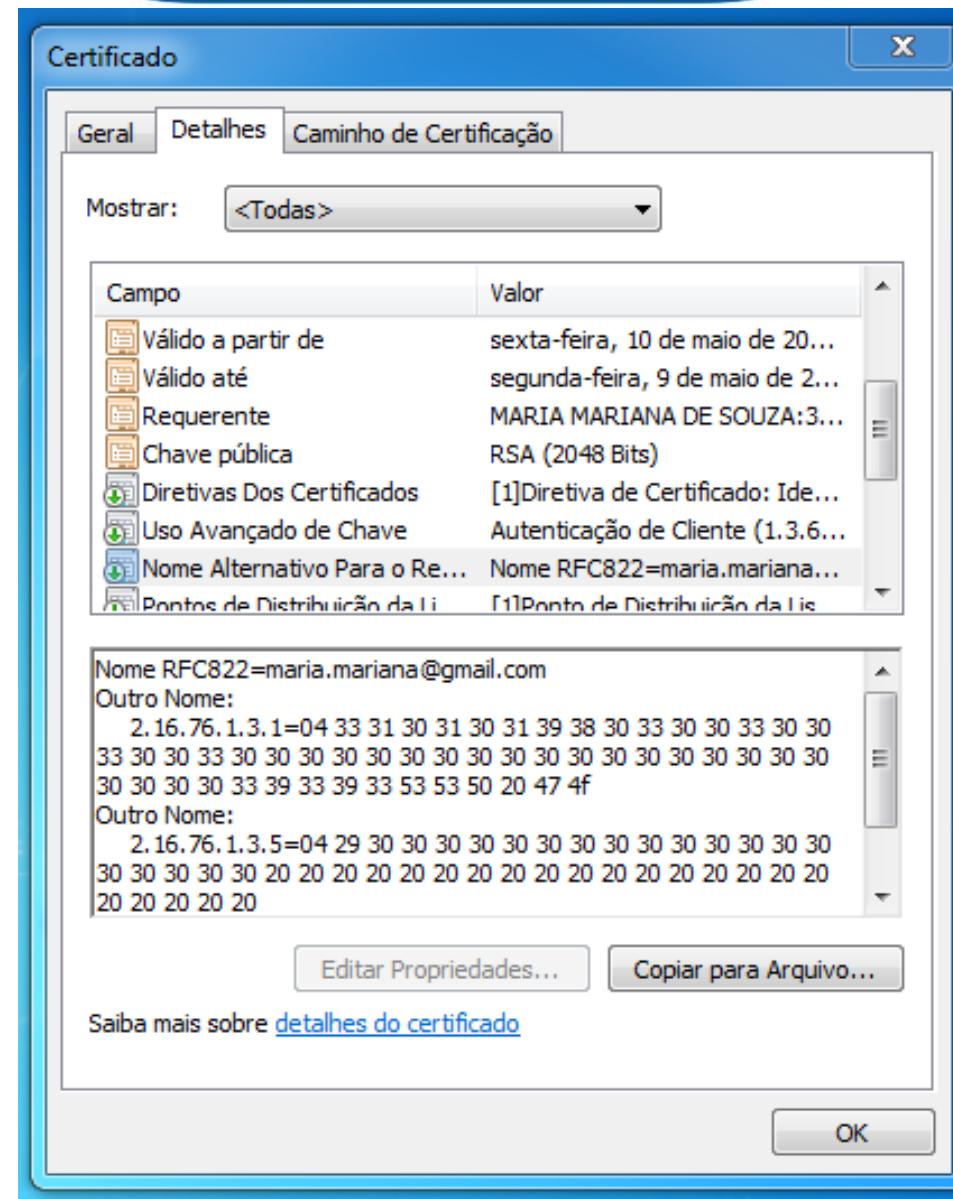


# Estrutura Certificado X.509v3



# Atributos do Certificado





# Object Identifier

- Um OID – Object Identifier é um número único que identifica uma classe de objetos ou um atributo em um diretório ou combinação de diretórios.



# Object Identifier

- O Brasil recebeu da ISO o OID raiz **2.16.76.1** e a partir dele o Instituto Nacional de Tecnologia da Informação – ITI criou OIDs para identificar cada Autoridade Certificadora e cada Política de Certificados, bem como outros elementos necessários ao funcionamento da ICP-Brasil.



# Object Identifier - Exemplos

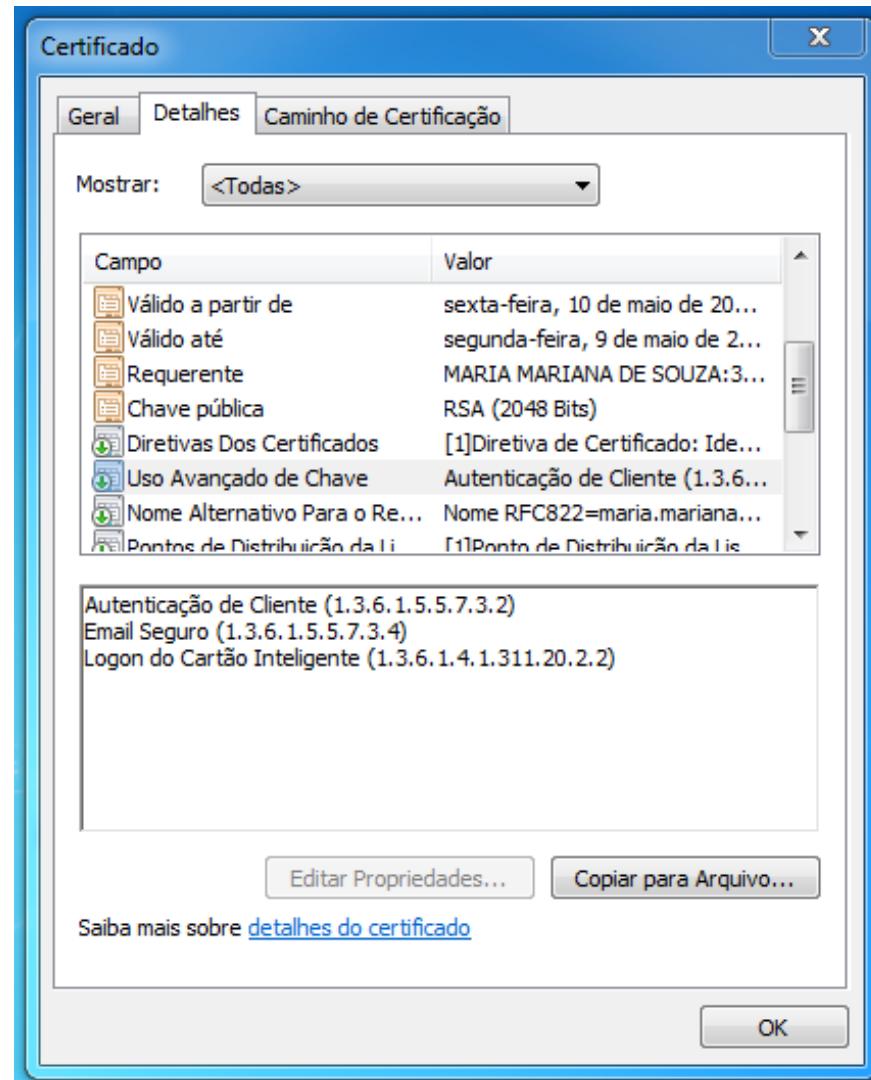
- 2.16.76.1.3.1
  - campo **otherName** em certificado de **pessoa física**, contendo os dados do titular (data de nascimento, CPF, PIS/PASEP/CI, RG).
- 2.16.76.1.3.2
  - campo **otherName** em certificado de **pessoa jurídica**, contendo o nome do responsável pelo certificado.



# Object Identifier - Exemplos

- 2.16.76.1.3.4
  - campo **otherName** em certificado de **pessoa jurídica**, contendo os dados do responsável pelo certificado de pessoa jurídica titular do certificado (data de nascimento, CPF, PIS/PASEP/CI, RG);
- 2.16.76.1.4.x
  - **Identificação do ramo** (Entidades sindicais / empresas / estados da federação, etc.)





# Infraestrutura de Chaves Públcas

A Infraestrutura de Chaves Públcas (ICP) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual de pessoas, servidores, sistemas, etc.



# ICP-Brasil

- › Infra-Estrutura de Chaves Públicas Brasileira
  - Instituída pelo Governo Federal - MP 2.200 - Agosto/2001
- › A ICP-Brasil é uma estrutura hierárquica com uma Autoridade Certificadora Raiz, várias autoridades certificadores de primeiro nível e várias autoridades de registro associadas as autoridades de primeiro nível.



- ▶ Autoridades certificadoras são “terceiros confiáveis” responsáveis pela emissão de certificados digitais



# AC-Raiz

- Primeira AC da cadeia de certificação da Infra-Estrutura de Chaves Públicas Brasileira cujo certificado é auto-assinado.



# Autoridades Certificadoras

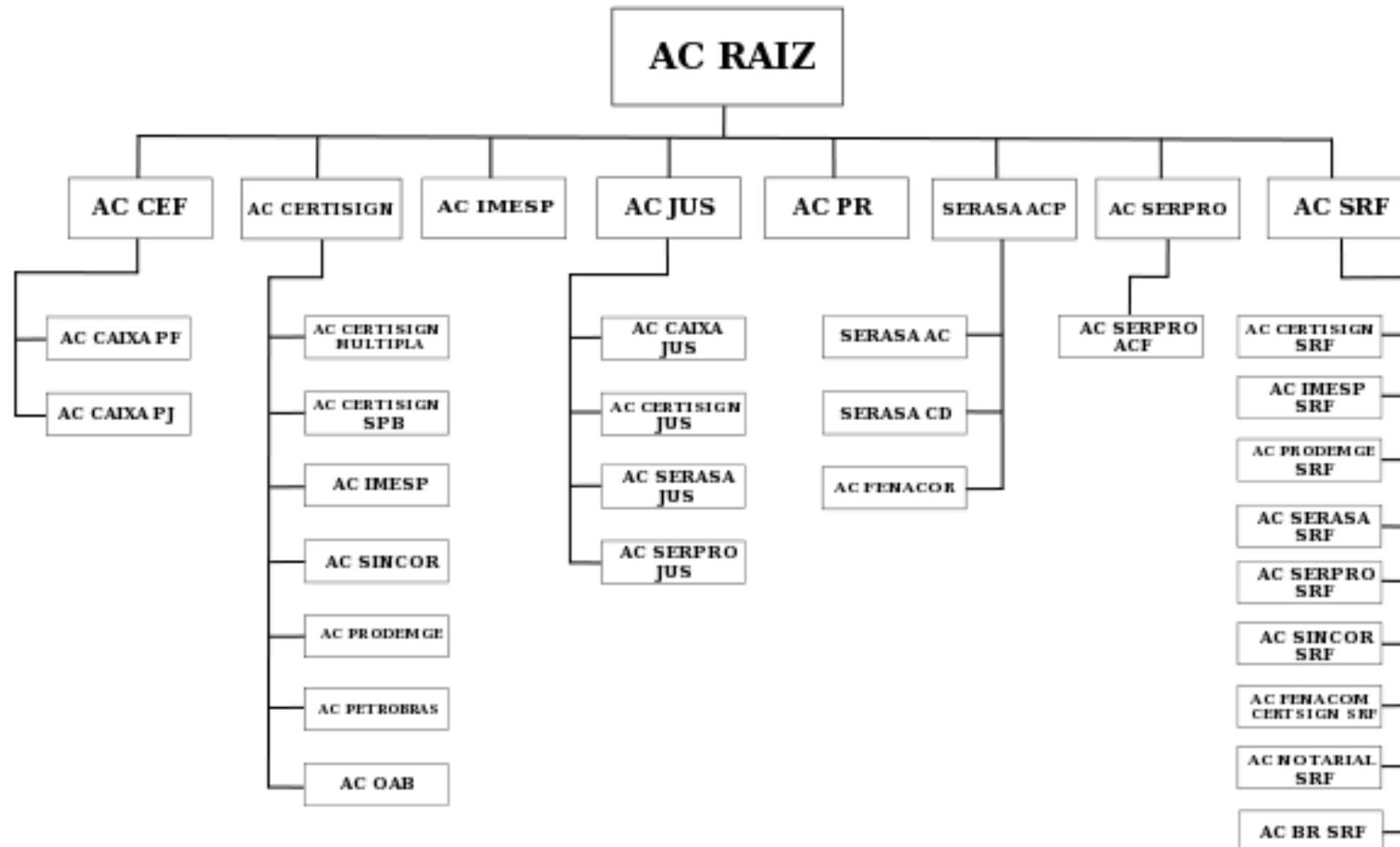
- São entidades subordinadas à hierarquia da ICP-Brasil, responsáveis por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Cabe também à AC emitir listas de certificados revogados (LCR).
- Os certificados das AC's de primeiro nível são assinados pela AC-Raiz.



# Autoridades de registro

- Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. É vinculada a uma AC e tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, *de forma presencial*, de seus solicitantes.

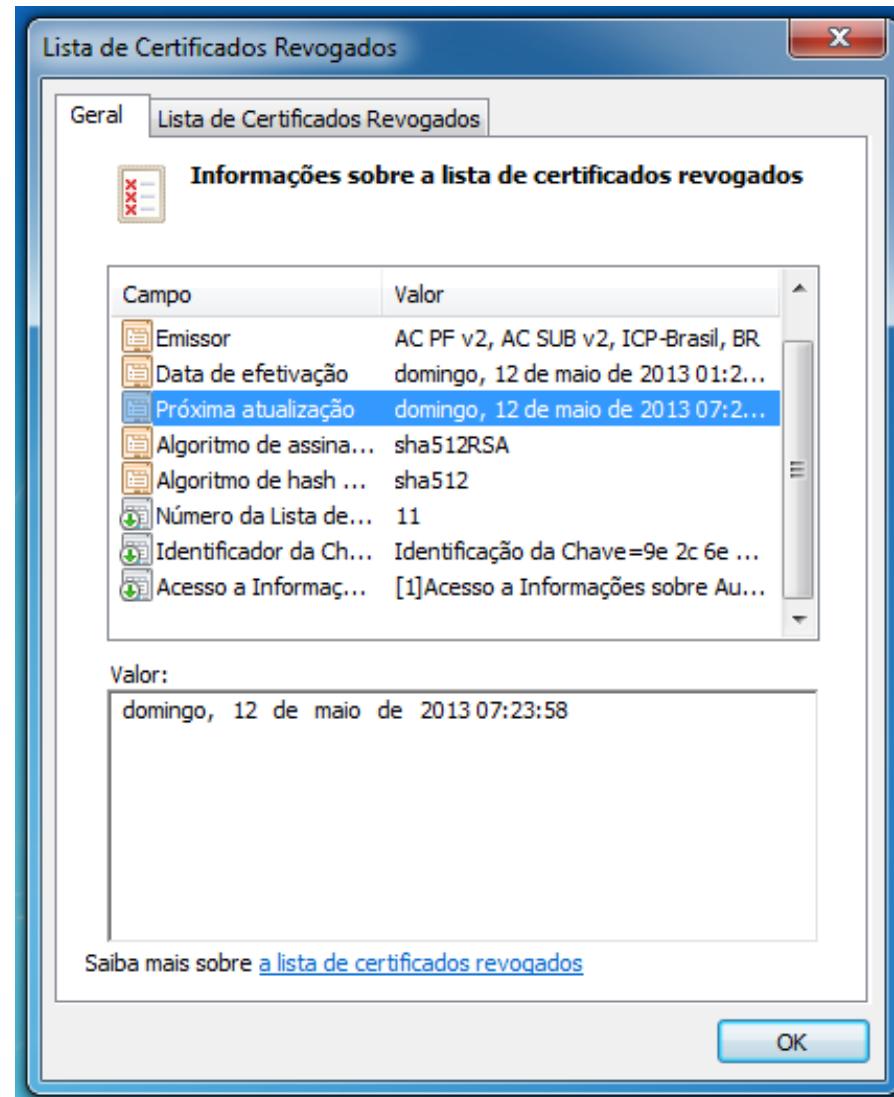




# Lista Certificados Revogados

- LCR
  - AC raiz publica em intervalos de 90 dias.
  - ACs de primeiro nível a cada 45 dias.
  - ACs de segundo nível em até 6 horas.
- Motivos para revogação
  - Comprometimento da Chave Privada
  - Troca do nome do titular;
  - Saída de um funcionário da empresa





**Lista de Certificados Revogados**

Geral    **Lista de Certificados Revogados**

Certificados revogados:

Número de série	Data de revogação
01 39 ff 13 b4 09	sexta-feira, 26 de abril ...
01 3e 71 5f 13 49	sexta-feira, 10 de maio ...
01 3e 97 a1 8b d7	sexta-feira, 10 de maio ...
01 3e 97 c6 e3 04	sexta-feira, 10 de maio ...

Entrada de revogação

Campo	Valor
Número de série	01 3e 97 c6 e3 04
Data de revogação	sexta-feira, 10 de maio de 2013 22:...
Código de Razão da ...	Cessação da Operação (5)

Valor:

Saiba mais sobre [a lista de certificados revogados](#)

OK



# OCSP

- *Online Certificate Status Protocol*
  - É o Protocolo *Online* para verificação de Estado de Certificados.



# HSM

- ***Hardware Security Module***

- É um dispositivo baseado em *hardware* que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.



# FCT

- **Fonte Confiável de Tempo**

- É a denominação dada ao Relógio Atômico localizado no Observatório Nacional.



# Obrigado!!

