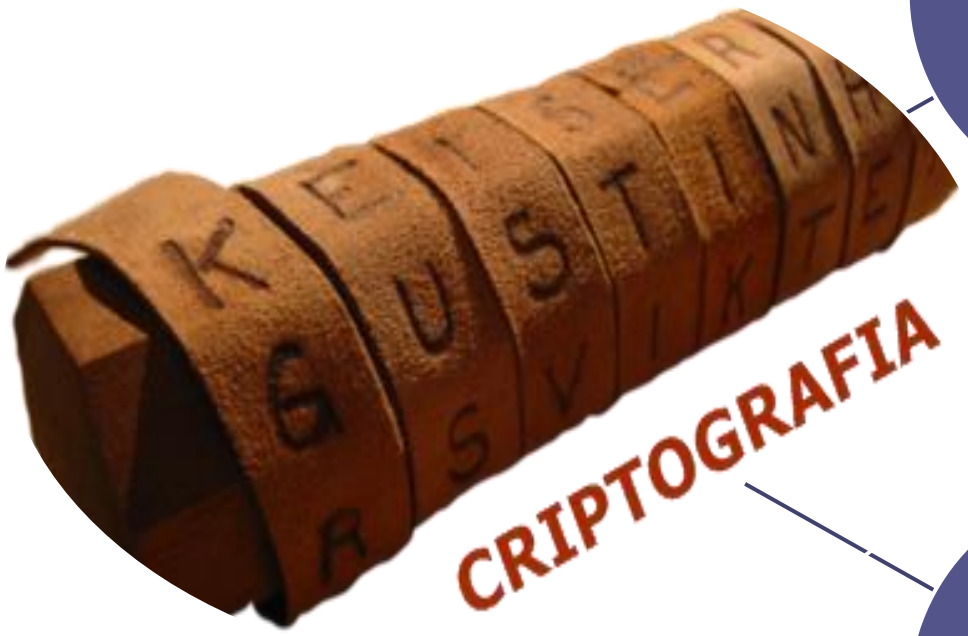
Aula 8 – Parte 1
Introdução à Criptografia, Assinatura e Certificados Digitais



Crypto

- oculta

Grafia

- escrita

Criptologia - Conceitos

- A palavra criptologia deriva da palavra grega kryptos (oculto) e logos (estudo).

- Disciplina/Ciência que reúne os conhecimentos e as técnicas necessários à criptoanálise ('solução de criptogramas') e à criptografia ('modificação codificada').

- Uma cifra não é um código.
- A cifra é um ou mais algoritmos que cifram e decifram um texto.

- Na linguagem não-técnica, um Código secreto é o mesmo que uma cifra.

- Porém, na linguagem especializada os dois conceitos são distintos:

  - Um código funciona manipulando o significado, normalmente pela substituição simples de palavras ou frases.

  - Uma cifra, ao contrário, trabalha na representação da mensagem (letras, grupos de letras ou, atualmente, bits).

- A palavra cifra vem do hebraico saphar, que significa "dar número".

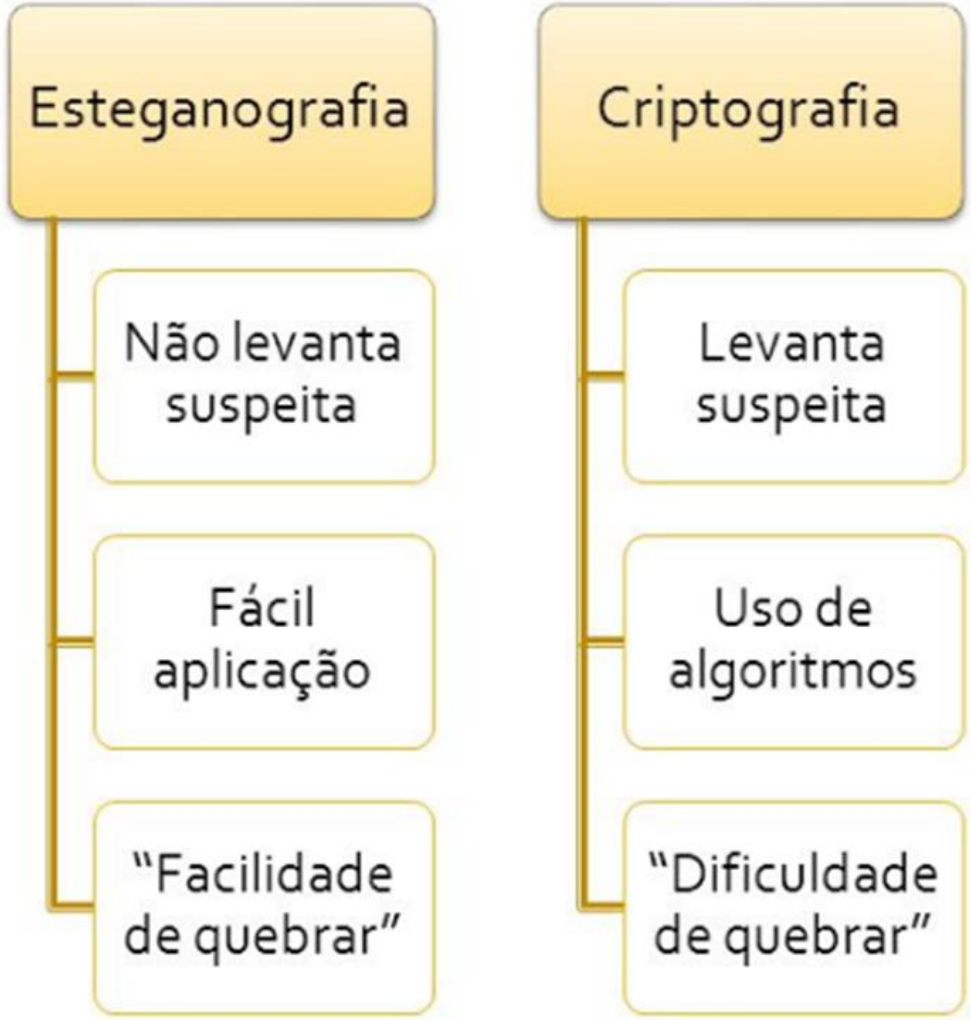
- A maiorias dos ciframentos são intrinsecamente sistemáticos, frequentemente baseados em técnicas de sistemas numéricos.

- A cifra pode ser visualizada por qualquer pessoa. Porém, a mensagem a ser transmitida só poderá ser decifrada pela pessoa autorizada. Caso a mensagem ou cifra estivesse oculta, estaria sendo utilizada a técnica de esteganografia.

- **Esteganografia**: É o estudo das técnicas de ocultação de mensagens dentro de outras, diferentemente da criptografia, que altera a mensagem de forma a tornar seu significado original ininteligível.

- A esteganografia não é considerada parte da criptologia, é uma tecnologia de segurança de informação paralela, sendo usualmente estudada em contextos semelhantes aos da criptografia e pelos mesmos pesquisadores.

Esteganografia x Criptografia



Criptologia - Conceitos

- **Criptoanálise**: É o processo de examinar informações criptografadas para tentar determinar qual a mensagem cifrada ou qual a chave que criptografou a mensagem (que, evidentemente, leva à própria mensagem).

- Dentro da criptologia, a ciência da criptografia tem como seu objeto de estudos os processos de ciframento.

- **Ciframento**: É a transformação dos dados em uma forma que torna impossível a sua leitura sem o apropriado conhecimento da chave. O seu principal propósito é assegurar privacidade da informação protegendo o entendimento da mensagem oculta de qualquer um a qual ela não seja destinada.

- **Deciframento (ou decodificação)**: O deciframento é o processo inverso do ciframento; é a transformação de dados cifrados novamente em uma forma legível.

- **Texto simples**: É qualquer informação que está escrita de maneira legível.

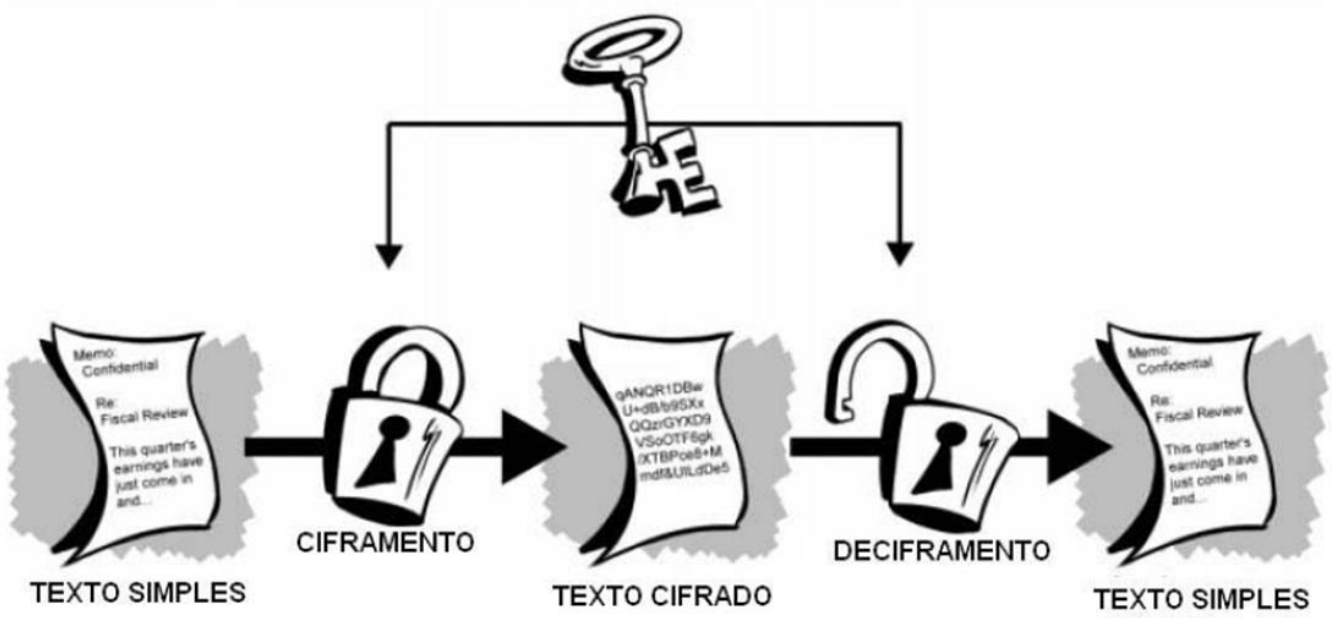
- **Texto cifrado**: É resultado de um texto simples que passou pelo processo de ciframento.

- **Chave**: A chave é um valor único utilizado por algoritmos de ciframento para criar versões únicas do texto codificado; isto faz com que uma mensagem, ao ser cifrada com chaves diferentes, apresente textos codificados diferentes.

- O **ciframento** e o **deciframento** são realizados por programas de computador chamados de cifradores e decifradores (algoritmos). Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar.

- Os **cifradores** e **decifradores** se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um texto cifrado.

- Assim, para manter uma informação secreta, basta cifrar a informação através de um algoritmo criptográfico reconhecido pela comunidade técnica, mantendo todos os cuidados técnicos especificados e manter em sigilo a chave.



Esquema de ciframento e deciframento.

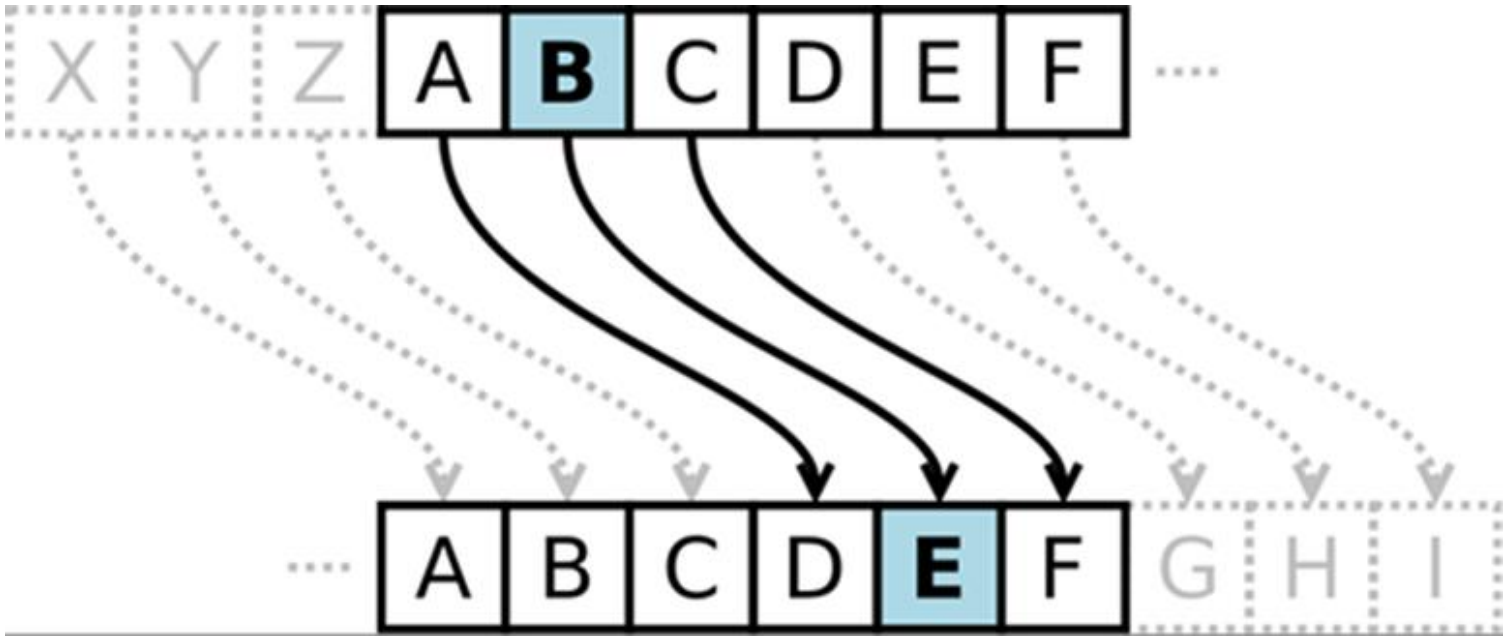
Panorama Histórico

- A criptografia é tão antiga quanto à própria escrita. Já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que a tecnologia de criptografia não mudou muito até meados do século passado.

Cifra de César

- A **Cifra de César** é um modelo histórico que foi utilizado pelos gregos na Grécia Antiga para proteger as mensagens militares onde uma letra do alfabeto era substituída por um número fixo de letras em posições seguintes. A transformação é feita alinhando dois alfabetos e rotacionar um para a esquerda ou para a direita. No exemplo abaixo a letra é substituída pela terceira letra a seguir

Cifra de César



Cítala ou bastão de Licurgo

- Uma cítala ou bastão de Licurgo foi uma ferramenta utilizada pelos gregos antigos mais precisamente por espartanos para se fazer uma cifragem por transposição. Consistia em um cilindro com uma faixa de papiro ou couro ao redor no qual era escrita a mensagem.

- A pessoa que escrevia a mensagem utilizava uma cilindro de um diâmetro pré-determinado onde era enrolada a tira para ser escrita, a pessoa que receberia a tira devia usar um cilindro de mesmo diâmetro para decifrar. Apesar do método ser rápido e difícil de cometer erros, era também facilmente quebrado o seu código.

Cítala ou bastão de Licurgo

Disco de cifra de Alberti

- O **disco de cifra de Alberti** é um disco que foi descrito por Leon Battista Alberti em 1467. O dispositivo é o primeiro exemplo do substituição poli alfabética no qual misturava alfabetos diferentes. Ele é feito por dois discos concêntricos e presos por um mesmo pino no centro. Cada um dos discos pode girar independente do outro, para a codificação os discos eram travados em uma determinada posição. Este dispositivo foi muito utilizado na Guerra Civil americana.

Disco de cifra de Alberti

Cifra de Vigenère

- Blaise de Vigenère em 1586 constituiu um método muito interessante; é a **cifra de Vigenère** que utiliza a substituição de letras. Tal processo consiste na sequência de várias cifras (como as de César) com diferentes valores de deslocamento alfanumérico. A partir desse período, Renascença, a criptologia começou a ser seriamente estudada no Ocidente e, assim, diversas técnicas foram utilizadas e os antigos códigos monoalfabéticos foram, aos poucos, sendo substituídos por polialfabéticos.
- A seguir podemos ver a tabela que era usada para codificação e decodificação por este método.

Cifra de Vigenère

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

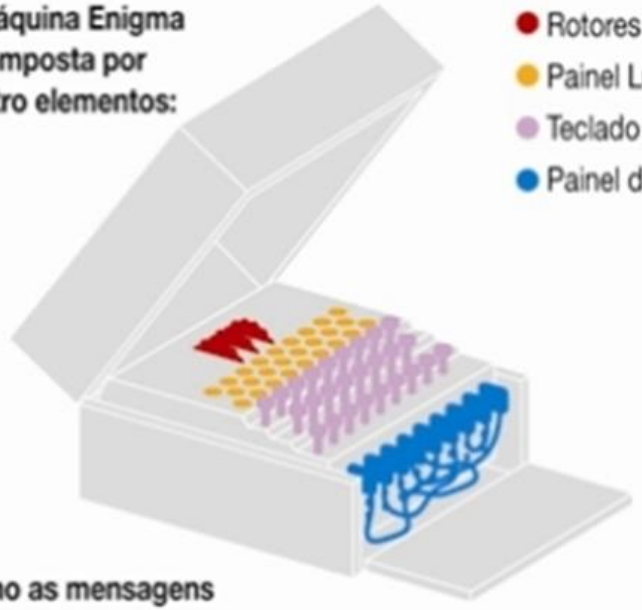
Panorama Histórico

- A história da criptografia da era moderna foi marcada pelo seu uso militar. Em situações de guerra nenhum comandante deseja que seus inimigos conheçam suas estratégias caso viesse interceptar uma mensagem.

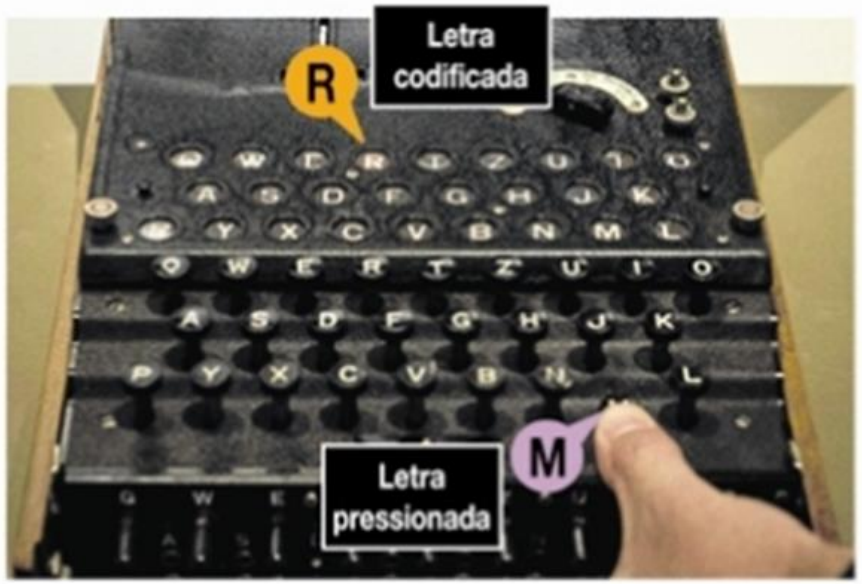
- O advento dos computadores, e a capacidade de processamento de dados sempre crescente, fizeram com que a criptografia se fizesse agora de forma digital.

A máquina Enigma

A máquina Enigma é composta por quatro elementos:



- Rotores e Refletores
- Painel Luminoso
- Teclado
- Painel de Conectores



Como as mensagens eram codificadas e enviadas:

1 Mensalmente, cada operador nazista recebia uma tabela (chamadas de code book) para configurar os quatro elementos da máquina. Todo dia havia mudanças nesses parâmetros. Dependendo da combinação, a máquina poderia produzir milhões de possibilidades de códigos.

2 O militar digitava uma letra no teclado e outra, diferente, aparecia iluminada no painel. A letra codificada devia ser anotada em um papel para compor o texto criptografado. A cada letra digitada, engrenagens giravam, impedindo que a mesma letra fosse reproduzida na sequência.

3 De posse da mensagem criptografada, anotada em um papel, o texto era transmitido por rádio via código morse. Ou seja, uma nova codificação era realizada.

4 Sintonizado na mesma frequência do rádio, um soldado em outro local anotava a mensagem em código morse. Com o texto, configura a máquina com os mesmos parâmetros e fazia o processo inverso para ler a mensagem original.

A máquina Enigma

- Durante a Segunda Guerra Mundial, versões da Enigma são usadas por praticamente todas as comunicações de rádio alemãs. Mesmo os boletins meteorológicos são codificados com a Enigma.

- Os espanhóis usaram uma versão comercial e menos segura da Enigma durante a Guerra Civil Espanhola. Os italianos também usaram a Enigma durante a Segunda Guerra Mundial, e a criptoanálise bem-sucedida da Enigma italiana pelos Aliados beneficiou os esforços de inteligência. Esta imprudência beneficia os Britânicos que fizeram a criptoanálise mais rapidamente.

- O serviço secreto francês conseguiu obter informações sobre as chaves mensais da Enigma por meio de espionagem e outras atividades de inteligência. Essas informações foram compartilhadas com os poloneses, que fizeram avanços significativos na criptoanálise da Enigma antes mesmo do início da Segunda Guerra Mundial.

- O código foi quebrado em 1943 pelos “aliados” com a ajuda de meios eletromecânicos.

- A criptoanálise bem-sucedida da máquina Enigma foi um esforço conjunto dos Aliados e envolveu várias técnicas e avanços tecnológicos.

- Embora os poloneses tenham feito progressos iniciais, o trabalho contínuo de criptoanalistas britânicos, incluindo Alan Turing, e o uso de máquinas eletromecânicas como a "Bomba" permitiram que os Aliados quebrassem o código da Enigma alemã.

- Esse avanço foi um dos marcos cruciais na Segunda Guerra Mundial, permitindo aos Aliados ler comunicações alemãs e obter informações vitais sobre os planos e movimentos das forças inimigas.

Para saber mais...

Panorama Histórico

- Em 1976, a IBM desenvolveu um sistema criptográfico denominado **Data Encryption Standard (DES)**, que logo foi aprovado pelos órgãos de normatização do governo americano. O **DES** baseia-se em elaborados sistemas matemáticos de substituição e transposição os quais fazem com que seja particularmente difícil de ser rompido um ciframento. O **DES** é um exemplo clássico de criptografia simétrica.

- O **RSA** é um sistema criptográfico de chave pública amplamente aceito e divulgado, desenvolvido em abril de 1977, pelos professores do Massachusetts Institute of Technology (MIT) Ronald Rivest e Adi Shamir e pelo professor da University of Southern California (USC) Leonard Adleman, batizado com as iniciais de seus nomes.

- Mais tarde a patente do RSA foi registrada pelo MIT que a cedem a um grupo denominado Public Key Partners (PKP) para uso doméstico. Esta patente foi expirada por completo em setembro de 2000.

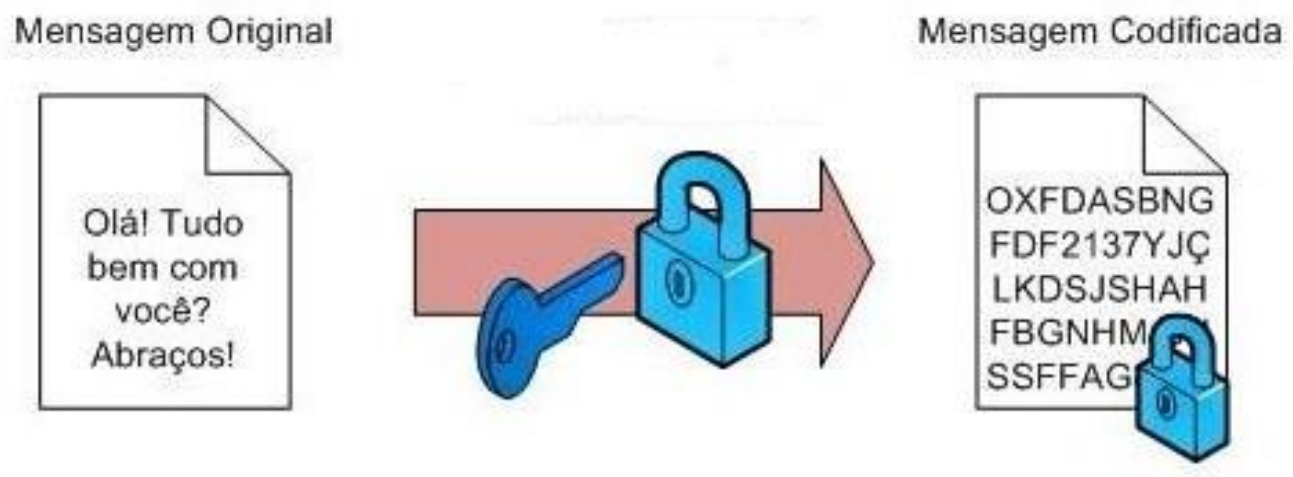
- Em 1991, o programador Phil Zimmermann autorizou a publicação em boletins eletrônicos e grupos de notícias de um programa por ele desenvolvido e batizado como **Pretty Good Privacy (PGP).**

- O **PGP** tem como base entre outros o algoritmo do **RSA**. Quando Zimmermann publicou o **PGP** se viu em problemas com o departamento de estado norte-americano que abriu uma investigação para determinar se ele havia violado as restrições de exportação de criptografia ao autorizar a divulgação do código fonte do **PGP** na internet.

Nos dias atuais, com o aumento do comércio e de transações eletrônicas que requerem algum tipo de segurança, a criptografia tornou-se uma ferramenta fundamental para a utilização da internet.

Criptografia

- Quando se trata de criptografia, a informação não é alterada. O significado da mesma que é escondido.
- Transforma-se o texto legível em ilegível.
- Elementos fundamentais:
  - Algoritmo criptográfico
  - Chave criptográfica



- Cada algoritmo possui suas características, como veremos nas aulas a seguir.
- Sobre a chave criptográfica, a grande questão é que ela deve ser SECRETA e ALEATÓRIA!!!

POR QUE USAR UMA CHAVE SECRETA?

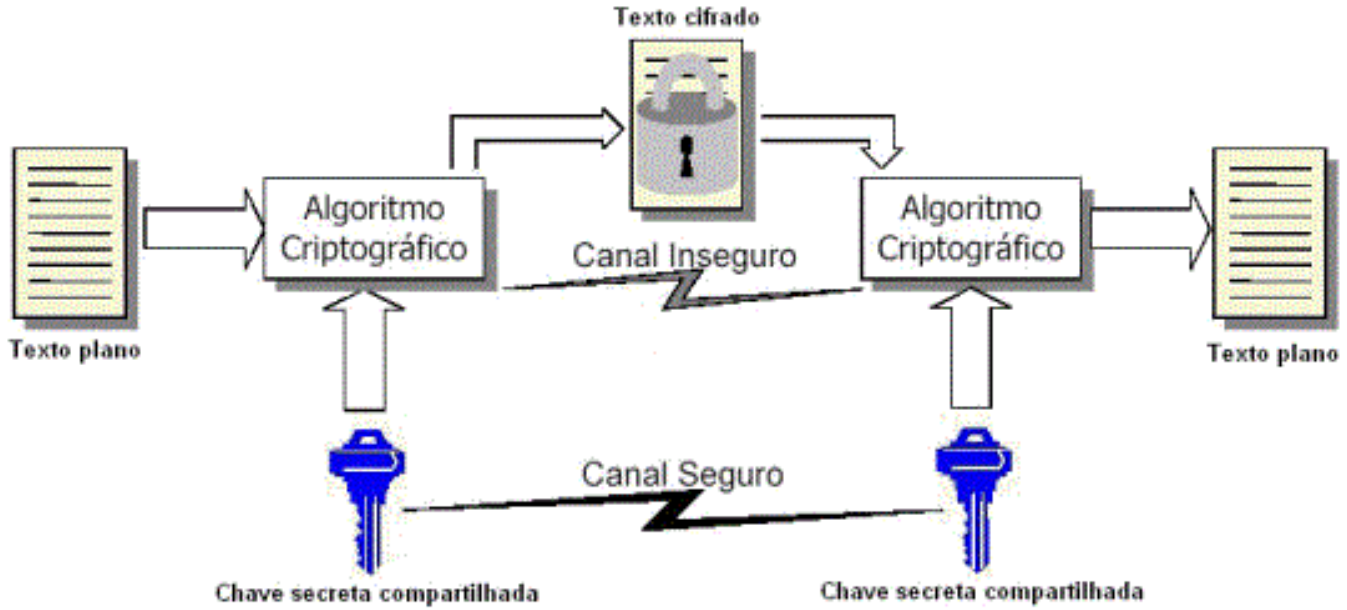
- O algoritmo criptográfico não pode ser secreto... Você precisa que o receptor da mensagem conheça seu método criptográfico.
- Por isso a chave deve ser secreta... Se você transmitir a informação cifrada com a chave junto, qualquer pessoa que interceptar a informação pode decifrá-la.

- Antigamente um código (segredo) era usado na criptografia... Hoje em dia usam-se as chaves criptográficas.
- O método de criação da chave criptográfica vai depender do algoritmo criptográfico que está sendo usado.
- O tamanho da chave também depende do algoritmo em uso.
- Temos que ter chaves aleatórias.

CRIPTOGRAFIA SIMÉTRICA

- CRIPTOGRAFIA CONVENCIONAL
- Apenas uma chave criptográfica e um algoritmo criptográfico são usados no processo de cifrar e decifrar a informação.
- Principais tipos de ataque para quebrar criptografia simétrica:
  - Vulnerabilidades no algoritmo
  - Força bruta
- Única forma de criptografia usada até os anos 70.

- Componentes da criptografia simétrica:
  - Informação legível
  - Algoritmo de criptografia
  - Chave secreta
  - Informação cifrada
  - Algoritmo de decifração (o mesmo da criptografia)



- Requisitos para que a criptografia simétrica seja mais segura:
  - A chave não pode ser descoberta pela pessoa mal intencionada
  - O compartilhamento da chave deve ser feito de forma **SEGURA**!!!

COMO COMPARTILHAR A CHAVE DE MANEIRA SEGURA???????

- O algoritmo não precisa ser secreto, assim como o texto cifrado, se a chave estiver segura durante todo o processo.

- Vantagens:
  - Mais rápida
- Desvantagens:
  - Trabalha com chaves menores
  - Necessidade de canal seguro para a troca da chave
  - Gerenciar muitas chaves.
- Agora veremos alguns algoritmos de criptografia simétrica.

- DES
  - Derivado do Lucifer (IBM)
  - Década de 70
  - Usava chaves de 128 bits
  - Foi alterado pela NSA (National Security Agency dos EUA)
  - Chaves passaram a ter 56 bits
  - Trabalha com blocos de 64 bits
  - Chave de 56 bits é fraca

- 3DES
  - Criado para suprir as deficiências do DES
  - Executa o DES 3 vezes
  - Trabalha com blocos de 64 bits
  - Cifra cada bloco com a 1ª. chave, cifra o resultadocom a 2ª. chave e cifra o novo resultado a 3ª. chave
  - O processo de decifração consiste na apresentação das chaves ao contrário

EXEMPLO DE FUNCIONAMENTO DO 3DES - CIFRAR

EXEMPLO DE FUNCIONAMENTO DO 3DES - DECIFRAR

- AES
  - Criado para substituir o DES
  - Foi criado através de um concurso
  - O algoritmo escolhido e que deu origem ao AES foi o Rijndael
  - Tornou-se padrão em 2002
  - Usa chaves de 128, 192 ou 256 bits
  - Ótimo desempenho
  - Usado no e-cpf e no WPA2
  - Funciona muito bem em smart cards
- RC4
  - Desenvolvido em 1987 por Ron Rivest
  - Chave variável de 8 a 2048 bits
  - Trabalha em bloco de byte (8 bits)
  - Usado pelo SSL (browsers) e nas redes sem fio WEP
  - Se usadas chaves de mais de 128 bits era bastante resistente a ataques
  - Uso não recomendado desde 2015

- **Simulador 3DES on-line**
  - Encriptar:
    - https://www.browserling.com/tools/triple-des-encrypt
  - Decriptar:
    - https://www.browserling.com/tools/triple-des-decrypt

CRIPTOGRAFIA ASSIMÉTRICA

- Usa 2 chaves no processo de cifrar e decifrar uma informação, sendo uma diferente da outra.

- Usa o conceito de números primos (número dividido por um e por ele mesmo) e da aritmética modular (o resultado sempre está dentro de um intervalo específico).

- Na criptografia simétrica, o envio das chaves deve ser seguro. Aqui, o armazenamento da chave privada é que deve ser seguro.

- Como dito anteriormente, 2 chaves são usadas, uma chave pública e uma chave privada.

Como podemos ver acima, Regina quer mandar uma informação confidencial para Breno. Usando a criptografia assimétrica, ela (que já recebeu previamente a chave pública de Breno) cifrou a mensagem e enviou para ele, que por sua vez, usou sua chave privada (e secreta) para decifrar a informação.

A chave privada é pessoal e intransferível, e será usada sempre no processo de DECIFRAR uma informação, e também para GERAR a chave pública.

Já a chave pública é “derivada” da chave privada do indivíduo, e ele compartilha a mesma com as entidades que desejam lhe enviar algo. Essas entidades irão usar a chave pública para CIFRAR a informação.

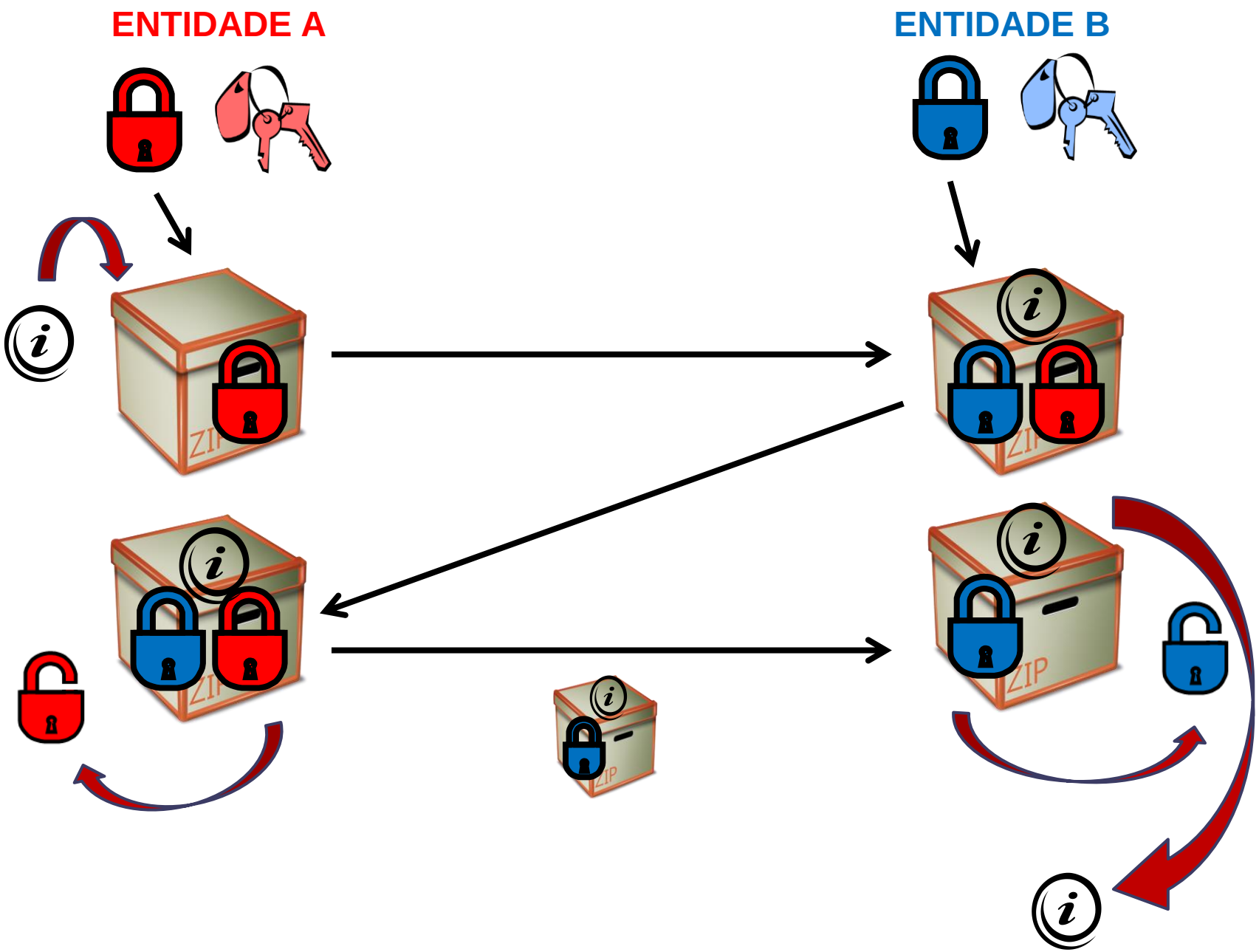
Para decifrar a informação, apenas a chave privada que deu origem a chave pública poderá ser usada.

Assim, se uma pessoa mal intencionada acessar a informação cifrada, mesmo que ela tenha acesso à chave pública, ela não irá conseguir ler essa informação, pois ela não terá a chave privada (que está em posse do receptor).

- A criptografia assimétrica é mais lenta que a criptografia simétrica, devido ao tamanho das chaves.
- Na criptografia assimétrica, não precisamos de um meio seguro para transmitir a informação.
- A criptografia assimétrica é mais segura.
- Agora veremos alguns algoritmos de criptografia assimétrica.

ACORDO DE CHAVES DIFFIE – HELLMAN

- Criado por Whitfield Diffie e Martin Hellman
- Começou a ser criado em 1974
- Usa o conceito de caixas com cadeados para transmitir informações de maneira segura.

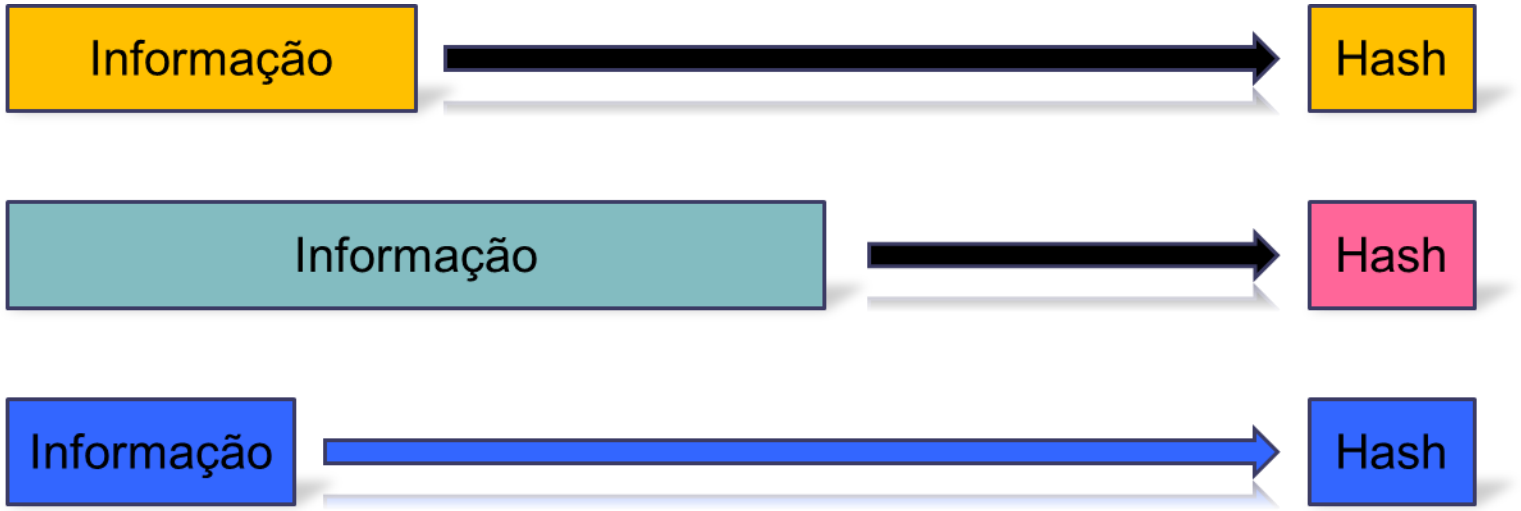

ENTIDADE A
ENTIDADE B
ZIP

RSA

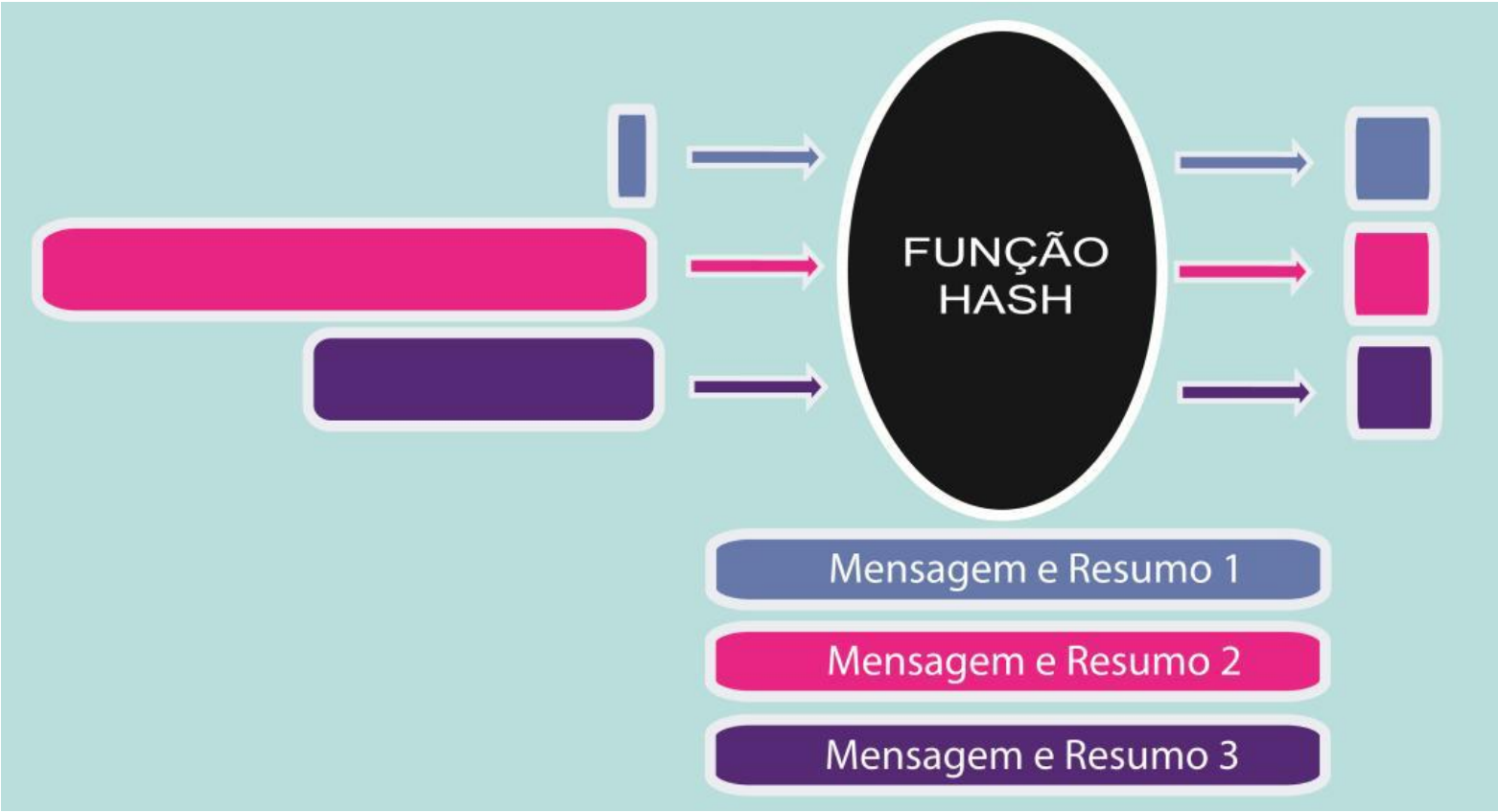
- Usa o conceito do acordo Diffie Hellman
- Projetado por **R**on Rivest, Adi **S**hamir e Len **A**dleman
- Foi criado em 1978
- Gera o par de chaves com base em números primos e aritmética modular
- Principais formas de ataque ao RSA:
  - Força bruta
  - Ataques matemáticos (por fatoração dos números primos)

FUNÇÃO HASH

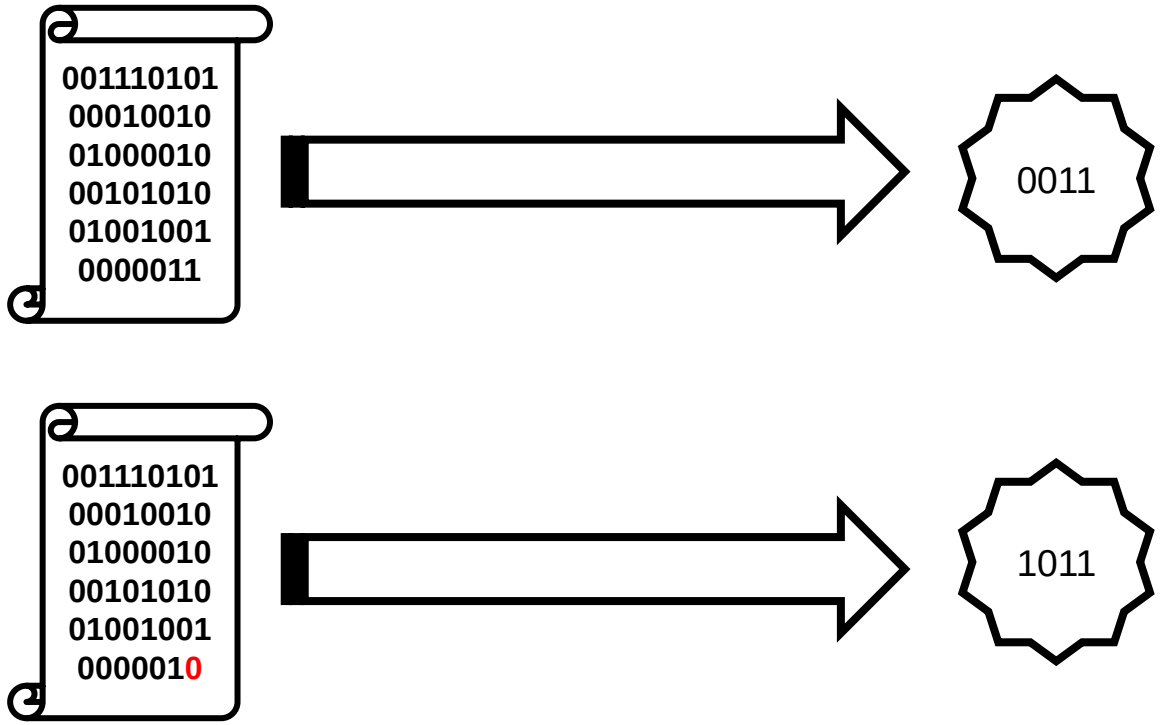
- Função criada para prover, principalmente, integridade
- Gera um resumo dos dados
- É usado na assinatura digital
- A entrada pode ter tamanho variável, mas a saída sempre tem tamanho fixo



- A função hash nada mais é que uma função matemática que analisa todos os bits da informação original e gera um código, o **RESULTADO HASH**.



- Se um bit for alterado na informação original, o resumo hash será alterado.
- Com isso, é possível verificar se a informação foi alterada durante seu transporte, por exemplo.



- Propriedades da função hash:
  - Pode ser aplicada a qualquer tamanho de informação
  - A saída (resultado hash) é sempre fixa
  - Deve ser simples para que sua implementação seja viável.

- A função hash garante a integridade da informação, ou seja, é possível verificar se a informação foi alterada indevidamente.

- MAS LEMBRE-SE: ela NÃO garante a confidencialidade, e NÃO garante que a informação não será alterada... Ele apenas permite verificar se alterações ocorreram.

O QUE PODEMOS USAR JUNTO COM A FUNÇÃO HASH PARA GARANTIR A CONFIDENCIALIDADE???

- Funções hash com resultado hash menor que 160 bits são consideradas inseguras.
- Tipos de ataque a função hash:
  - Força bruta
  - Criptoanálise
    - Criptoanálise: estudo dos procedimentos necessários para comprometer as técnicas criptográficas e, mais genericamente, os serviços de segurança da informação.

- Agora veremos 2 funções hash muito usadas:

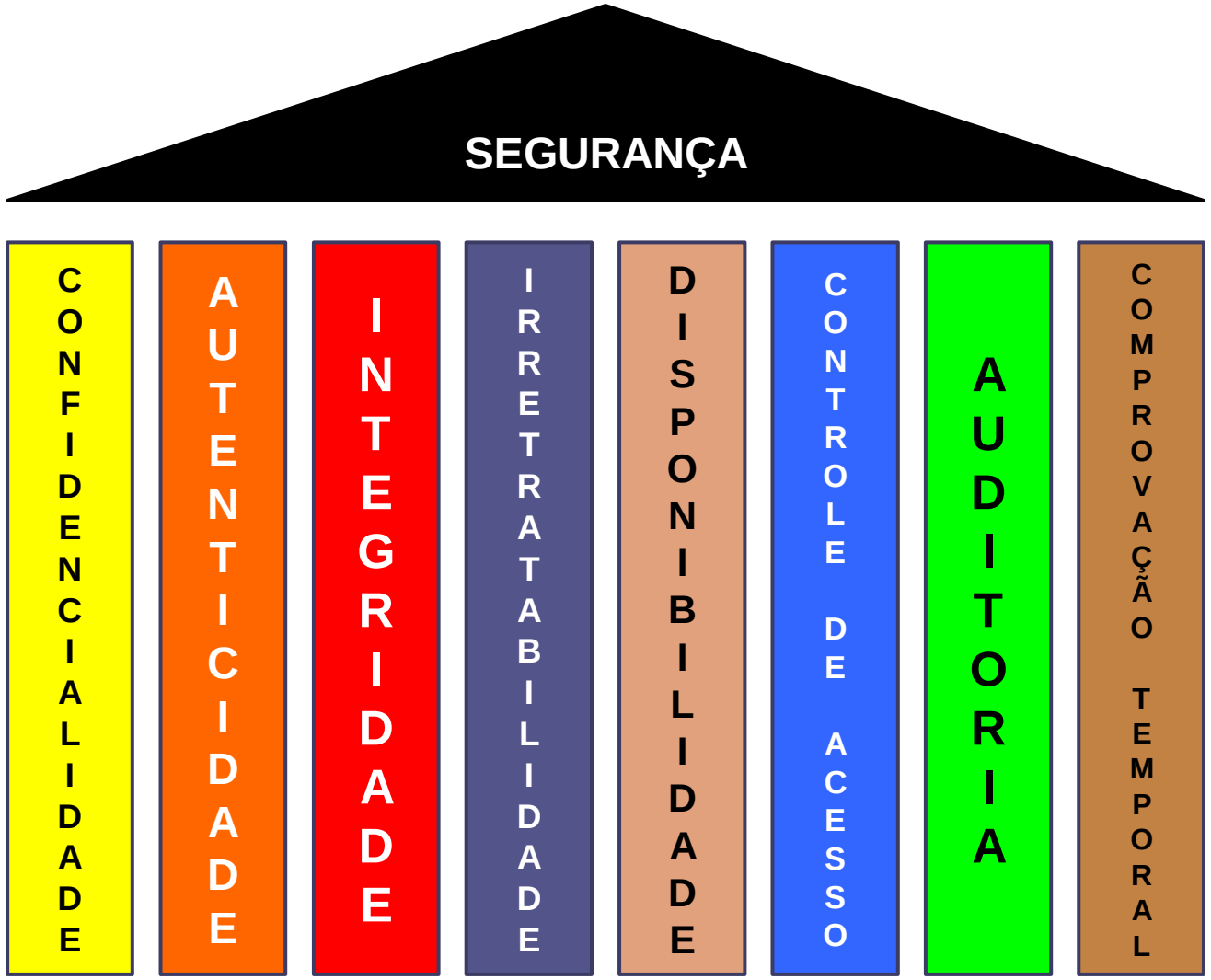
- **MD5**
  - Criada por Ron Rivest
  - Desenvolvido em 1991
  - A ideia era ter uma função hash rápida e resistente a ataques
  - Sucessora da MD2
  - Foi o algoritmo mais usado na época em que foi criado e é usado até hoje
  - Usado na emissão de certificados digitais
  - Saída: 16 bytes (128 bits)

- **SHA-1**
  - Secure Hash Algorithm
  - Desenvolvido pelo NIST (Instituto Nacional de Padrões e Tecnologia)
  - Criado em 1993 (SHA) e revisado em 1995 (SHA-1)
  - Baseado no MD4
  - Depois dele foram criados o SHA-256, o SHA-384 e o SHA-512
  - A SHA-1 é a mais usada

Característica	SHA-1	SHA-256	SHA-384	SHA-512
Tamanho do resumo (bits)	160	256	384	512
Tamanho do bloco (bits)	512	512	1024	1024
Etapas	80	64	80	80

- **Gerador on-line de Hash MD5**
  - http://md5-hash-online.waraxe.us/

SERVIÇOS DE SEGURANÇA



CONFIDENCIALIDADE

- Manter a informação confidencial, acessível apenas pelas pessoas que precisam fazer uso dela
- Primeiro serviço buscado em segurança
- Temos uma necessidade de manter a informação segura, longe de acessos indevidos por parte de entidades não autorizadas
- Podemos manter a confidencialidade protegendo o meio físico ou implementando a criptografia

AUTENTICIDADE

- Garantir que a entidade que está acessando a informação é ela mesma
- Confirmação de identidade; identificação
- Podemos efetuar a autenticação da identidade da entidade (quando ela se loga em um sistema por exemplo)
- A assinatura digital é uma forma de se garantir a autenticidade

INTEGRIDADE

- Garantir que a informação não será alterada indevidamente em NENHUM momento
- Alcançada por meio das funções hash
- Usada nos certificados digitais

IRRETRATABILIDADE

- Assegurar que a entidade não será repudiada ou retratada
- Irretratabilidade de transmissão: garantir que a entidade que realizou uma transmissão não possa revogar tal ato e que o receptor possa conferir isso
- Irretratabilidade de recepção: garantir que a entidade que recebeu uma informação não possa revogar tal ato e que o transmissor possa conferir isso

DISPONIBILIDADE

- Garantir que a informação estará à disposição das entidades autorizadas sempre que elas precisarem fazer uso da mesma
- Principais ações para garantir disponibilidade: mitigações contra negações de serviço, definição real das necessidades de recursos nos serviços/ processos envolvidos

CONTROLE DE ACESSO

- Garantir que o uso não autorizado da informação seja impedido
- Controlar qual entidade pode fazer o que com os recursos disponíveis, suas permissões
- Objetivo: que apenas entidades autorizadas tenham acesso aos recursos, de acordo com o administrador

AUDITORIA

- Manter mecanismos para monitorar as ações dos usuários
- Usado para rastrear eventos ocorridos

COMPROVAÇÃO TEMPORAL

- Visa provar a existência de uma informação através de uma autoridade confiável do tempo, anterior ao momento de assinatura digital dessa informação.
- Serviço realizado por carimbadores de tempo.
- Primordial para o funcionamento adequado de gerenciamento de documentos eletrônicos

ASSINATURA DIGITAL

- Serviço de segurança alcançado por meio de criptografia / hash
- Visa buscar integridade e autenticidade.
- Integridade: alcançada por meio do uso de algoritmos de hash
- Autenticidade: alcançada por meio do processamento criptográfico de chaves assimétricas.

- Componentes necessários no processo de assinatura digital:
  - A entidade assinante deve possuir um par de chaves assimétricas (Kpri e Kpub);
  - A entidade assinante deve possuir à sua disposição um algoritmo hash para realizar o resumo do bloco de dados assinados;
  - A entidade assinante deve possuir à sua disposição um algoritmo criptográfico assimétrico que será utilizado para realizar a criptografia do resumo da mensagem.

- Existem 2 formas de realizar o processo de assinatura digital:

1. **Assinatura digital direta:**
   - Apenas emissor e receptor são envolvidos no processo
   - O receptor tem que conhecer a chave pública do emissor (assinante)
   - A chave privada do emissor tem que ser secreta (como toda chave privada)

2. **Assinatura digital arbitrada:**
   - Um arbitro (entidade) confiável é incluído no processo
   - Ele quem realiza as verificações para ver se a assinatura digital é válida.

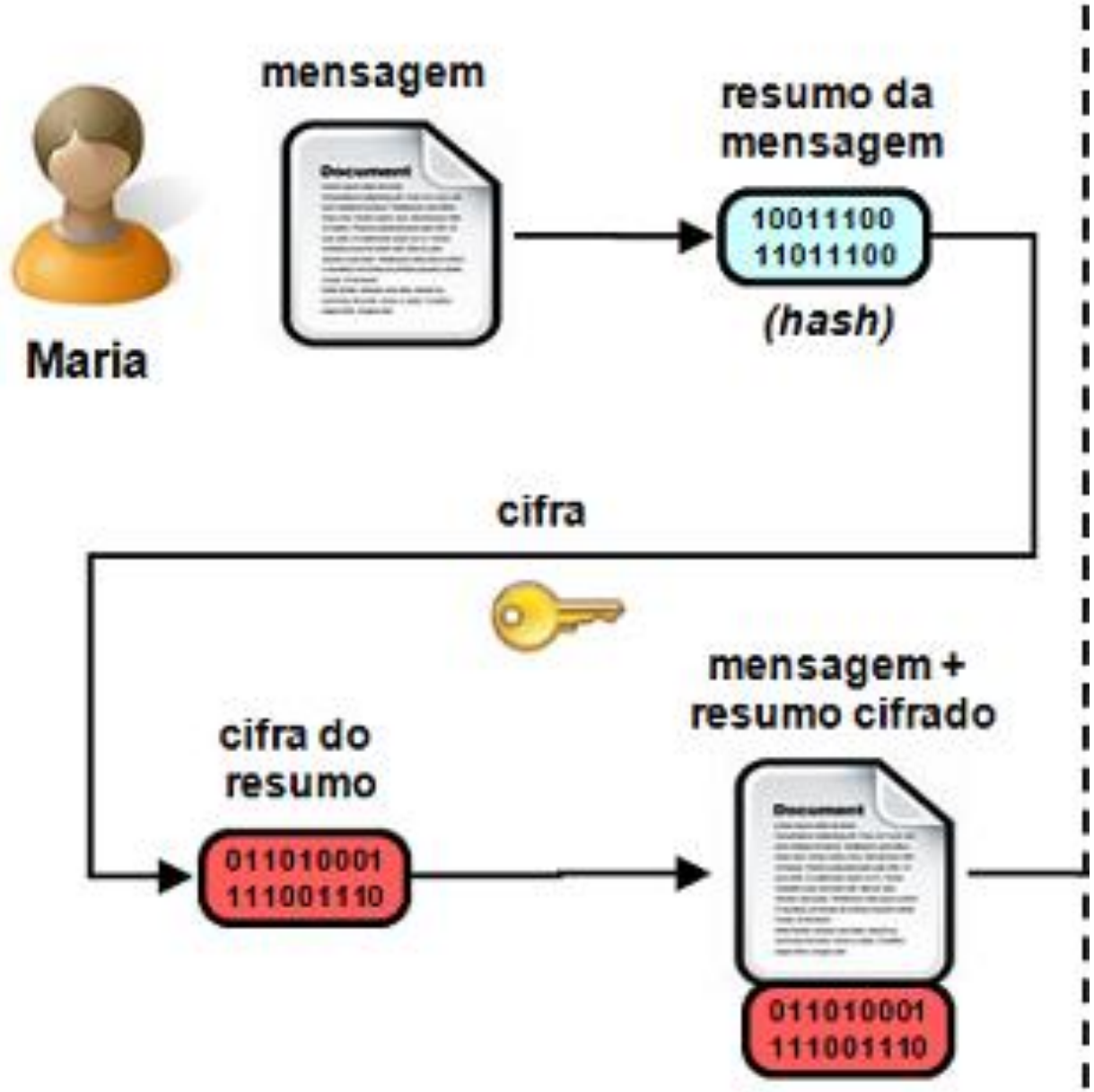
- Propriedades da assinatura digital:
  - Integridade
  - Tem sempre um resumo criptográfico (hash)
  - Permite que se verifique alterações na informação original
  - Usa chave criptográfica
  - Deve ser simples (realização e verificação)
  - Deve ser impossível de falsificar
  - A chave privada do assinante deve ser secreta
  - Não garante o momento da assinatura

- Processo de geração da assinatura digital:

1. Realiza-se o cálculo do resumo hash submetendo a mensagem a ser assinada à função hash escolhida

2. Submete-se o resumo hash gerado no passo anterior ao algoritmo de criptografia assimétrico escolhido usando a chave privada do assinante

3. Monta-se o bloco de dados que será enviado
   - Bloco de dados originais (chamado agora de bloco de dados assinado)
   - Bloco de assinatura (resumo hash cifrado com a chave privada da entidade assinante).

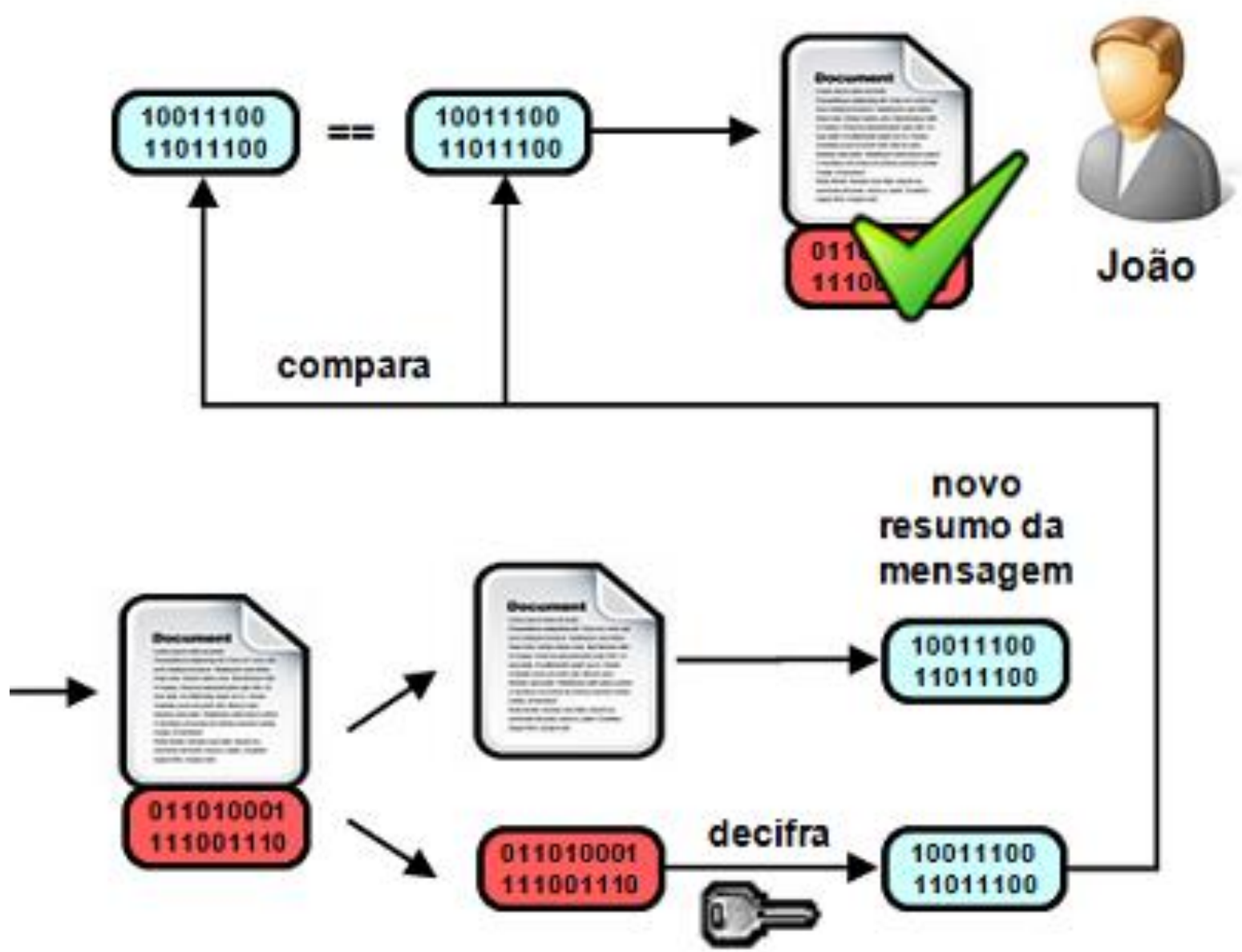

mensagem
resumo da mensagem
10011100
11011100
(hash)
Maria
cifra
mensagem + resumo cifrado
cifra do resumo
011010001
111001110
011010001
111001110

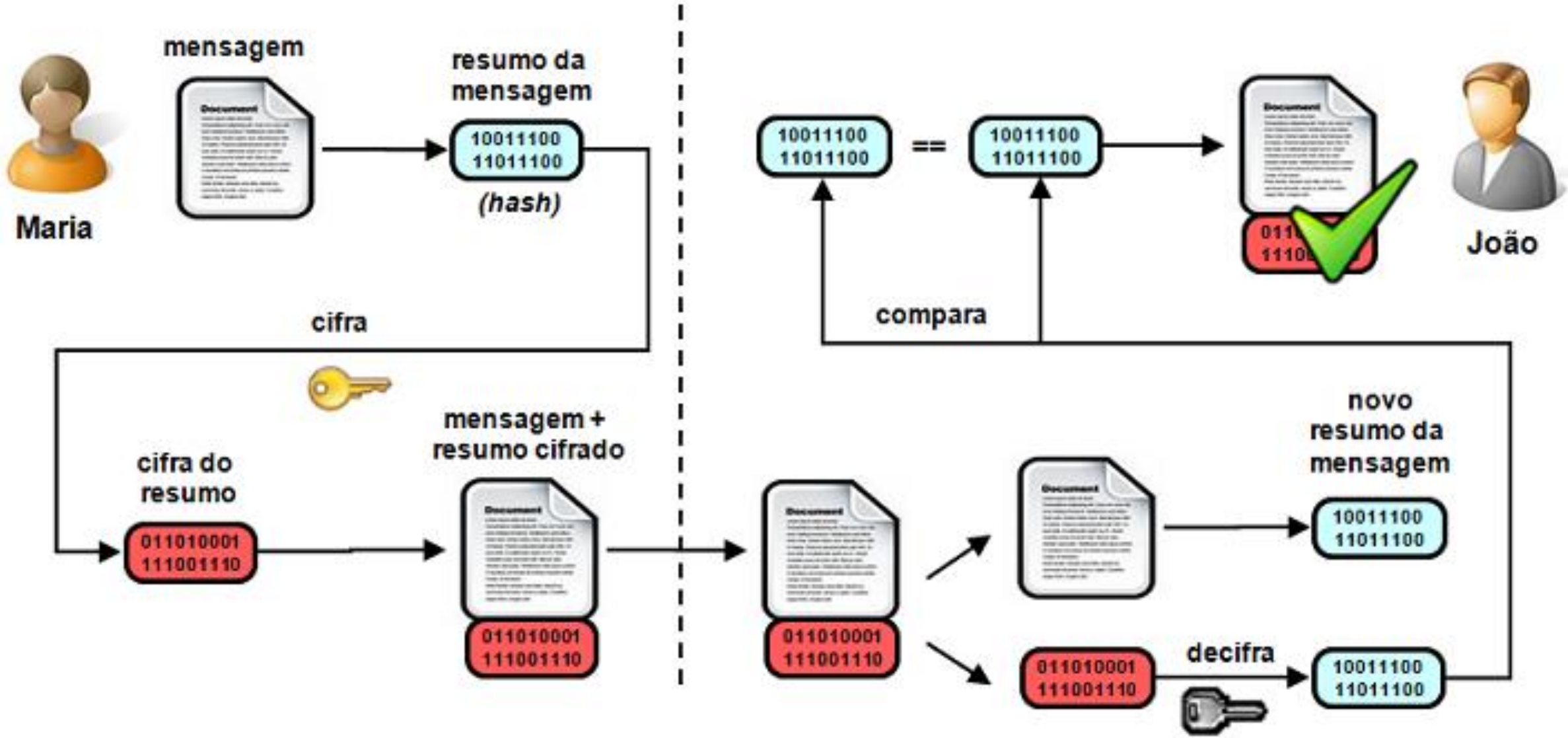
- Processo de verificação da assinatura digital:

1. O receptor submete o bloco de dados assinados (não a assinatura) à mesma função hash usada no processo de assinatura digital, gerando assim um resumo hash novo

2. O receptor decifra o resultado da assinatura digital enviado pelo emissor usando o mesmo algoritmo assimétrico com a chave pública do assinante, obtendo o resumo hash protegido pela criptografia assimétrica

3. O receptor compara o resumo hash novo que ele gerou com o resumo hash que ele descriptografou. Se os resultados forem iguais, a assinatura digital será considerada válida.


10011100
11011100
==
10011100
11011100
João
compara
novo
resumo da
mensagem
011010001
111001110
10011100
11011100
011010001
111001110
decifra
10011100
11011100

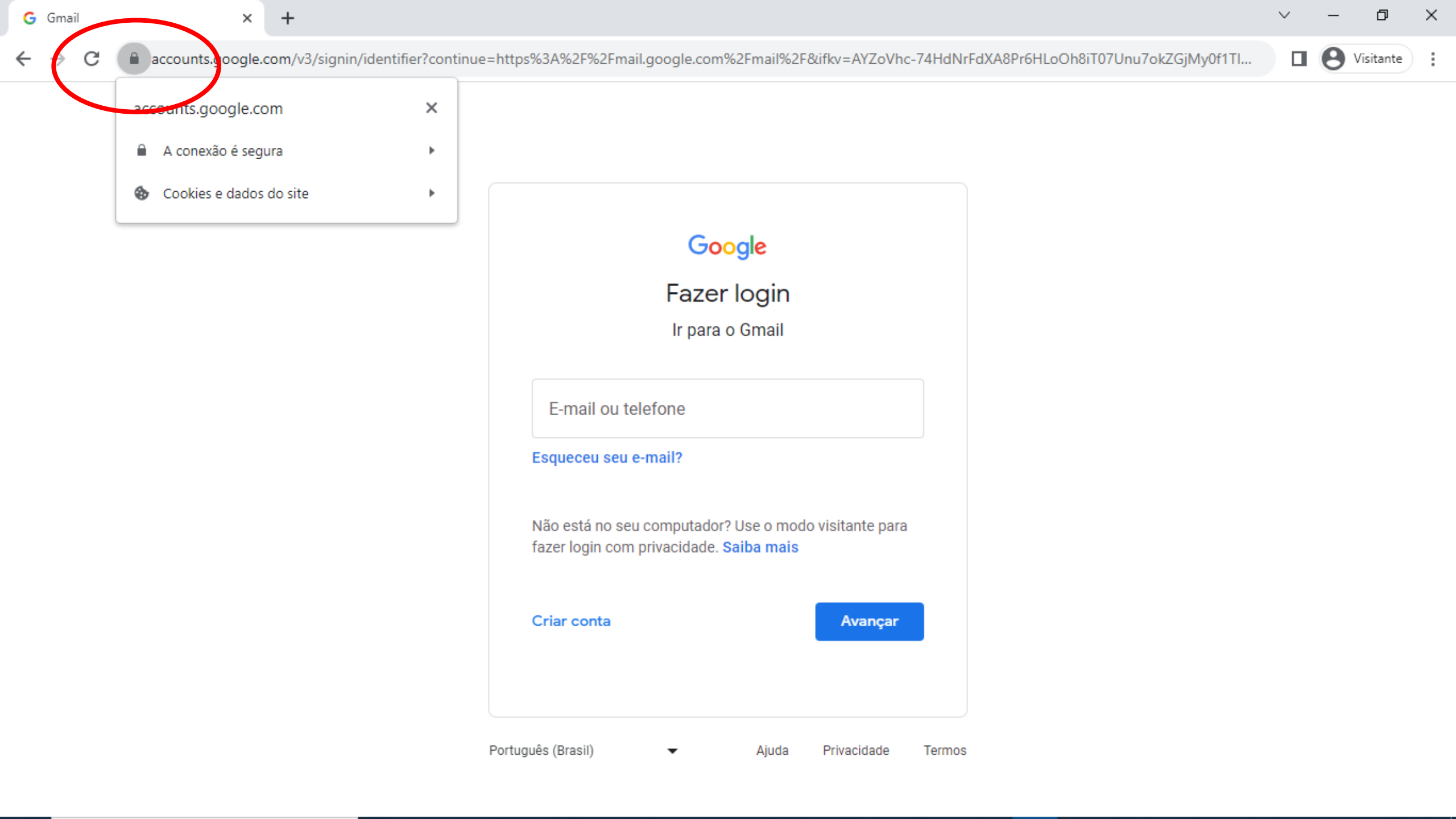

mensagem
resumo da mensagem
10011100 11011100
(hash)
Maria
cifra
cifra do resumo
011010001 111001110
mensagem + resumo cifrado
011010001 111001110
10011100 11011100 == 10011100 11011100
compara
João
novo resumo da mensagem
10011100 11011100
decifra
011010001 111001110
10011100 11011100

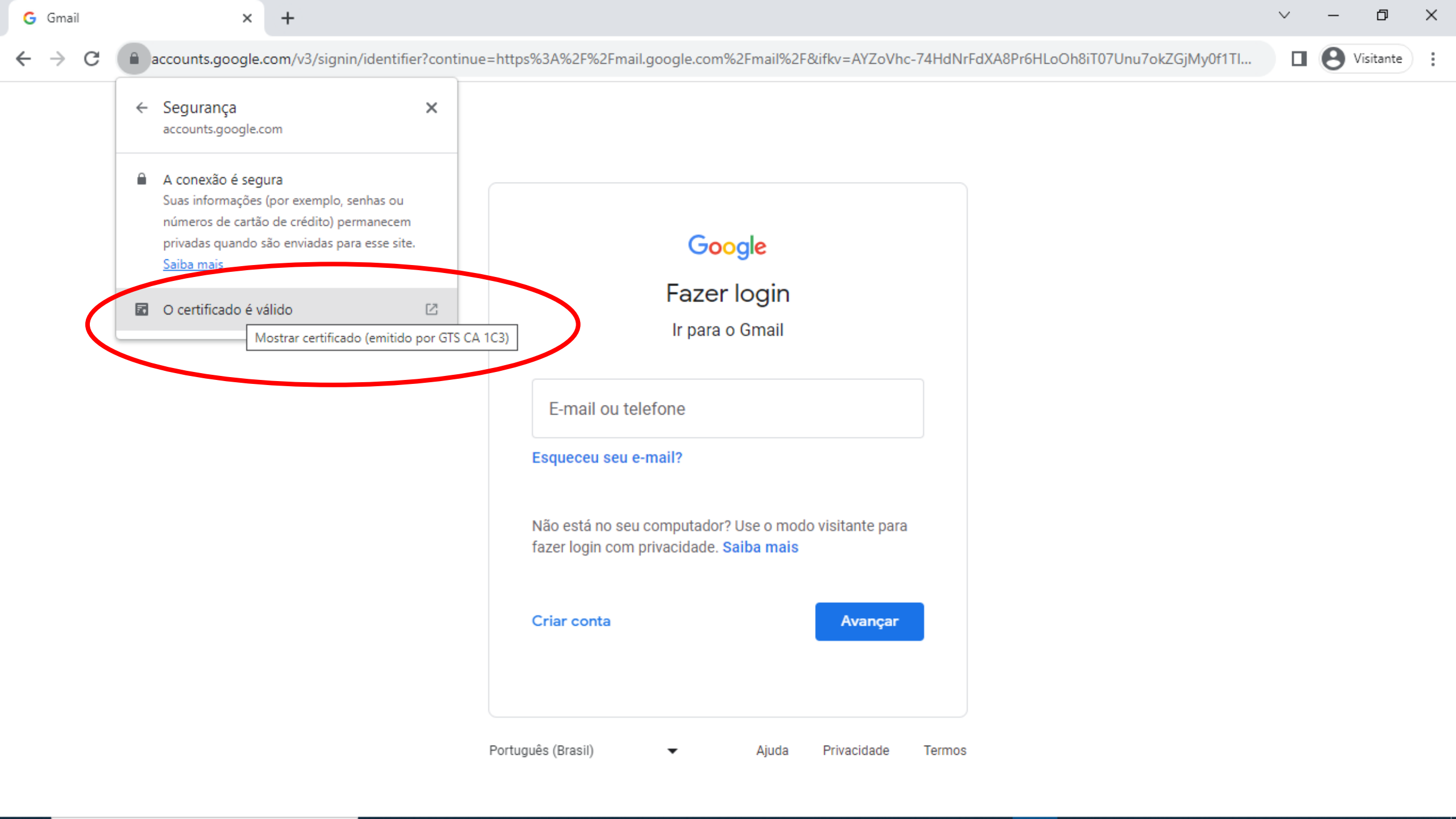
Certificados Digitais

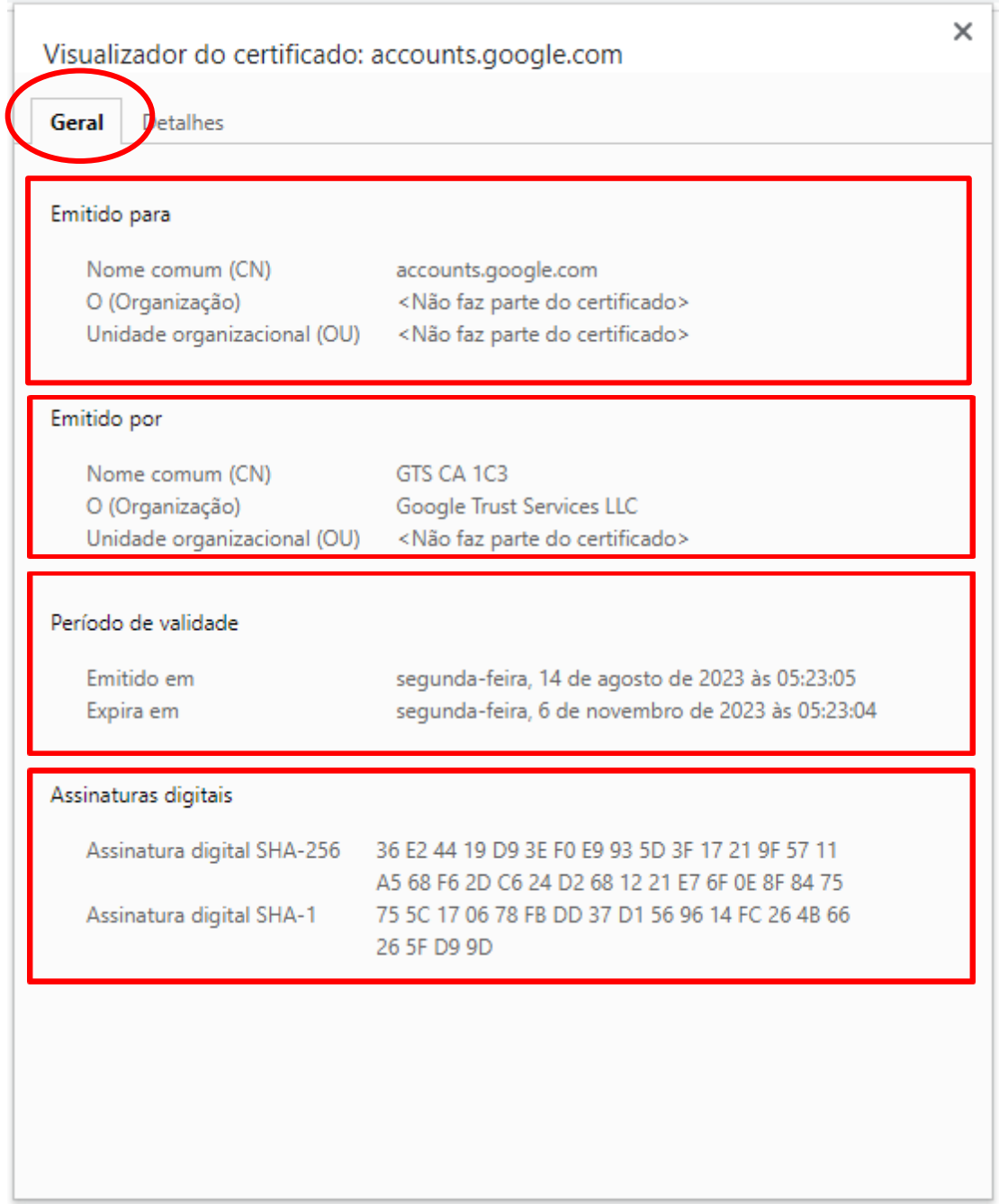
- Documentos digitais que atestam de forma legal a identidade de uma entidade.
- É associado a um par de chaves criptográficas assimétricas, sendo que somente a chave pública encontra-se disponível no certificado digital.
- Objetivo: distribuir de forma confiável e segura a chave pública de uma entidade final e conferir sua identidade junto à AC responsável por aquele certificado.

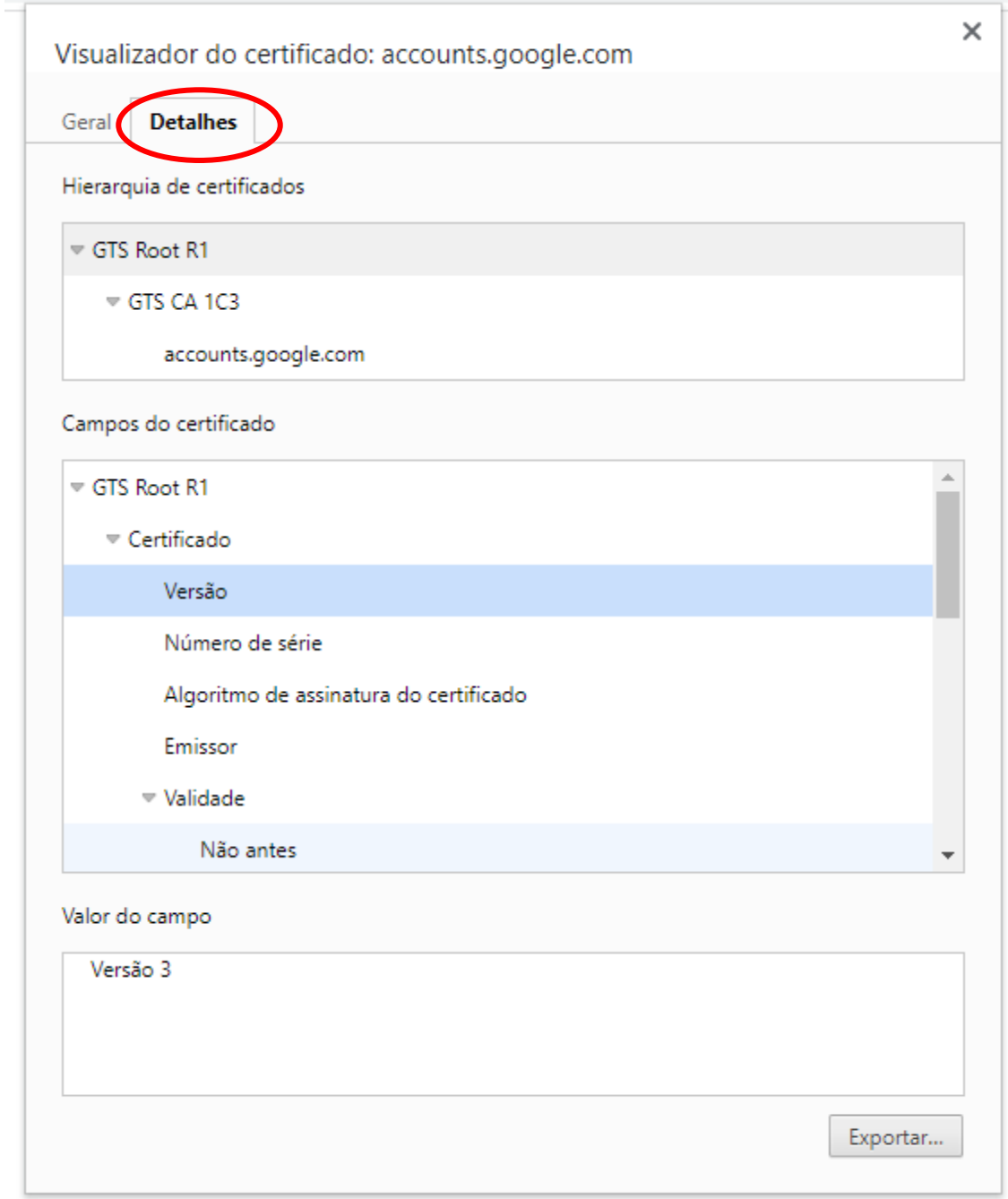
- Repositório de Certificados Digitais (RCD)
  - Local onde pode-se divulgar (e consultar) os certificados digitais emitidos pelas ACs.

- Lista de Certificados Revogados (LCR)
  - Lista que permite qualquer entidade realizar consultas sobre o status de um certificado digital.
  - É de responsabilidade da AC.
  - Deve ser uma lista pública e de fácil acesso.


Gmail
accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&ifkv=AYZoVhc-74HdNrFdXA8Pr6HLoOh8iT07Unu7okZGjMy0f1TI...
Visitante
accounts.google.com
A conexão é segura
Cookies e dados do site
Google
Fazer login
Ir para o Gmail
E-mail ou telefone
Esqueceu seu e-mail?
Não está no seu computador? Use o modo visitante para fazer login com privacidade. Saiba mais
Criar conta
Avançar
Português (Brasil)
Ajuda
Privacidade
Termos


Gmail
accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&ifkv=AYZoVhc-74HdNrFdXA8Pr6HLoOh8iT07Unu7okZGjMy0f1TI...
Visitante
Segurança
accounts.google.com
A conexão é segura
Suas informações (por exemplo, senhas ou números de cartão de crédito) permanecem privadas quando são enviadas para esse site.
Saiba mais
O certificado é válido
Mostrar certificado (emitido por GTS CA 1C3)
Google
Fazer login
Ir para o Gmail
E-mail ou telefone
Esqueceu seu e-mail?
Não está no seu computador? Use o modo visitante para fazer login com privacidade. Saiba mais
Criar conta
Avançar
Português (Brasil)
Ajuda
Privacidade
Termos


Visualizador do certificado: accounts.google.com
Geral
Detalhes
Emitido para
Nome comum (CN) accounts.google.com
O (Organização) <Não faz parte do certificado>
Unidade organizacional (OU) <Não faz parte do certificado>
Emitido por
Nome comum (CN) GTS CA 1C3
O (Organização) Google Trust Services LLC
Unidade organizacional (OU) <Não faz parte do certificado>
Período de validade
Emitido em segunda-feira, 14 de agosto de 2023 às 05:23:05
Expira em segunda-feira, 6 de novembro de 2023 às 05:23:04
Assinaturas digitais
Assinatura digital SHA-256 36 E2 44 19 D9 3E F0 E9 93 5D 3F 17 21 9F 57 11 A5 68 F6 2D C6 24 D2 68 12 21 E7 6F 0E 8F 84 75
Assinatura digital SHA-1 75 5C 17 06 78 FB DD 37 D1 56 96 14 FC 26 4B 66 26 5F D9 9D


Visualizador do certificado: accounts.google.com
Geral
Detalhes
Hierarquia de certificados
GTS Root R1
GTS CA 1C3
accounts.google.com
Campos do certificado
GTS Root R1
Certificado
Versão
Número de série
Algoritmo de assinatura do certificado
Emissor
Validade
Não antes
Valor do campo
Versão 3
Exportar...

Infraestrutura de chaves públicas brasileira (ICP-Brasil)

INFRAESTRUTURA DE CHAVES PÚBLICAS

- **Public Key Infrastructure – PKI**
- **Objetivo**: ser um mecanismo para o gerenciamento do ciclo de vida dos certificados digitais e os pares de chaves assimétricos.
- Além disso, o ICP permite a verificação de identidade de uma entidade, associando uma identidade digital a uma entidade real.

- **Principal função do ICP:** estabelecimento da confiança entre as partes envolvidas, tanto no processo de assinatura digital quanto na autenticação e validação do certificado digital.

MEDIDA PROVISÓRIA MP 2.200/2001

- Em 2001 o governo federal brasileiro, por meio da medida provisória 2200, criou a infraestrutura de chaves públicas brasileira, a ICP-BRASIL.

- Suas responsabilidades vão desde a elaboração de normas e procedimentos de homologação de equipamentos de certificado digital até a emissão de certificados digitais.

- A ICP-BRASIL está abaixo da Casa Civil (ITI – Instituto Nacional de Tecnologia da Informação).

- Como o ITI não possui pessoal técnico especializado, toda a parte de homologações fica por conta de um laboratório terceirizado, nomeado de LEA (Laboratório de Ensaios e Auditoria).

- O primeiro LEA do Brasil foi instituído pelo LSI-TEC (Laboratório de Sistemas Integráveis Tecnológico), proveniente da USP.

ICP-Brasil

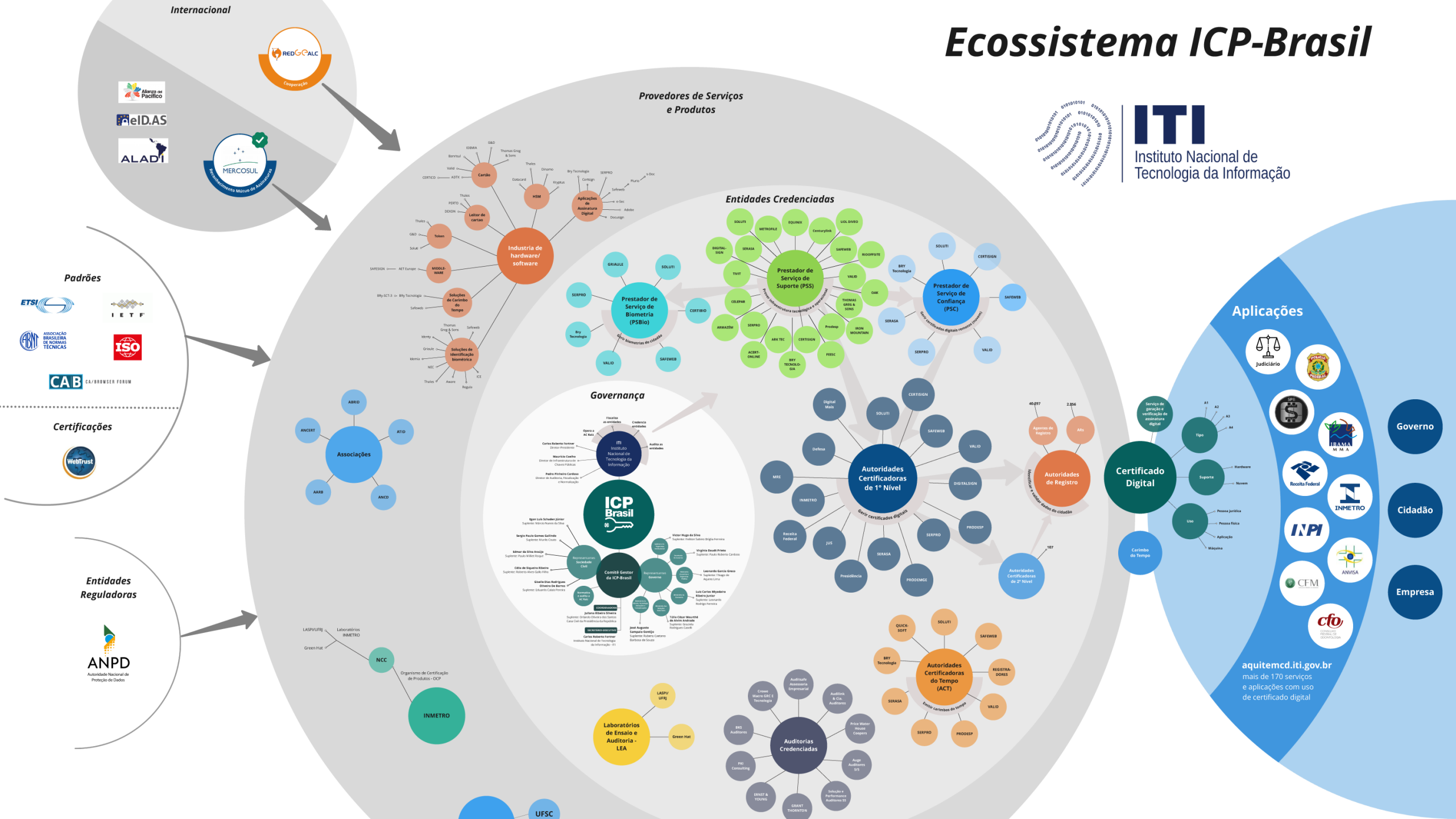
Publicado em 27/06/2017 21h02 | Atualizado em 21/06/2023 09h57

A **Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil** é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

- Ecossistema ICP-Brasil
- ICP-Brasil 20 anos
- Entes da ICP-Brasil
- Estrutura detalhada - ICP-Brasil

Ecossistema ICP-Brasil



ITI
Instituto Nacional de Tecnologia da Informação

ESTRUTURA DA ICP

- A ICP divide-se em 6 “entidades”:
  - AC raiz
  - AC – autoridade certificadora
  - AR – autoridade de registro
  - ACT - Autoridade Certificadora do Tempo
  - PSS - Prestador de Serviço de Suporte
  - PSBio - Prestador de Serviço Biométrico

- E o processo ainda envolve a entidade final.

- **AC - Raiz**
  - A Autoridade Certificadora Raiz é a primeira autoridade na cadeia de certificação. Suas responsabilidades incluem a execução das Políticas de Certificados e normas técnicas, emitir, expedir, distribuir e revogar certificados de autoridades certificadoras de nível inferior, além de gerenciar esses certificados.
  - A AC-Raiz emite a lista de certificados revogados (LCR) e supervisiona as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e outros prestadores de serviços na Infraestrutura de Chave Pública (ICP).
  - Verifica se as ACs estão seguindo as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP.

- **AC – Autoridade Certificadora**
  - Emissão, distribuição, renovação e revogação de certificados digitais.
  - Verifica a correspondência entre a chave privada do titular e a chave pública no certificado.
  - Gerencia o ciclo de vida dos certificados digitais.
  - Zela pela confiança no certificado após sua emissão.
  - Lida com o processo de renovação ou revogação de certificados digitais.
  - Recebe as requisições de emissão de certificados digitais para as entidades finais

- **AR – Autoridade Registradora**
  - Verifica informações fornecidas pelas entidades finais ao solicitar certificados digitais.
  - Atua como interface entre a entidade final e a Autoridade Certificadora (AC).
  - Sempre está vinculada a uma AC.
  - Recebe, valida e encaminha solicitações de emissão ou revogação de certificados digitais.

- **AR – Autoridade de Registro**
  - Realiza identificação presencial dos solicitantes.
  - Pode receber requisições de emissão de certificados, mas deve repassá-las a uma AC competente.
  - Verifica a identidade das entidades finais que solicitam certificados digitais.
  - Disponibiliza informações sobre os certificados emitidos pelas ACs aos usuários da Infraestrutura de Chave Pública (ICP).

- **ACT – Autoridade Certificadora do Tempo**
  - Fornecer Carimbos do Tempo confiáveis.
  - Emitir Carimbos do Tempo, que incluem informações temporais como ano, mês, dia, hora, minuto e segundo.
  - Associar esses atributos a uma assinatura digital, proporcionando prova da existência de um documento em um determinado período.
  - Atestar não apenas a questão temporal de uma transação, mas também seu conteúdo, por meio de criptografia e assinatura digital.

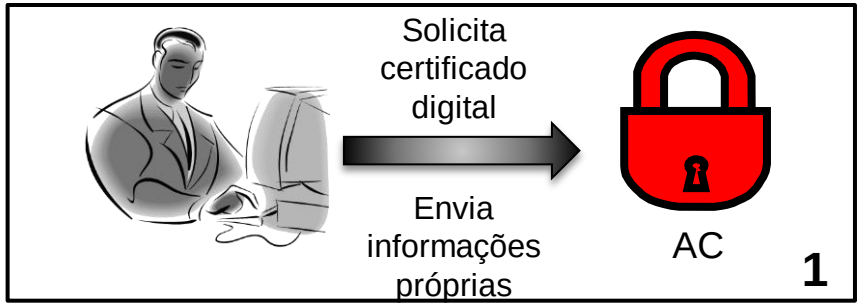
- **PSS – Autoridade Certificadora do Tempo**
  - Desempenha atividades de acordo com as políticas e práticas da Autoridade Certificadora (AC) ou Autoridade de Carimbo do Tempo (ACT) à qual está vinculada, ou nas atividades de PSBio, categorizando-se em três tipos:
    - Disponibilização de infraestrutura física e lógica.
    - Disponibilização de recursos humanos especializados.
    - Disponibilização de infraestrutura física e lógica, além de recursos humanos especializados, dependendo da natureza da atividade prestada.

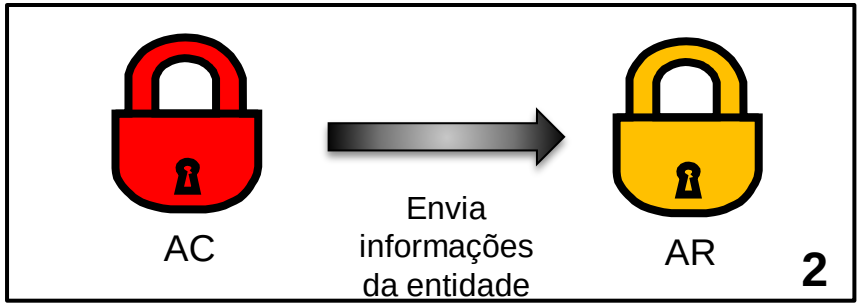
- **PSBio – Prestador de Serviço**
  - Entidade com capacidade técnica para executar a identificação biométrica, convertendo um registro ou solicitante em um único perfil em um ou mais bancos de dados biométricos para toda a ICP-Brasil.
  - Também é responsável por verificar a biometria do solicitante de um certificado digital e compará-la com uma característica biométrica conforme os padrões internacionais estabelecidos.

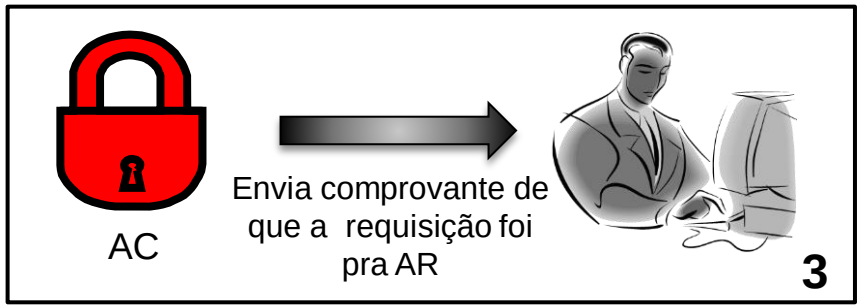
- **Entidade Final**
  - Entidade que pode provar legalmente e juridicamente sua existência e sua criação.
  - É quem solicita um certificado digital.
  - As principais entidades finais existentes em uma ICP são:
    - Pessoas;
    - Aplicações;
    - Servidores;
    - Empresas/organizações.

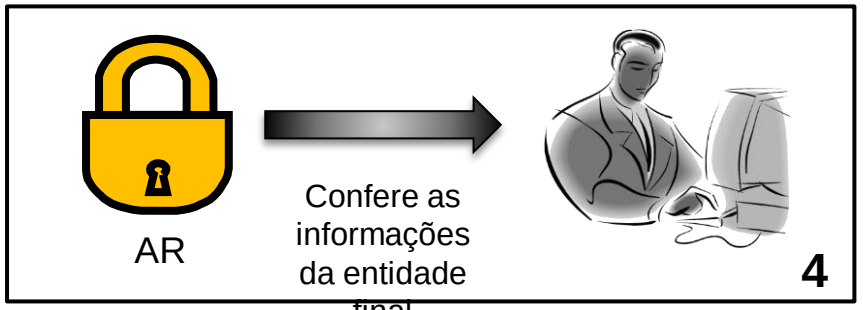
Processo de Emissão do Certificado Digital

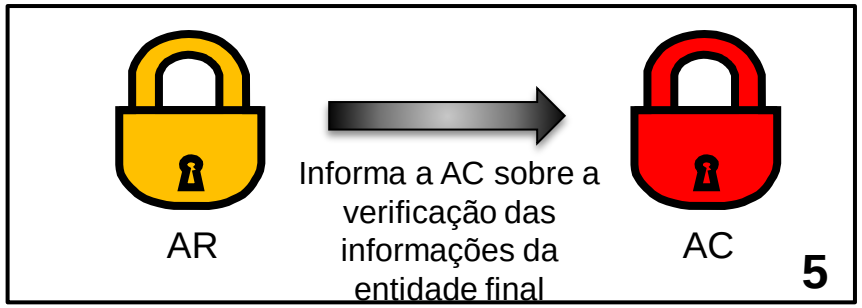
Processo de emissão do certificado digital para uma pessoa física

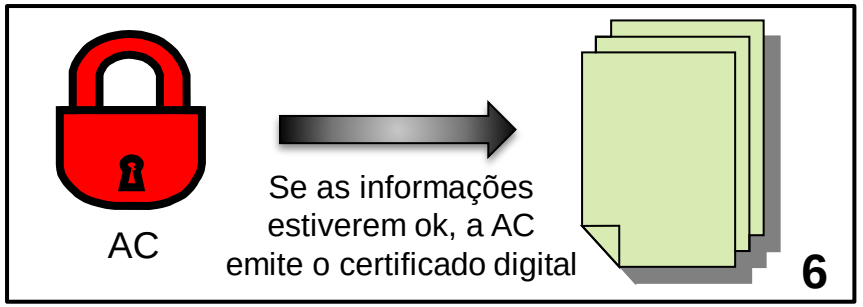

Solicita certificado digital
Envia informações próprias
AC
1

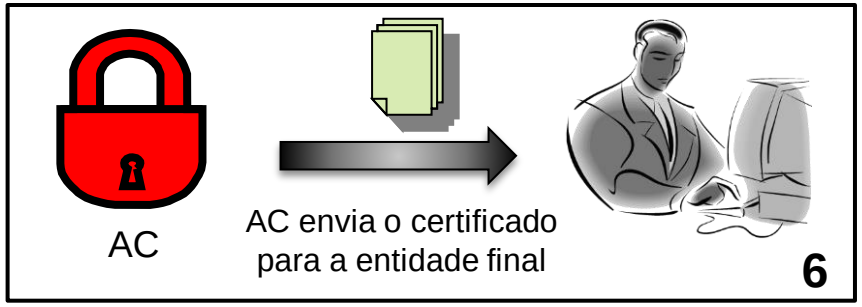

AC
Envia informações da entidade final
AR
2

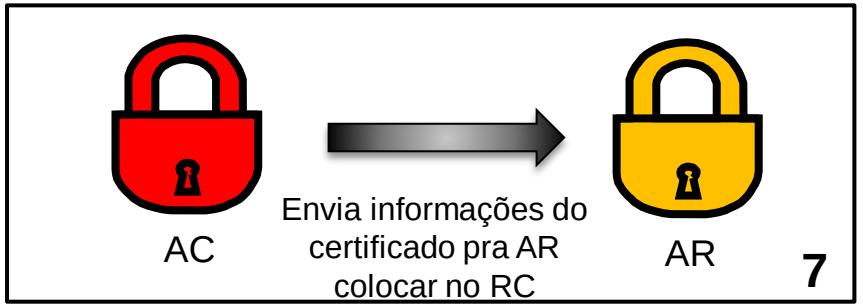

AC
Envia comprovante de que a requisição foi pra AR
3


AR
Confere as informações da entidade final
4


AR
Informa a AC sobre a verificação das informações da entidade final
AC
5


AC
Se as informações estiverem ok, a AC emite o certificado digital
6


AC
AC envia o certificado para a entidade final
6


AC
Envia informações do certificado pra AR colocar no RC
AR
7

- **Processo de Emissão do Certificado Digital**
  - Aqui vamos demonstrar o processo de emissão do certificado digital para uma entidade pessoa física:

1. A entidade final entra em contato com a AC e solicita a emissão de um certificado digital.
2. A AC envia as informações da entidade final (CPF, RG, título de eleitor e comprovante de residência) para a AR, que deve realizar a verificação e validação da identidade da entidade final.
3. A AC envia um comprovante para a entidade final, informando que a requisição da emissão de certificado digital foi encaminhada para uma AR, que entrará em contato para o agendamento de verificação presencial e validação de identidade.

4. A AR agenda uma visita à entidade final para verificar e validar suas informações (a entidade final pode comparecer diretamente na AR para evitar os custos de traslado do agente de registro).

5. A AR informa à AC sobre o resultado da verificação das informações da entidade final.
   - Se as informações forem validadas e verificadas com sucesso, a AR envia as informações checadas para a AC para que ela possa emitir o certificado digital.
   - Senão, a entidade final recebe a informação de que o processo de emissão foi negado.

6. A AC emite e assina o certificado digital e o envia para a entidade final.

7. A AC envia o certificado digital para a AR, para que essa publique esse certificado no repositório de certificados (RC)

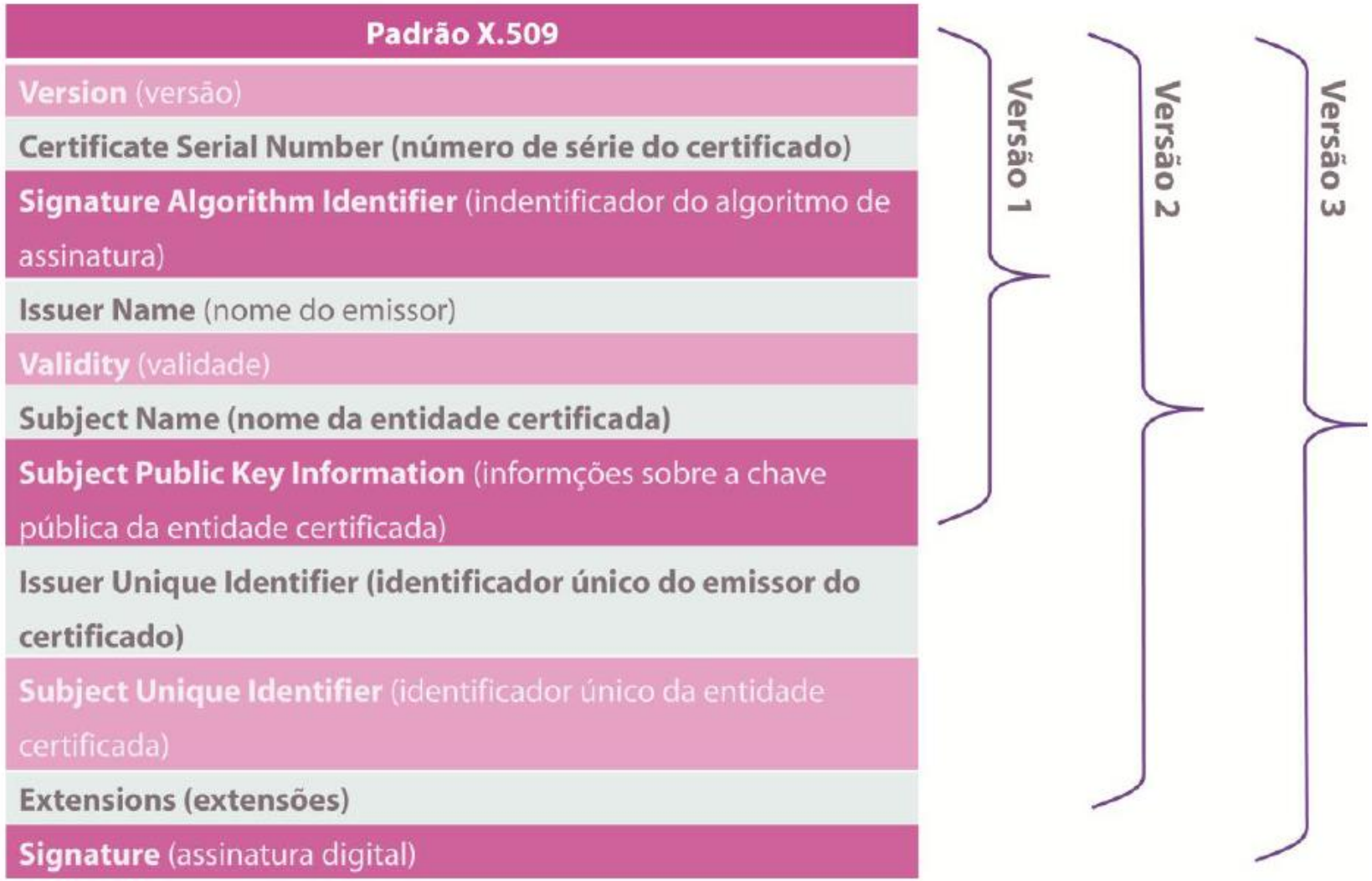
Certificados Digitais x.509

- Como já vimos, o certificado digital é um documento eletrônico que certifica a identidade de uma entidade através de uma terceira entidade.

- Essa terceira entidade é totalmente confiável e envolvida no processo, emitindo o certificado digital e verificando suas informações, tudo isso seguindo padrões de forma que possam ser usados pela maior quantidade de aplicações possível.

- O padrão mais usado de certificado digital é o x.509
  - Publicado em 1988
  - Era parte das recomendações sobre o diretório X.500
  - Foi revisado e publicado pelo IETF (Internet Engineering Task Force)
  - Está na versão 3

Estrutura dos Certificados x.509



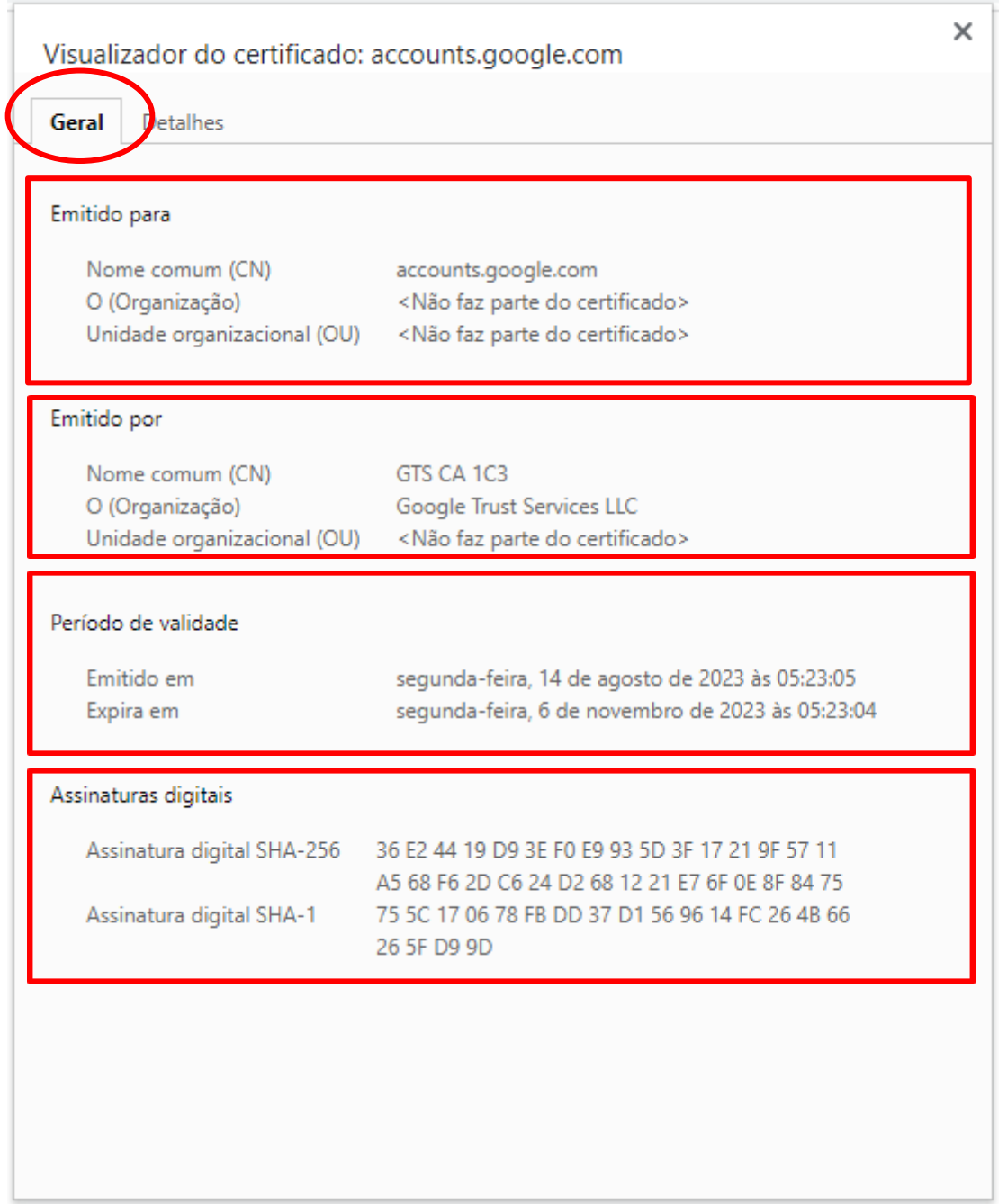
- Vamos analisar cada um dos campos do x.509.
- **Versão 1:**
  - **Versão:** indica a versão do certificado digital (1, 2 ou 3).
  - **Número de série do certificado:** apresenta o número serial do certificado digital, que é atribuído pela AC e deve ser único.
  - **Identificador do algoritmo de assinatura:** contém um código identificador de objeto que descreve qual o algoritmo criptográfico usado para a realização da assinatura digital da AC.
  - **Nome do emissor:** identifica qual AC emitiu o certificado

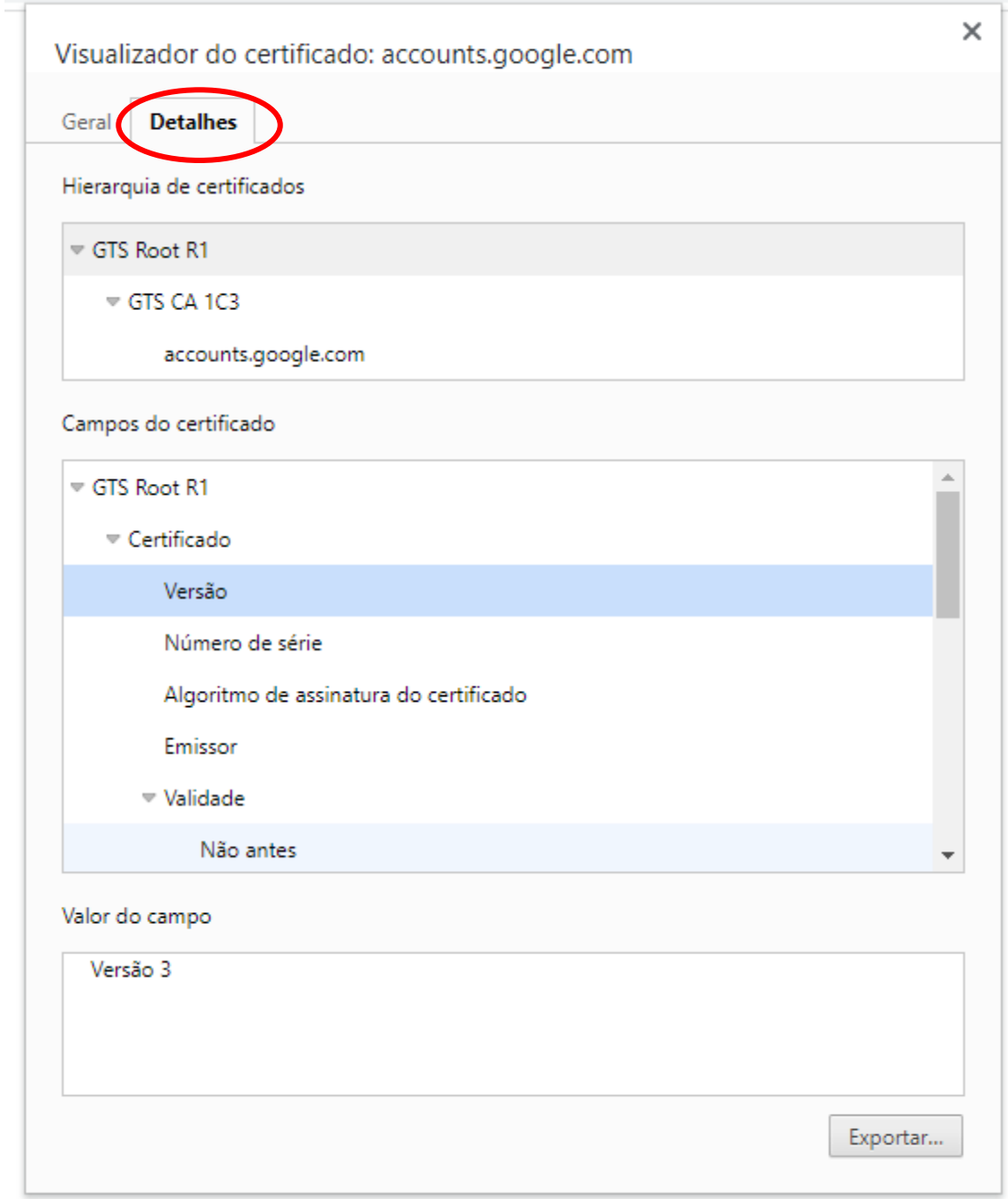
- **Validade:** indica o período de tempo em que o certificado digital estará válido para utilização
  - Possui mais 2 campos aninhados: NotBefore (indica que o certificado digital não pode ser usado antes de uma data específica) e NotAfter (indica que o certificado digital não pode ser usado depois de uma data específica).
- **Nome da entidade certificada:** nome da entidade final que recebeu o certificado.

- **Informações sobre a chave pública da entidade certificada:** apresenta informações referentes à chave pública do proprietário do certificado digital (chave pública associada ao certificado digital, identificador do algoritmo gerador do par de chaves e parâmetros necessários para a geração do par de chaves)
  - A chave privada deverá ser mantida em segurança e sigilo pelo proprietário do certificado digital.

- A versão 2 do x.509 foi criada para complementar a versão 1, tendo sido acrescentados os seguintes campos (lembrando que os campos da versão 1 continuam existindo na versão 2):
  - **Identificador único do emissor do certificado:** apresenta um código numérico e único que corresponde à AC emissora do certificado
  - **Identificador único da entidade certificada:** apresenta um código numérico e único que corresponde à entidade final que é proprietária do certificado.
    - Campo criado por conta dos homônimos.

- A versão 3 do x.509 foi criada para complementar a versão 2, tendo sido acrescentados os seguintes campos (lembrando que os campos das versões 1 e 2 continuam existindo na versão 3):
  - **Extensões:** apresenta campos adicionais que servem para complementar o certificado digital (alguns são opcionais e outros não).
- Além desses campos, existe um campo que está presente em todas as versões do x.509:
  - **Assinatura digital:** contém a assinatura digital realizada pela AC durante a emissão do mesmo


Visualizador do certificado: accounts.google.com
Geral
Detalhes
Emitido para
Nome comum (CN) accounts.google.com
O (Organização) <Não faz parte do certificado>
Unidade organizacional (OU) <Não faz parte do certificado>
Emitido por
Nome comum (CN) GTS CA 1C3
O (Organização) Google Trust Services LLC
Unidade organizacional (OU) <Não faz parte do certificado>
Período de validade
Emitido em segunda-feira, 14 de agosto de 2023 às 05:23:05
Expira em segunda-feira, 6 de novembro de 2023 às 05:23:04
Assinaturas digitais
Assinatura digital SHA-256 36 E2 44 19 D9 3E F0 E9 93 5D 3F 17 21 9F 57 11 A5 68 F6 2D C6 24 D2 68 12 21 E7 6F 0E 8F 84 75
Assinatura digital SHA-1 75 5C 17 06 78 FB DD 37 D1 56 96 14 FC 26 4B 66 26 5F D9 9D


Visualizador do certificado: accounts.google.com
Geral
Detalhes
Hierarquia de certificados
GTS Root R1
GTS CA 1C3
accounts.google.com
Campos do certificado
GTS Root R1
Certificado
Versão
Número de série
Algoritmo de assinatura do certificado
Emissor
Validade
Não antes
Valor do campo
Versão 3
Exportar...