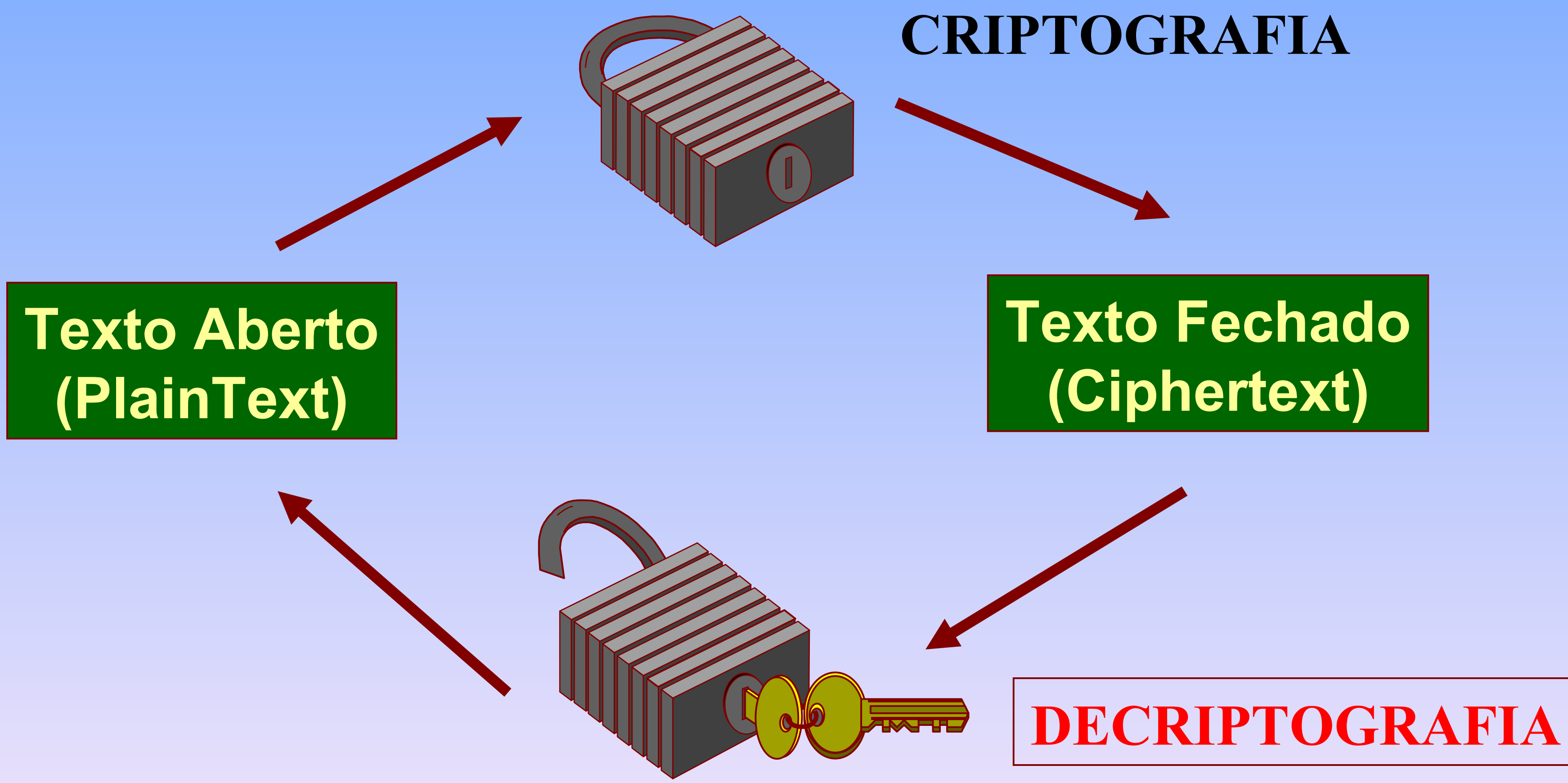
Criptografia
Assinaturas Digitais
Certificados Digitais

Criptografia e Descriptografia



Sistema de Criptografia Simples

- Caesar Cipher: usado por Julius Caesar
  - Substituição de letras pelas letras deslocadas de N.

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

Nada de novo no front.

N = 3

Qdgd gh qryr qr iurqw.

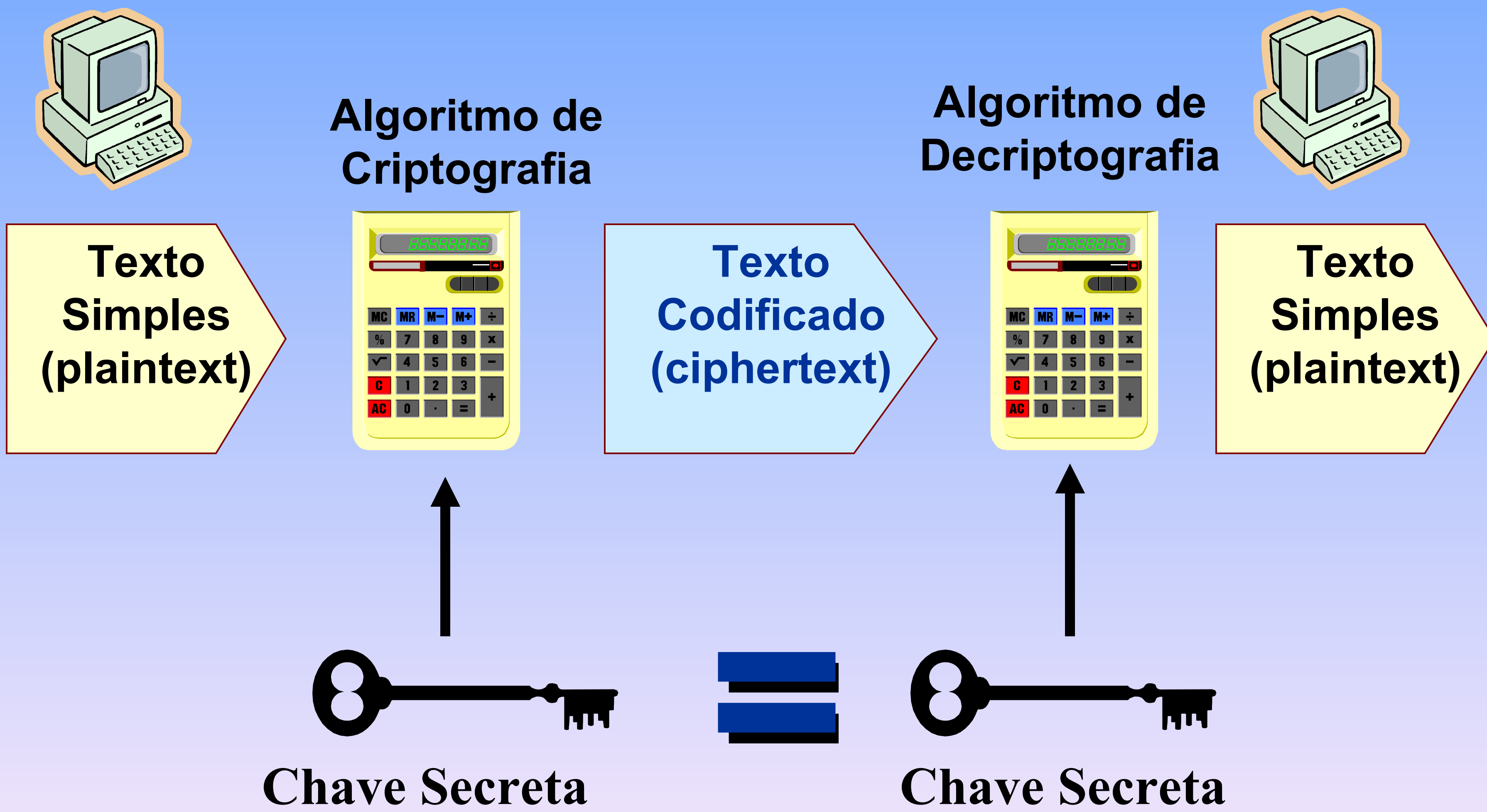
N = 4

Rehe hi rszs rs jvstx.

Criptografia Simétrica e Assimétrica

- Dois sistemas de criptografia são usados atualmente:
  - sistemas de chave secreta (secret-key)
    - Também denominados simétricos 
    - Trabalha com uma única chave, denominada SECRETA.
  - sistemas de chave pública (public-key)
    - Também denominado assimétrico
    - Trabalho com um par de chaves
      - CHAVE PÚBLICA 
      - CHAVE PRIVADA 

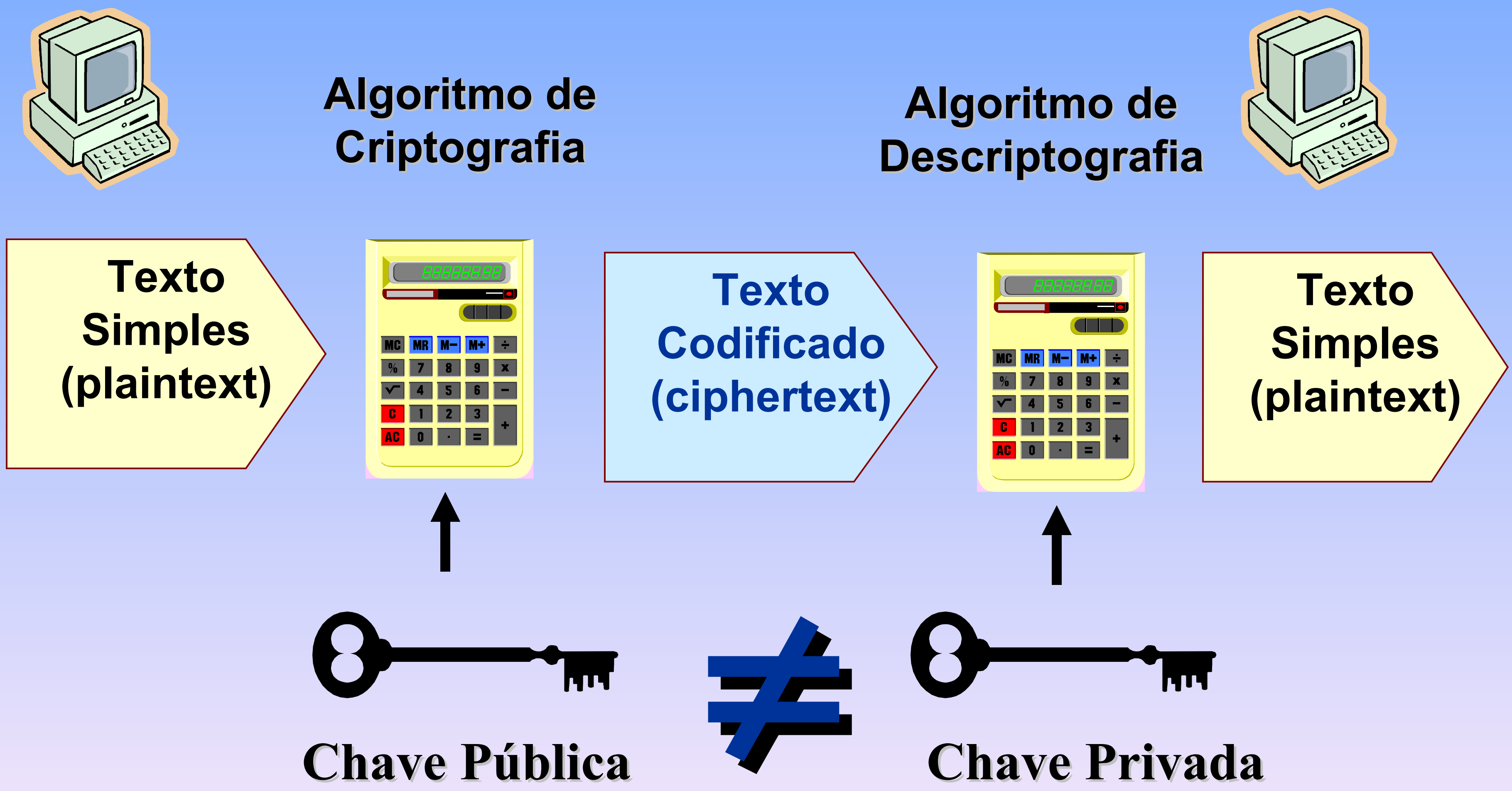
Chave Secreta (Criptografia Simétrica)



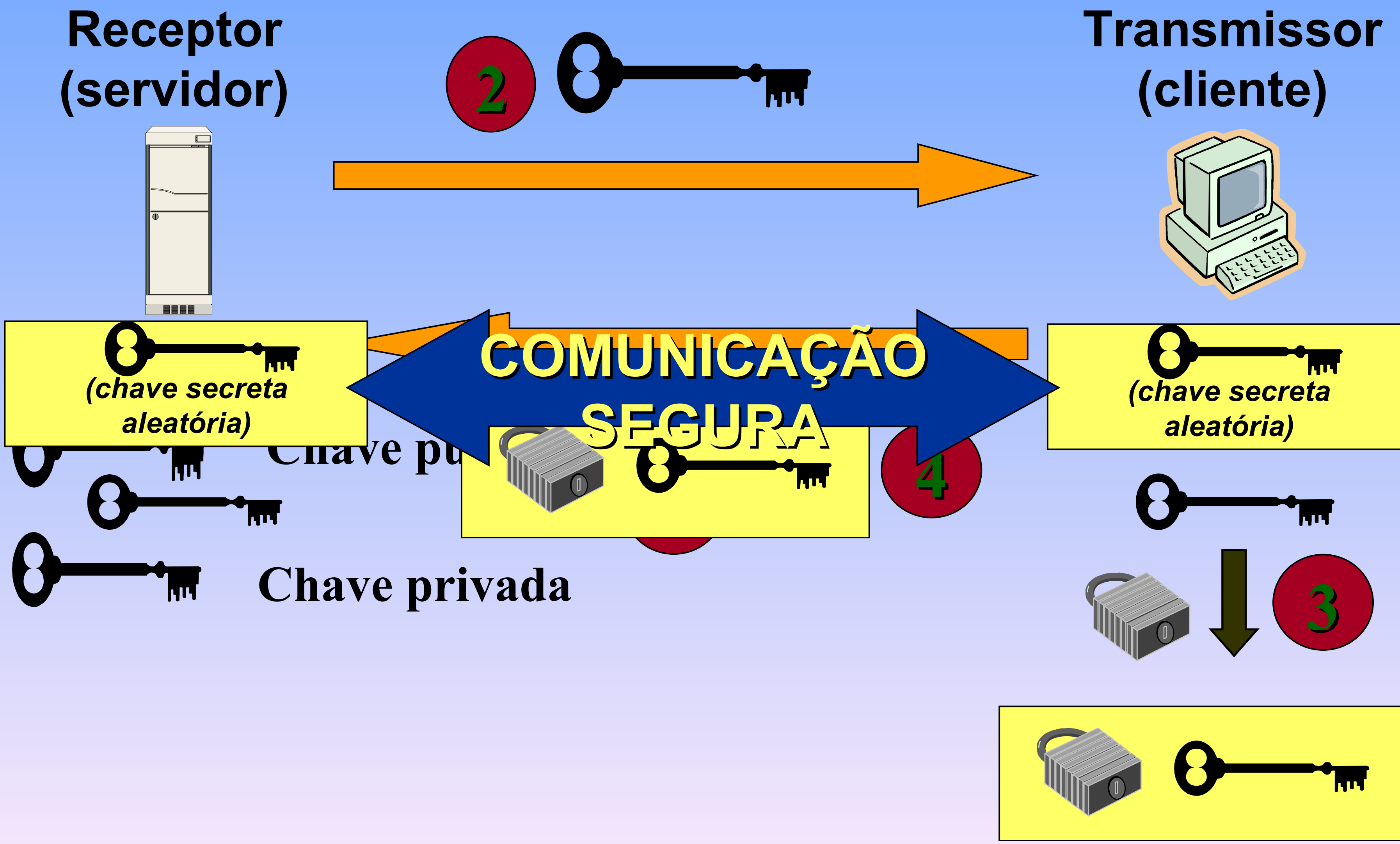
Chave Pública = CRIPTOGRAFIA ASSIMÉTRICA

- Sistema de Criptografia Assimétrico
  - Utiliza um par de chaves.
  - Uma chave publica para criptografar a mensagem.
  - Uma chave privada para decriptografar a mensagem.
- A **chave pública** não é secreta.
- A **chave privada** é secreta.
- A chave pública deve ser distribuída para os usuário que desejarem enviar uma mensagem com segurança.

Chave Pública (Criptografia Assimétrica)



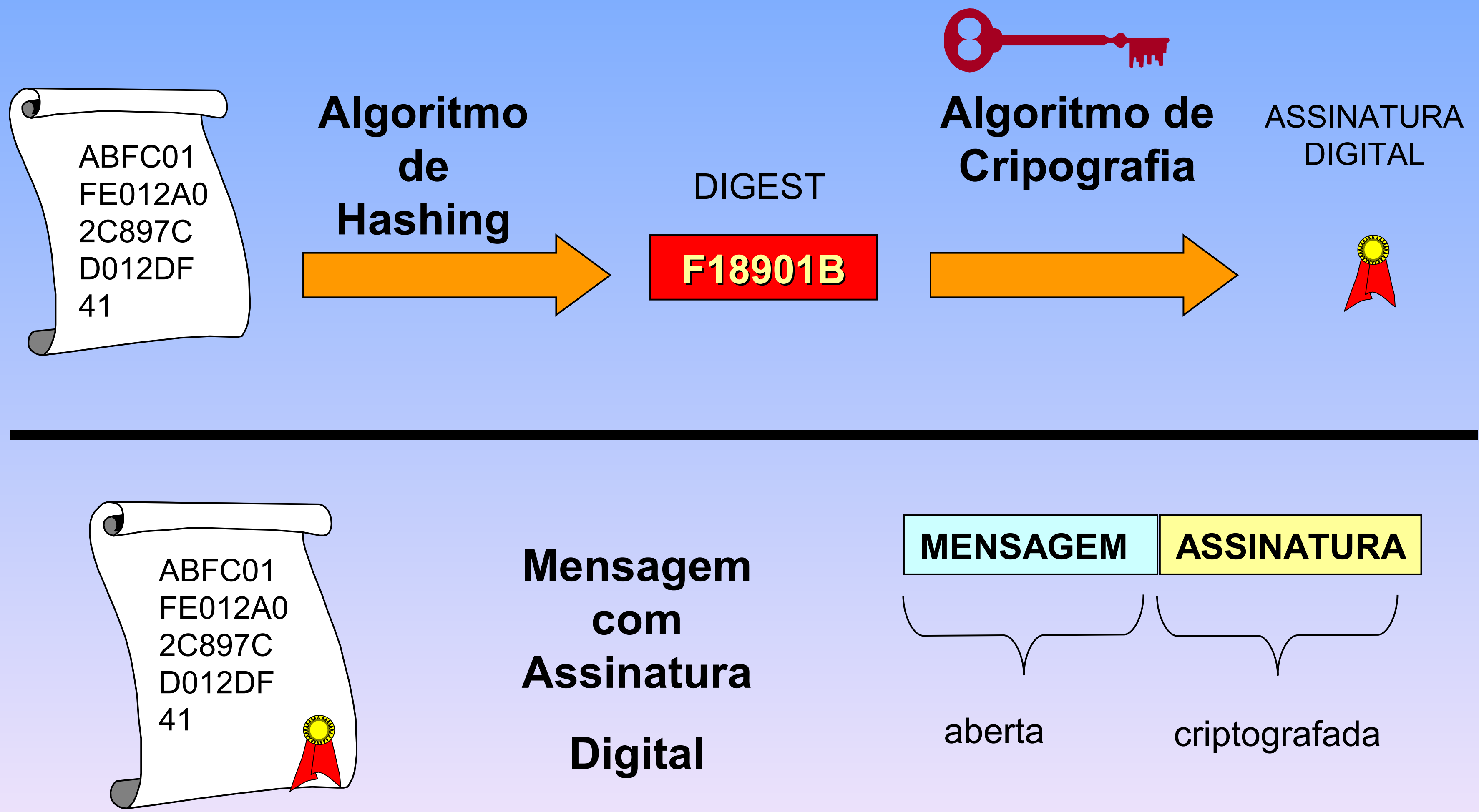
Chave Pública e Chave Secreta



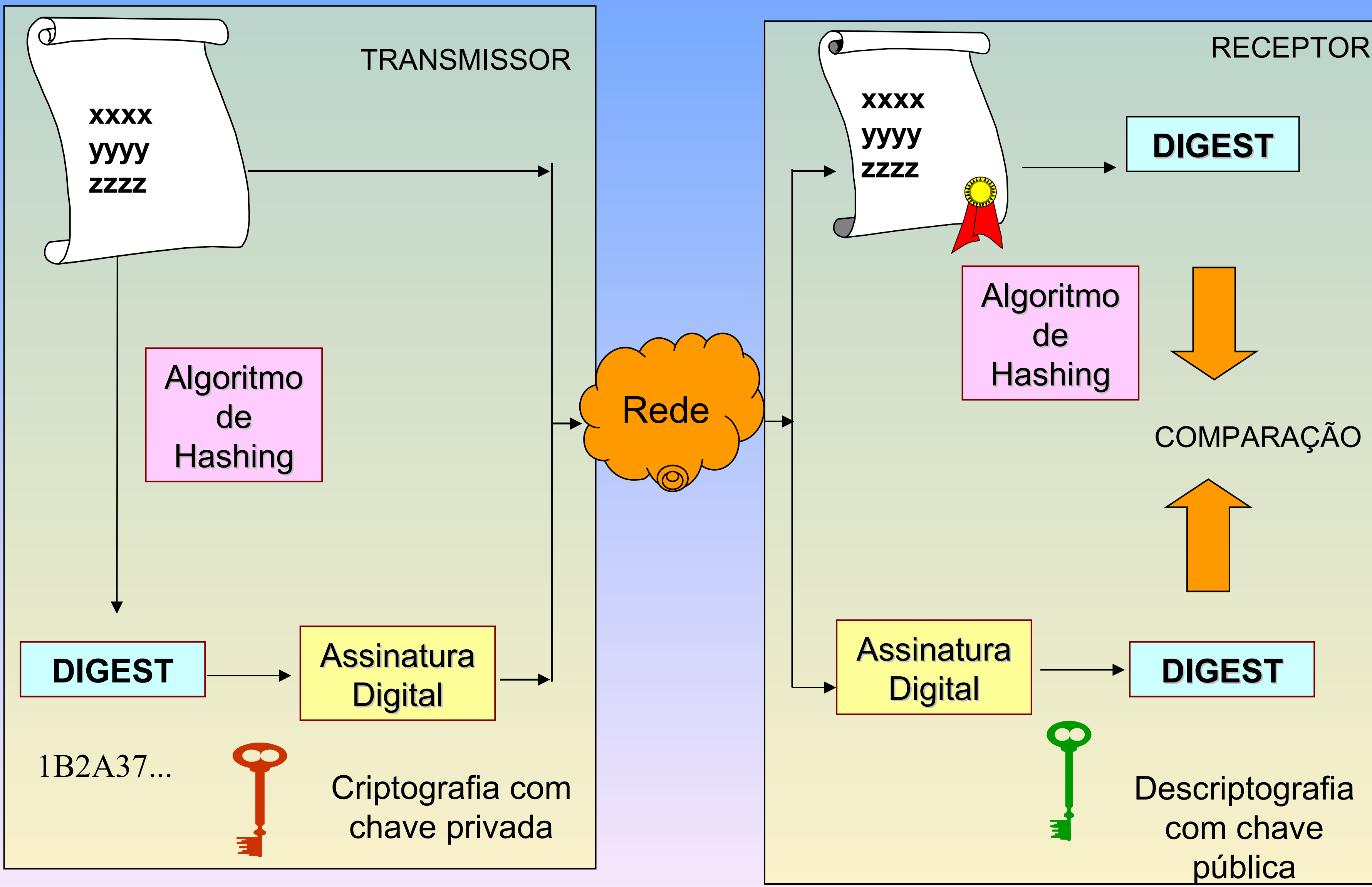
Assinatura Digital com Chave Pública

- Permite ao receptor verificar a integridade da mensagem:
  - O conteúdo não foi alterado durante a transmissão.
  - O transmissor é quem ele diz ser.

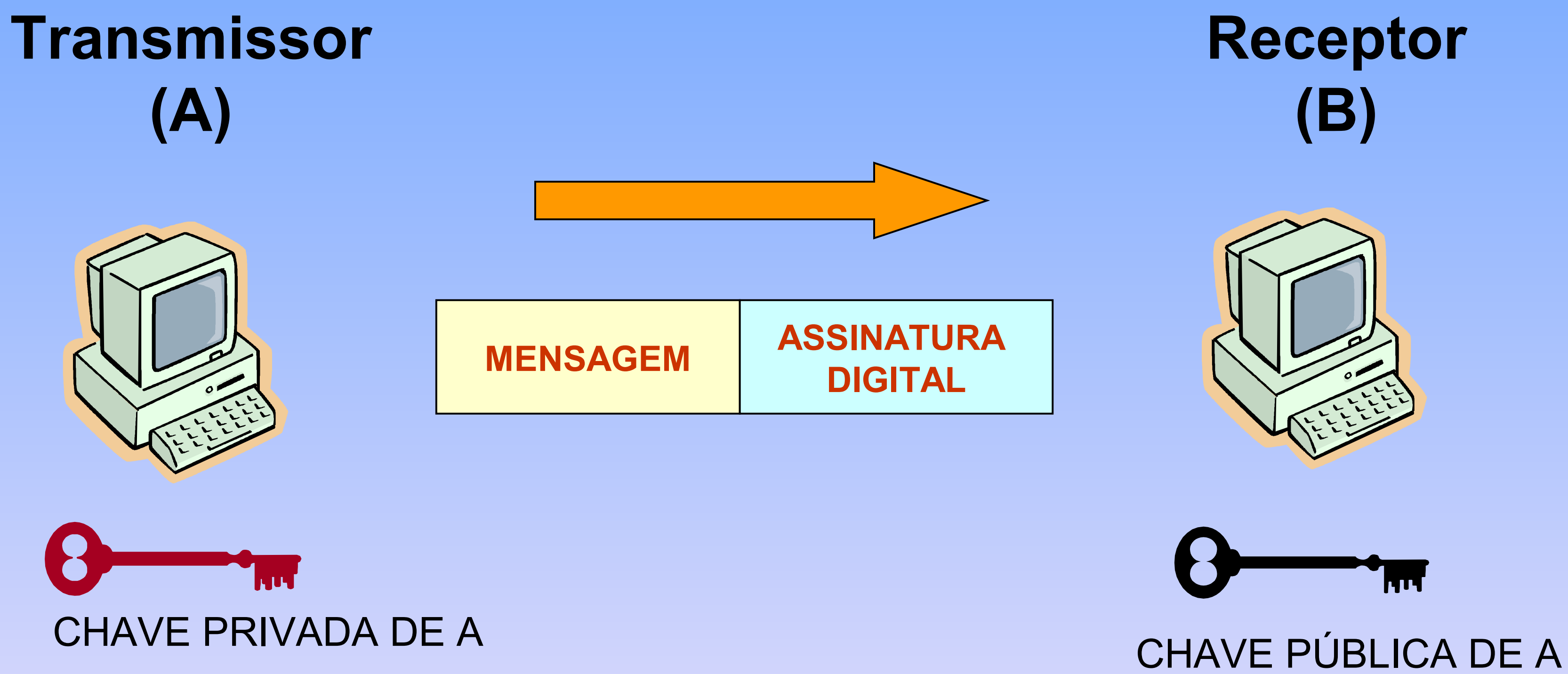
Implementação da Assinatura Digital



Geração e Validação das Assinaturas



Verificação da Integridade da Mensagem



O receptor precisa ter a chave pública do transmissor para verificar a assinatura.

Autoridade Certificadora

Autoridade Certificadora (Verisign, Certisign, Etc.)

C.A. (Certification Authority)

CHAVE PRIVADA

Certificado X509

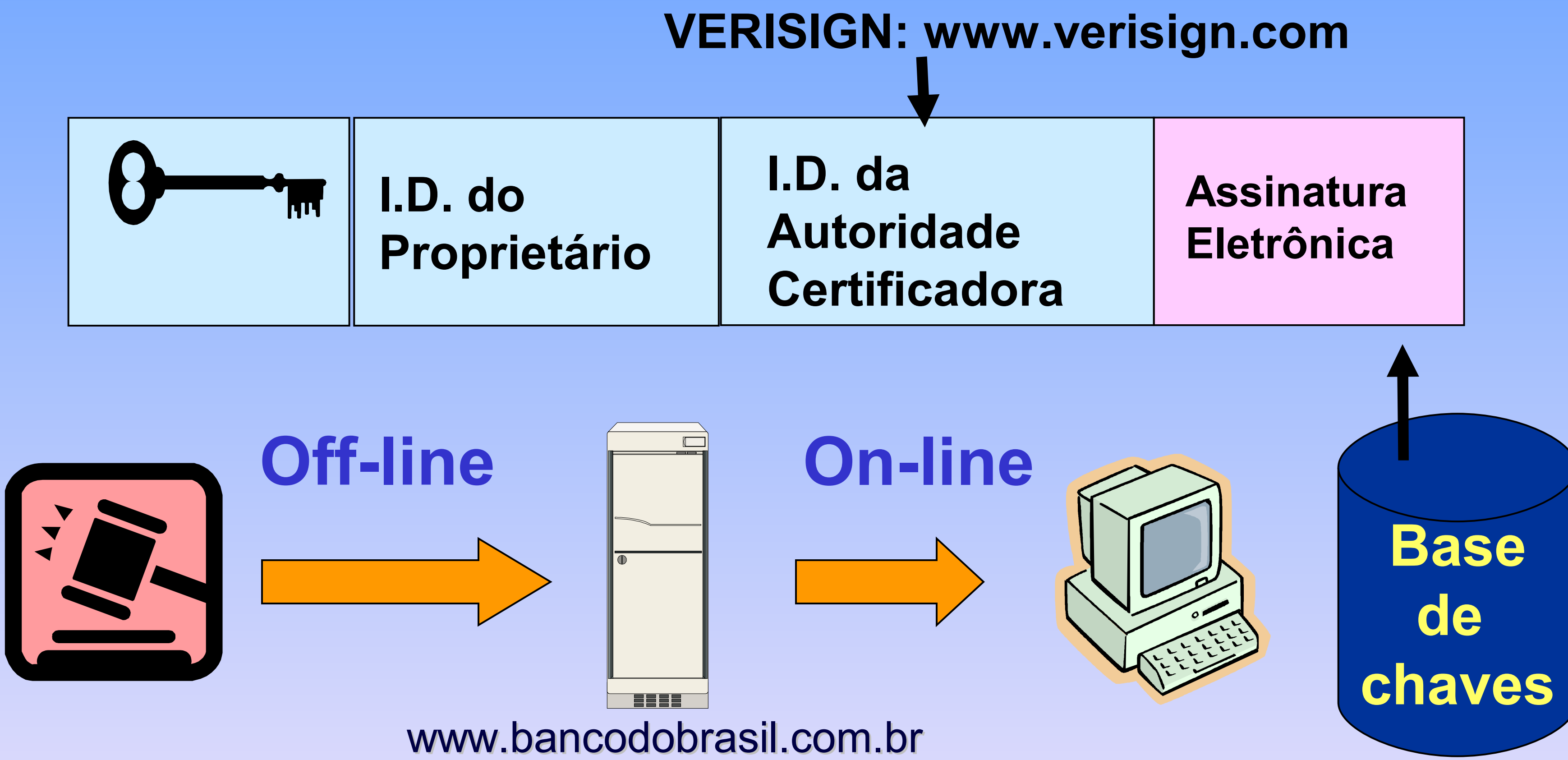
	I.D. do Proprietário	**I.D. da CA**	**Assinatura Digital**

Chave pública (e.g., Banco do Brasil)

www.bancodobrasil.com.br
Banco do Brasil S.A.
Brasilia, DF, Brasil

www.verisign.com
Verisign, Inc.

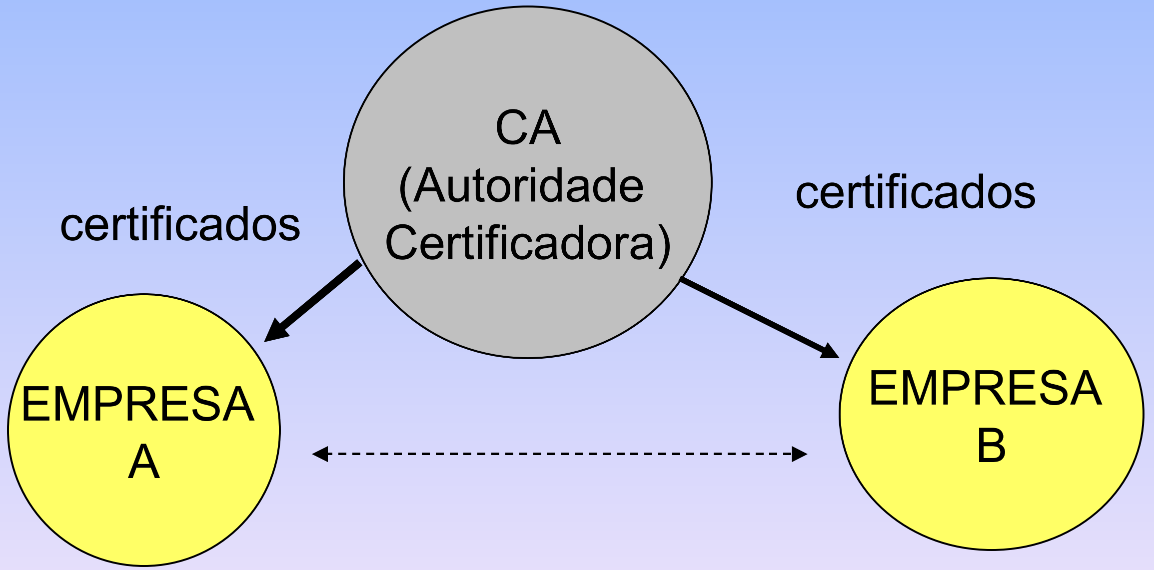
Estratégias de Certificação



- O software que recebe o certificado (por exemplo, o browser) deve possuir a chave pública da autoridade certificadora.

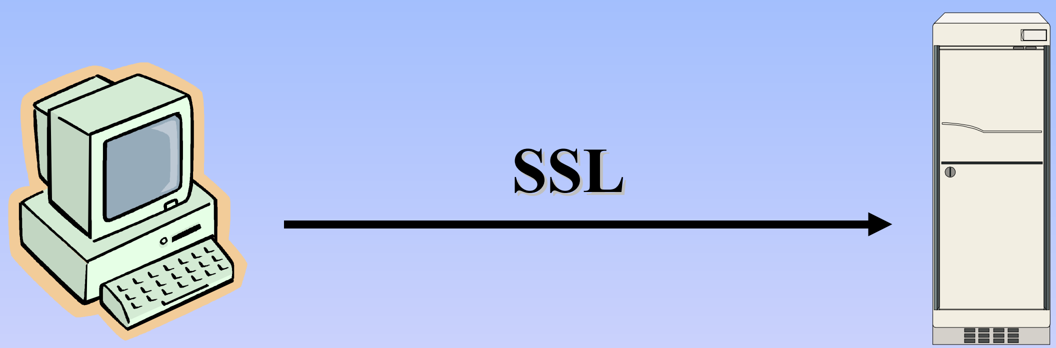
PKI (Public Key Infrastructure)

- O termo PKI (Infraestrutura de chave pública) é utilizado para descrever o conjunto de elementos necessários para implementar um mecanismo de certificação por chave pública.

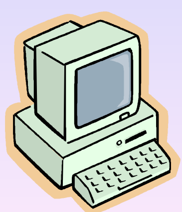


Autenticação do Cliente

- SSL permite ao servidor identificar a identidade do cliente.



Chave pública do Cliente	Identificação do Cliente	Identificação do CA	Assinatura Digital de uma CA

Criptografia da Comunicação

- Após a certificação, o SSL/TLS cria uma chave de sessão que garante:
  - Confidencialidade e Proteção contra Tampering (alteração dos dados em transito).