UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 7 – Assinaturas Digitais e HASH.

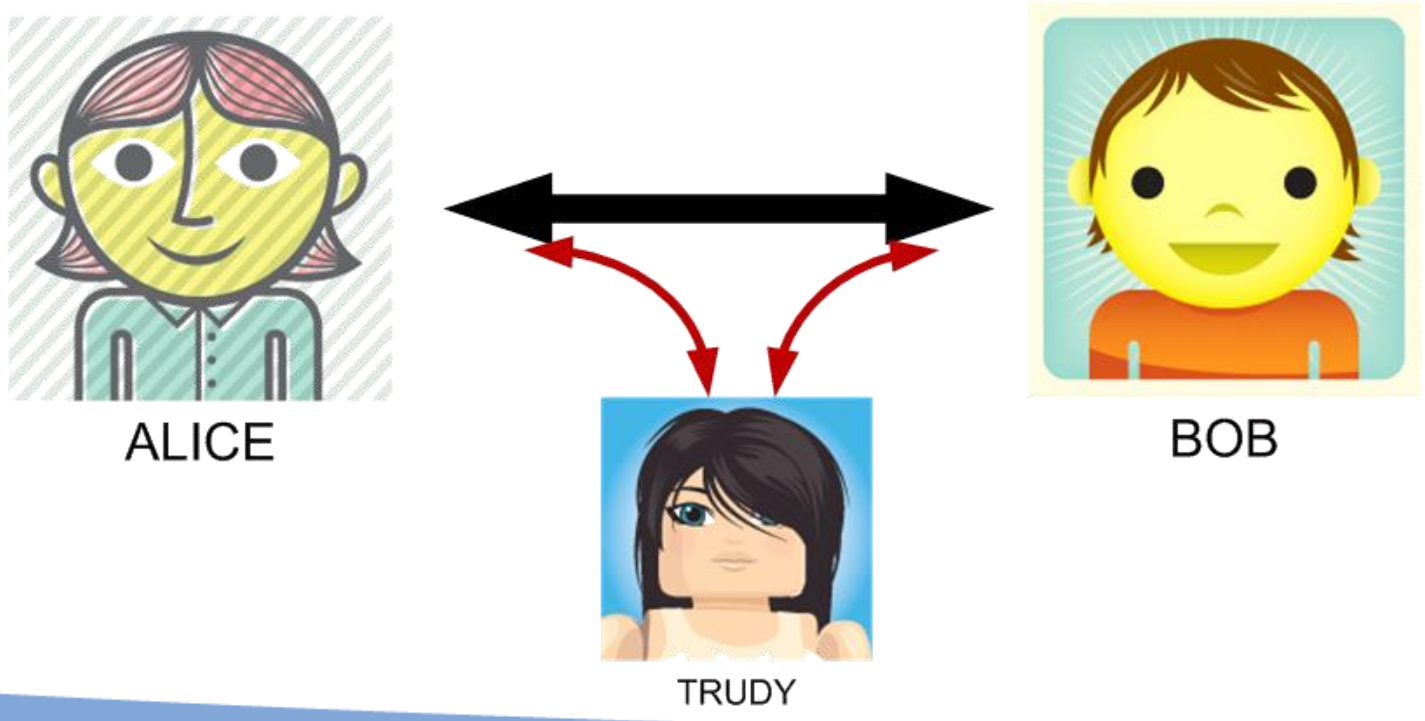
Prof. Dr. Eng. Fred Sauer

http://www.fredsauer.com.br

fsauer@gmail.com

Assinatura Digital
Objetivos

- Como Trudy não possui as chaves privadas de Alice e Bob, não consegue decodificar a mensagem cifrada → Confidencialidade OK!
- No entanto, Trudy pode possui as chaves públicas de ambos.
- O que a impede de enviar mensagens forjadas?



Assinatura Digital
Objetivos

- Confirmar a origem do dado
- Certificar que o dado não foi modificado
- Impedir a negação de origem

Assinatura Digital Algumas Vantagens

- Não repúdio.
- Autenticidade.
- Integridade.

Assinatura Digital
TIPOS

- Assinatura Digital Simétrica
  - Rabin, Lamport-Diffie, Desmedt, Matyas-Meyer

- Assinatura Digital Assimétrica

Assinatura Digital
Chave Simétrica

- Estratégia – uso de uma autoridade central.
- Cada usuário escolhe uma chave secreta e a publica na autoridade central.
- Somente Alice e a autoridade central conhecem a chave secreta de Alice.

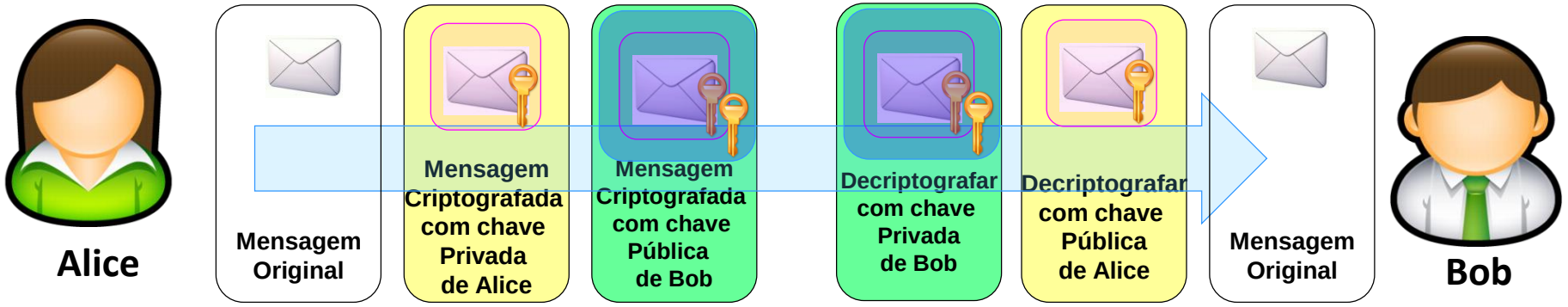
Assinatura Digital Simétrica Desvantagens

- Depende da Idoneidade da autoridade central.

- Autoridade central pode ler todas as mensagens.

Assinatura Digital Assimétrica Chave Pública

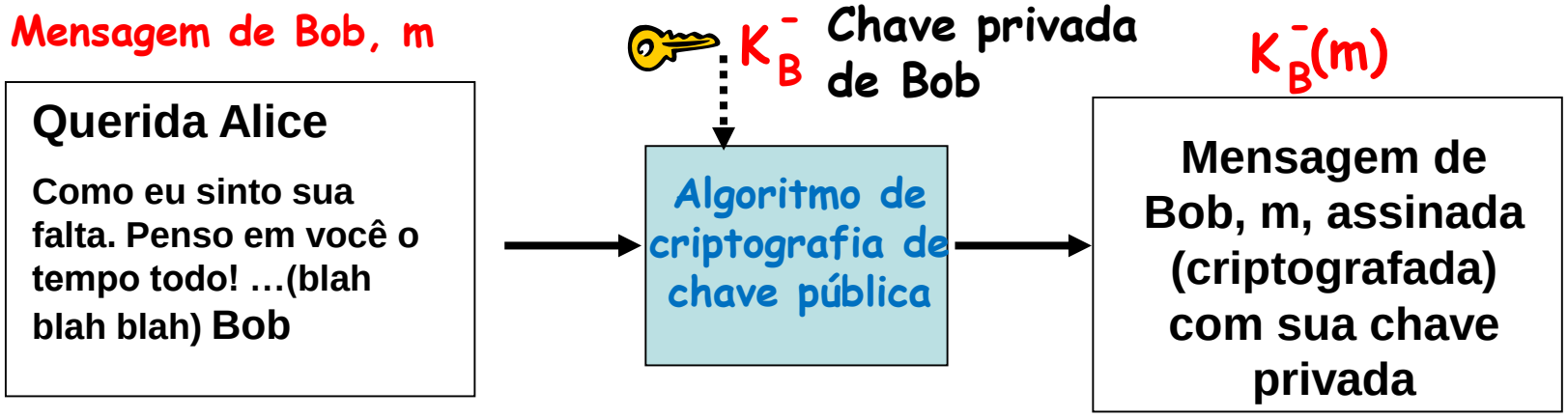
- Reúnem sigilo e autenticação
- Cifragem da mensagem inteira é lenta => Sumário de Mensagens



Assinatura Digital Chave Pública

Assinatura digital simples para mensagem m:

- Bob assina m criptografando com sua chave privada K_B^-, criando mensagem "assinada", $K_B^-(m)$



Problema: Processo para criptografar é lento

- Solução: uso de sumário da mensagem

Assinatura Digital
Sumários de Mensagens

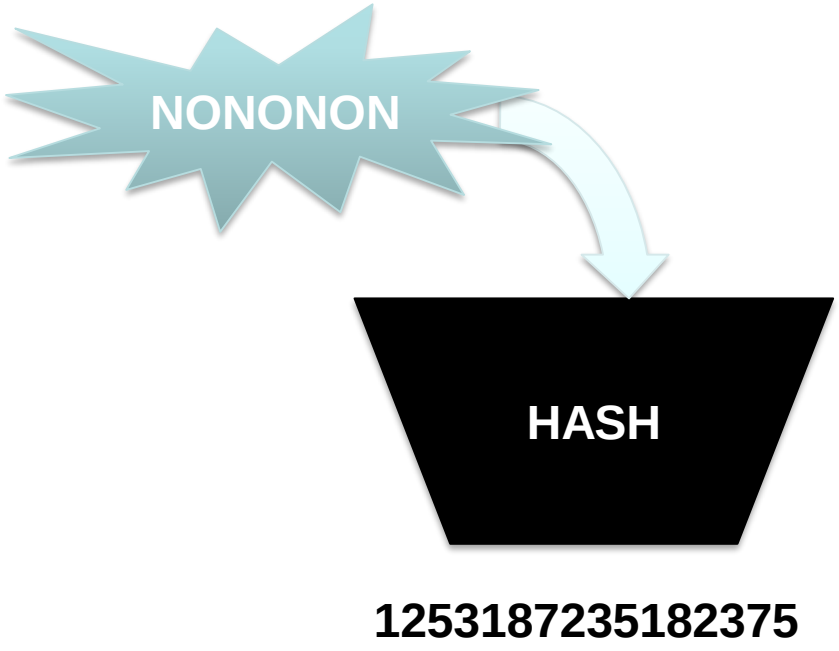
- Sumários de Mensagens (Message Digests)

  – Uso de uma **função hash** unidirecional que extrai um trecho qualquer do texto simples e, a partir deste, calcula um string de bits de tamanho fixo.

  – **Função hash** – geralmente denominada sumário de mensagens (MD).

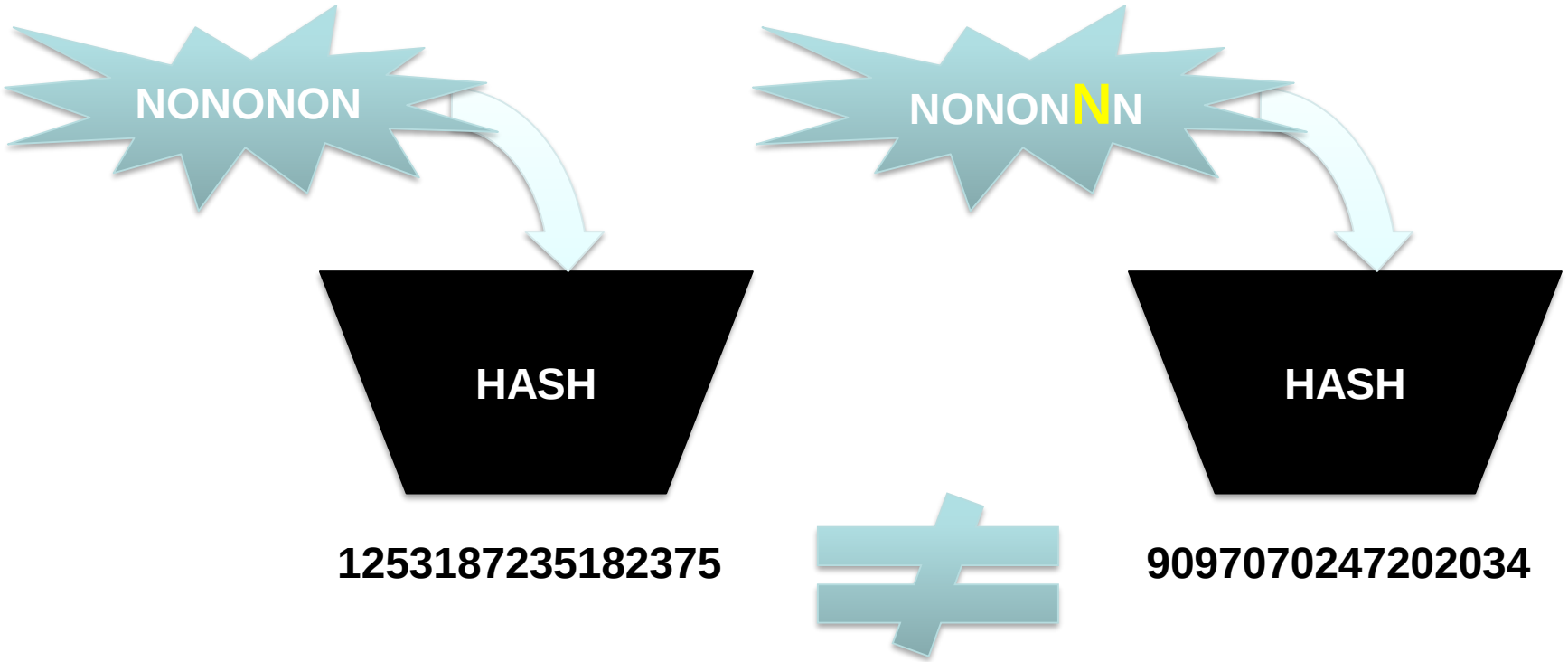
Hash

- Hash → Função de Condensação. É o nome de uma função que, a partir de manipulações algébricas, geram um conjunto único de caracteres.



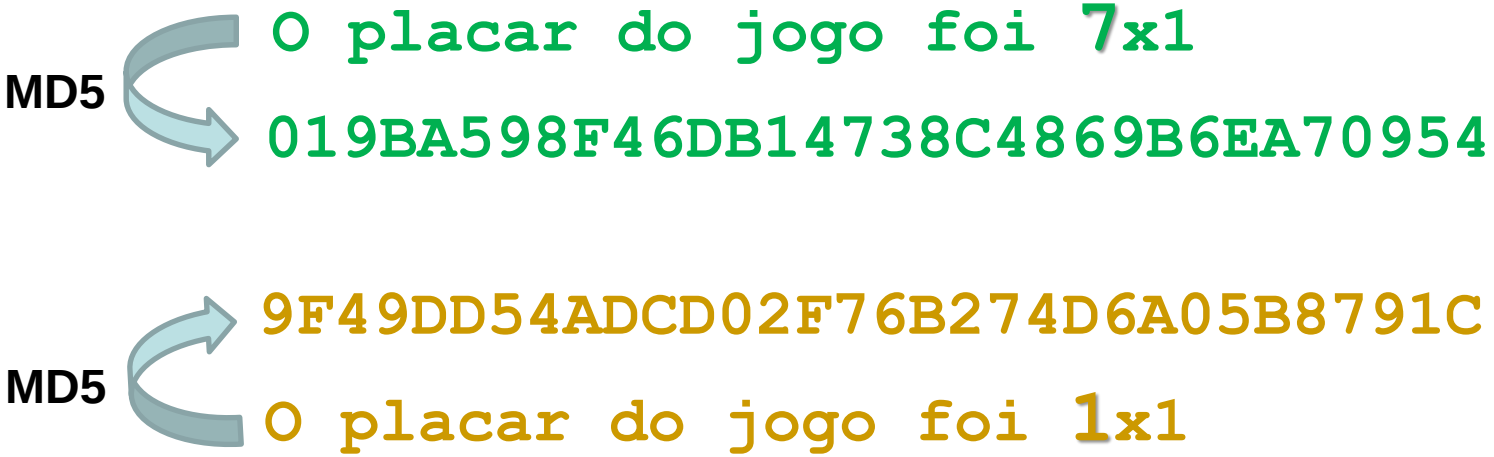
Hash

- A modificação de um bit da informação de entrada altera totalmente o resultado.



Hash

- A modificação de um bit da informação de entrada altera totalmente o resultado.



Hash

- Exemplo de funções hash:

FUNÇÃO	TAMANHO DA SAÍDA EM BITS
MD5	128
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512

Hash

- Exemplo de funções hash:

Entrada: **Segurança da Informação**

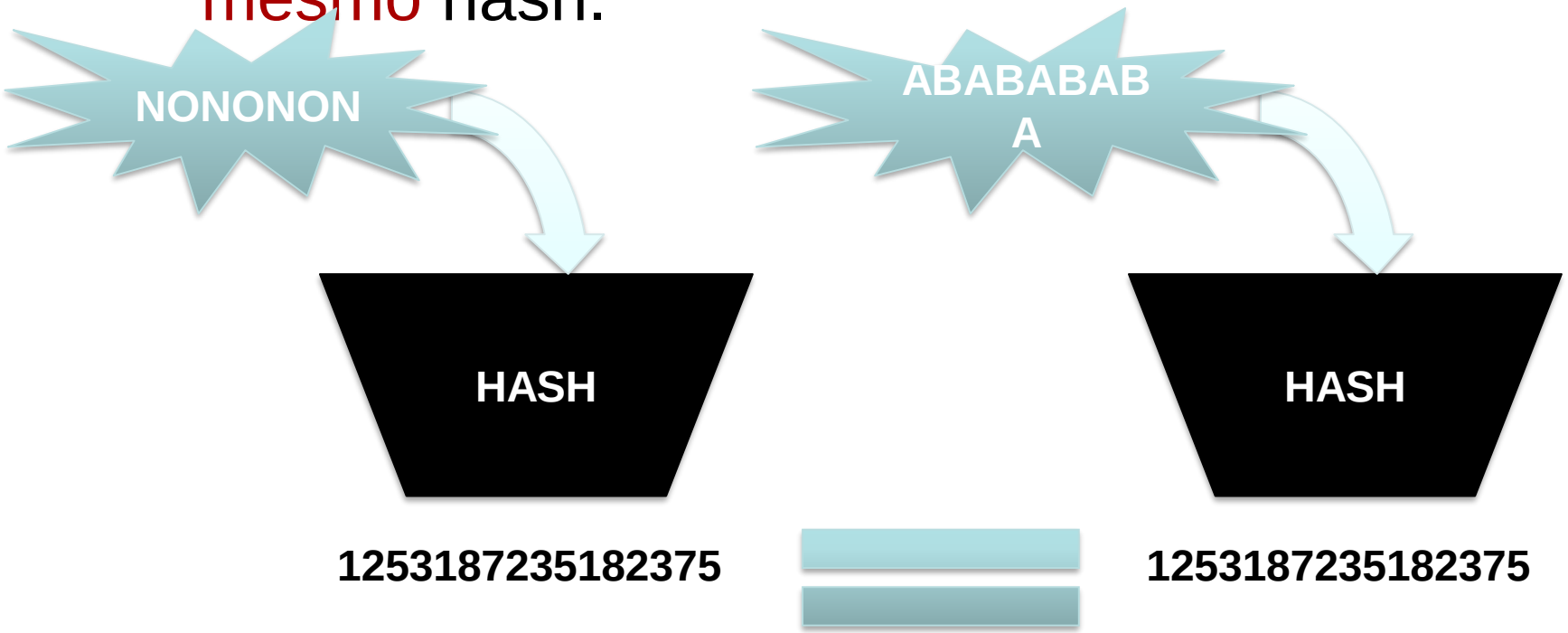
MD5 (128 bits): `2597568A2A61B57FAFD4ACED25985EAA`

SHA-1 (160 bits): `A85E94C5F1FDF90520C80F9F90FCFCE4A317D141`

SHA-256: `EC1A757E3C679B372BADFD01A7453AB4A6C80AB40D424D0135765DCBB50E8252`

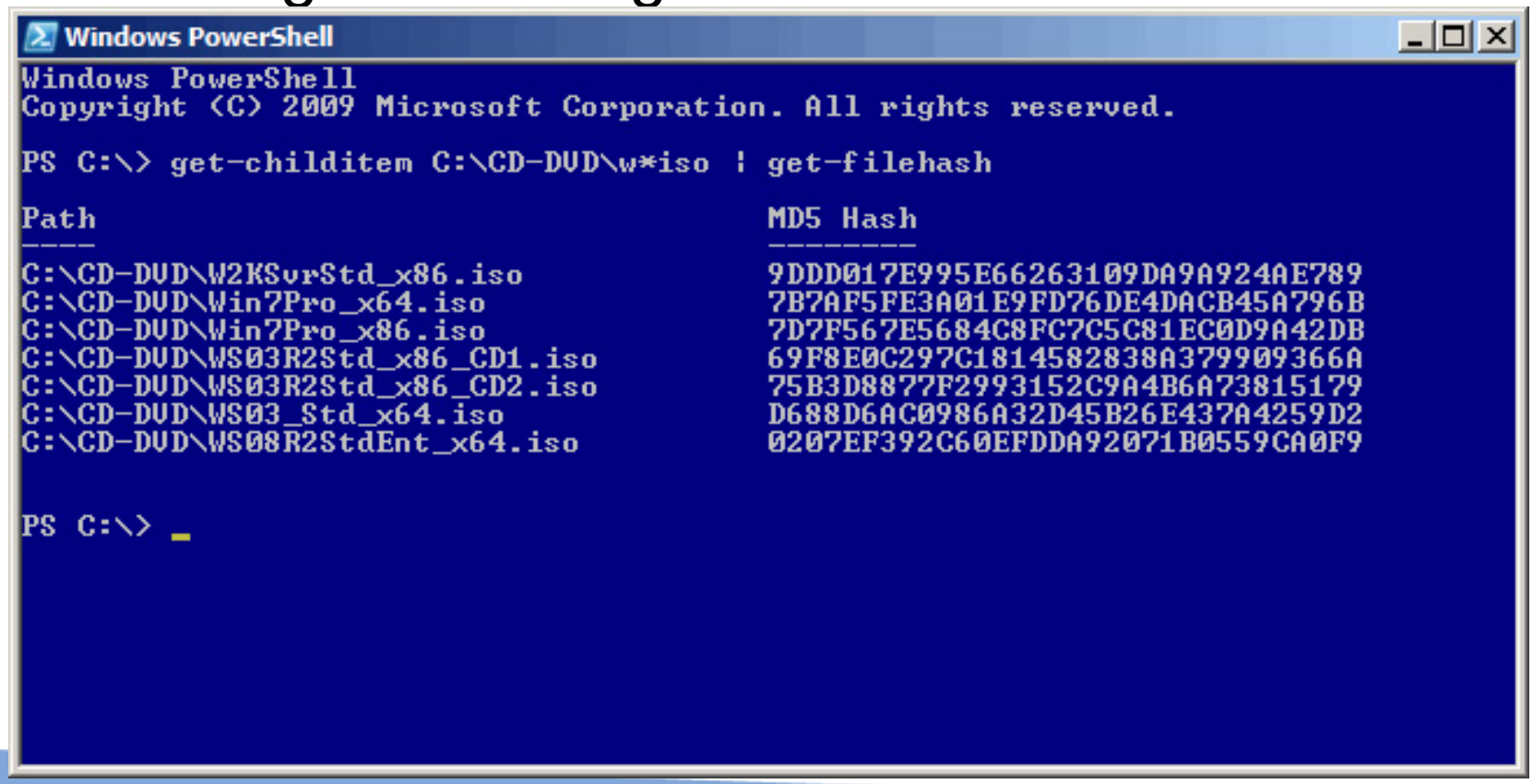
Hash

- COLISÃO:
  - quando informações diferentes geram o mesmo hash.



Hash

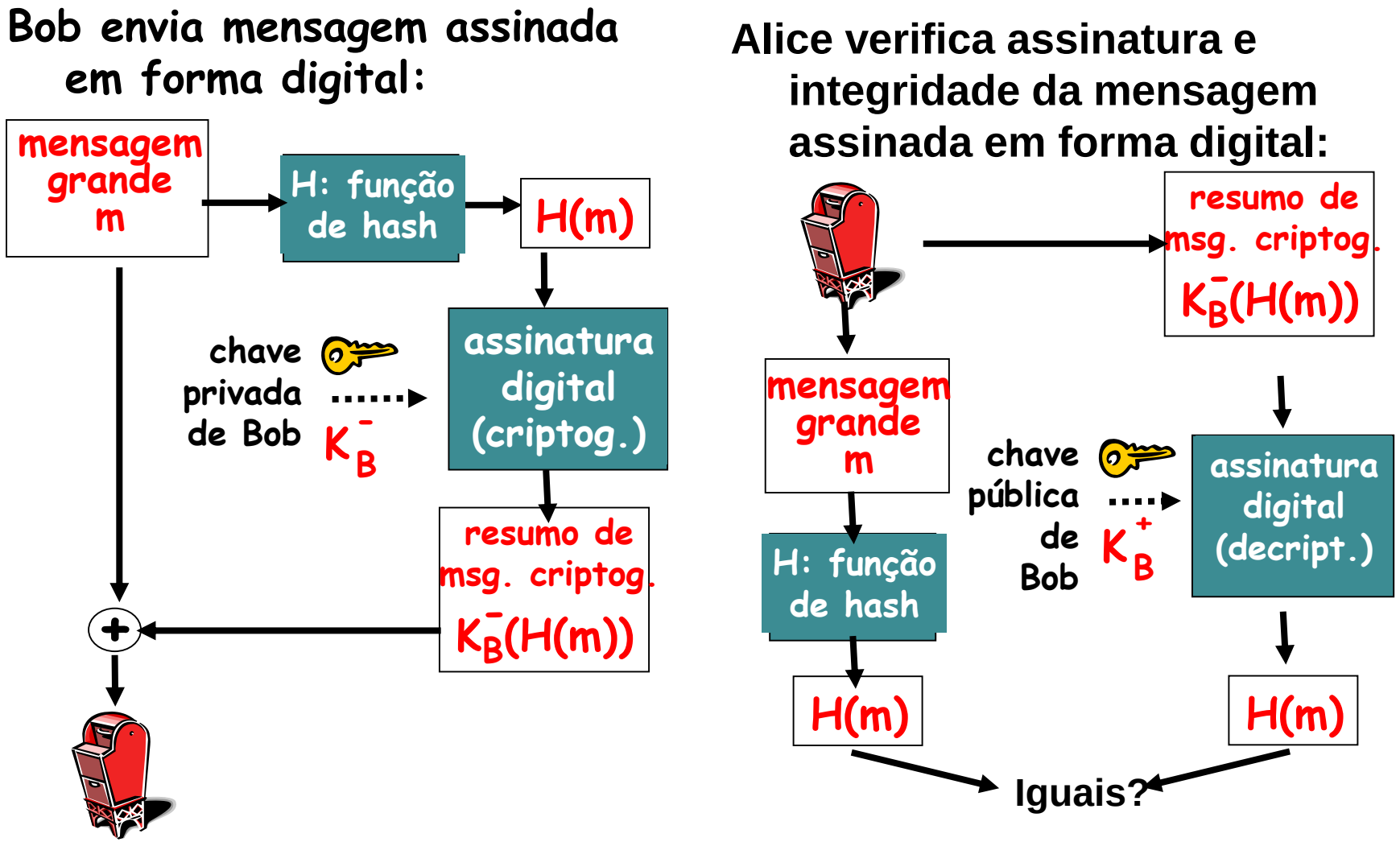
- APLICAÇÃO DE HASH:
  - Assegurar a integridade!



Assinatura Digital
Sumário de Mensagens

- Propriedades importantes
  - Gera um sumário de tamanho fixo para qualquer comprimento de mensagem.
  - Efetivamente impossível adivinhar a mensagem a partir do sumário.
  - Efetivamente impossível encontrar outra mensagem que gere o mesmo sumário.
  - Uma pequena mudança na mensagem altera bastante o sumário.
  - Exemplo
    - MD5("The quick brown fox jumps over the lazy dog") **9e107d9d372bb6826bd81d3542a419d6**
    - MD5("The quick brown fox jumps over the lazy cog") = **1055d3e698d289f2af8663725127bd4b**

Assinatura Digital



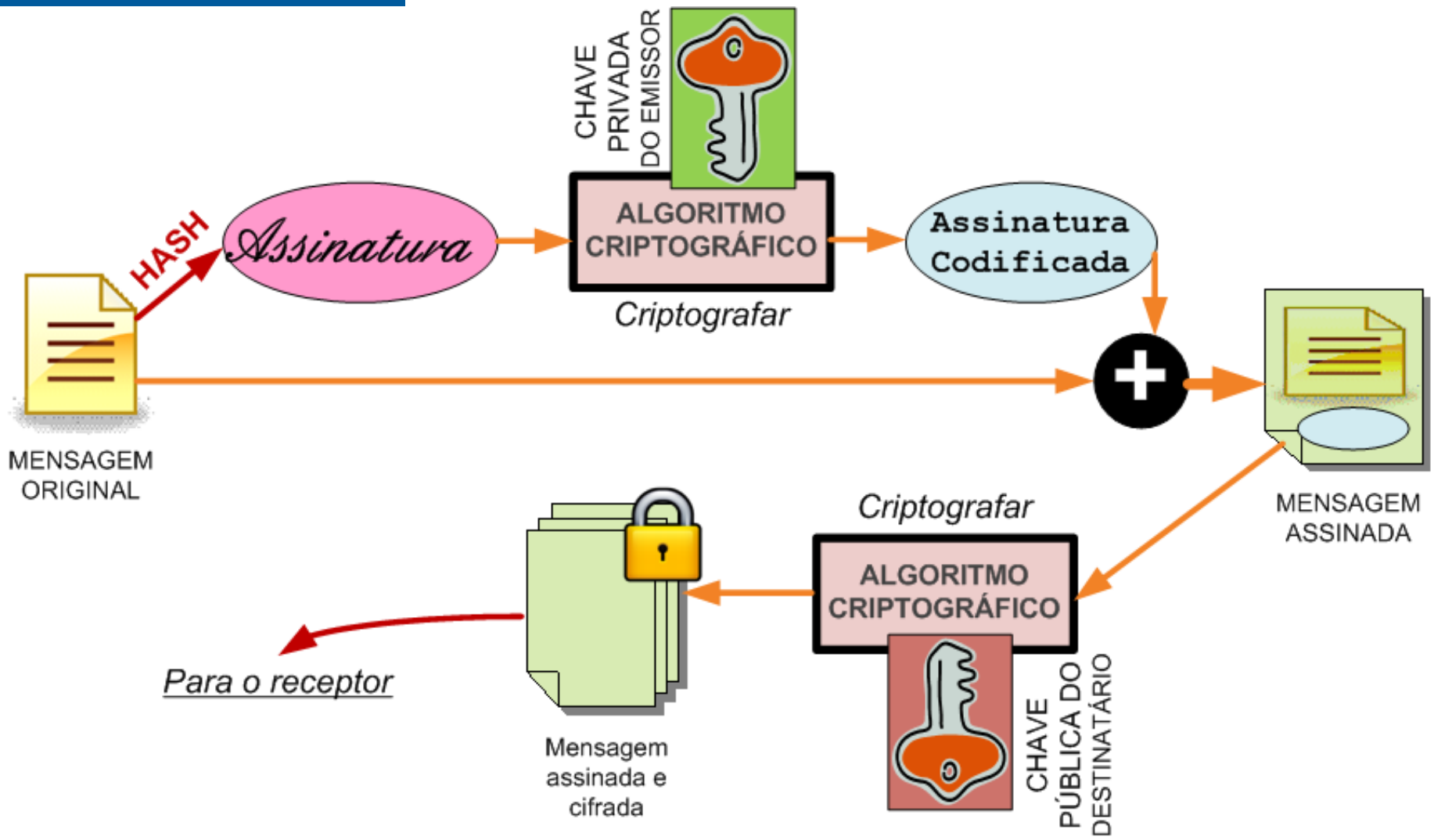
Assinatura Digital
Verificação

- Verificação da Assinatura Digital
  1. Executa-se a função MD (usando o mesmo algoritmo MD que foi aplicado ao documento na origem), obtendo-se um hash para aquele documento, e posteriormente, decifra-se a assinatura digital com a chave pública do remetente.
  2. A assinatura digital decifrada deve produzir o mesmo hash gerado pela função MD executada anteriormente.
  3. Se estes valores são iguais é determinado que o documento não foi modificado após a assinatura do mesmo, caso contrário o documento ou a assinatura, ou ambos foram alterados.

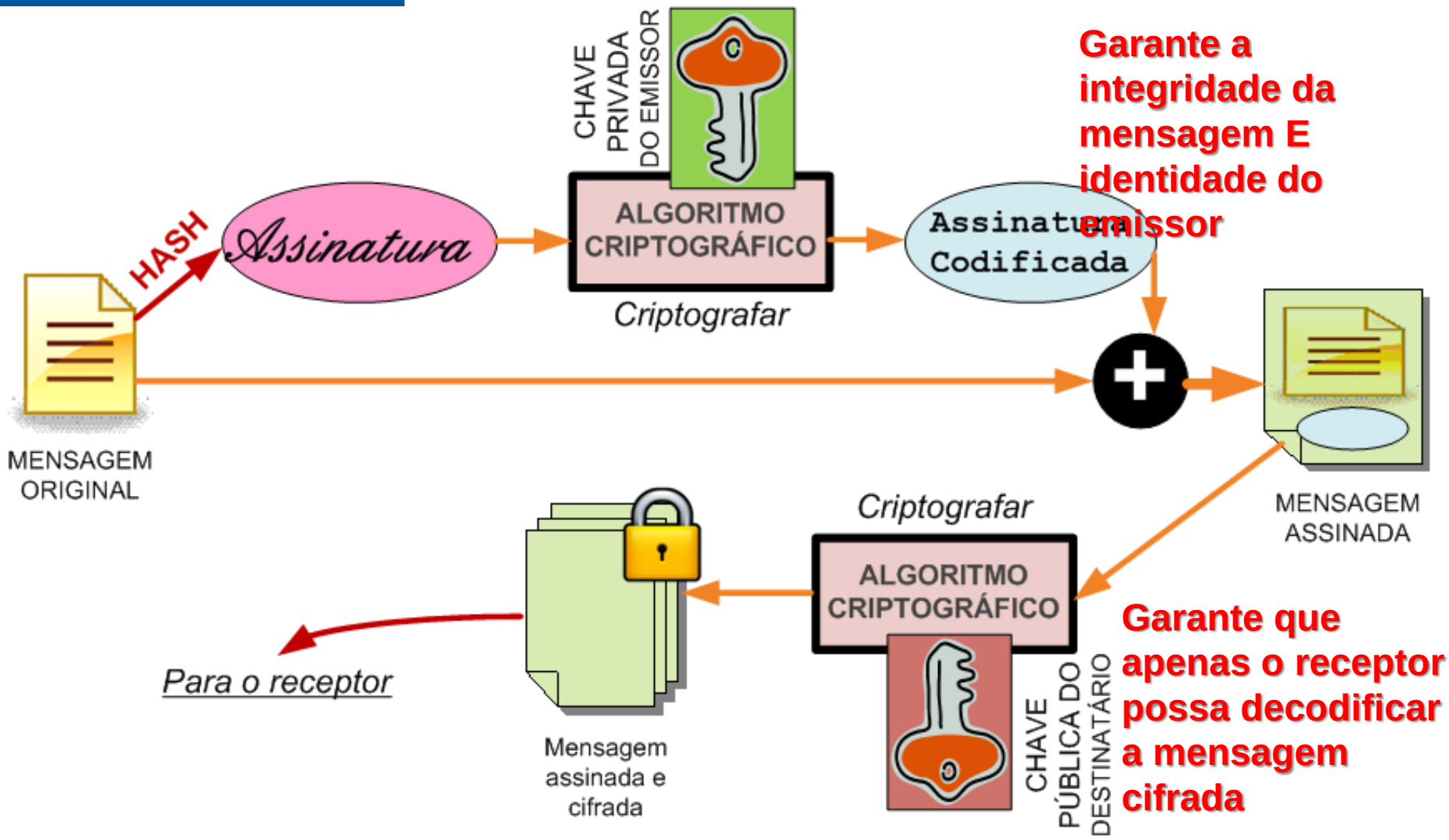
Assinatura digital – informa apenas que o documento foi modificado, mas não o que foi modificado e nem o quanto foi modificado.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Assinatura Digital



Assinatura Digital

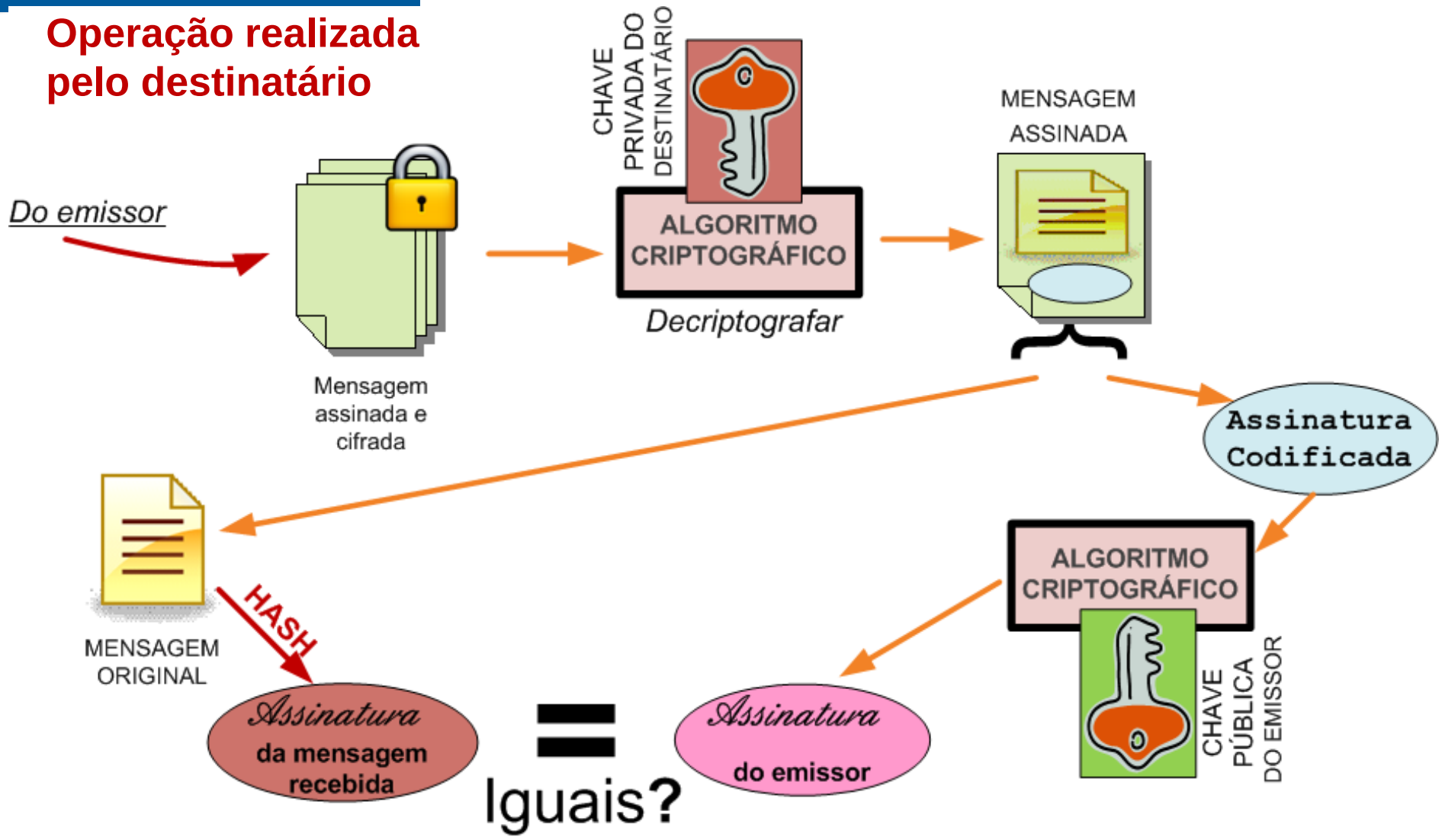


Garante a integridade da mensagem E identidade do emissor

Garante que apenas o receptor possa decodificar a mensagem cifrada

Assinatura Digital

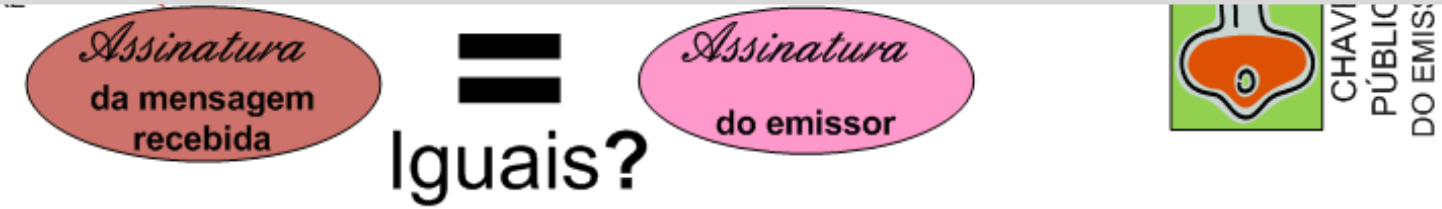
Operação realizada pelo destinatário



Assinatura Digital

-Assinatura enviada pelo emissor (e assinada com sua chave privada)
-Assinatura calculada pelo destinatário, sobre a mensagem recebida

As duas assinaturas são comparadas. Se forem iguais, estão garantidas:
-A integridade da mensagem, e;
-A identidade do emissor (a mensagem não foi forjada por um terceiro).



Assinatura Digital
Aplicações Práticas

- Correio eletrônico
  - Utilização
    - Autenticação de origem
    - Integridade do conteúdo
    - Confidencialidade
    - Não-repúdio
  - Protocolos
    - PEM (Public Enhanced Mail)
    - Security Multiparts for MIME/MOSS (Mime Object Security Services)
    - S/MIME (Secure/Multipurpose Internet Mail Extensions)
    - PGP (Pretty Good Privacy)
    - X.400

Assinatura Digital Aplicações Práticas

- WEB
  - Requisitos
    - Autenticação do servidor
    - Autenticação do cliente
    - Integridade de conteúdo
    - Confidencialidade
  - Protocolos
    - SSL (Secure Socket Layer) – Usado no HTTPS
    - Secure HTTP (Secure HyperText Transfer Protocol) – S-HTTP
  - Aplicativos
    - SSH (Secure Shell)
    - IPSec (Internet Protocol Security)
    - VPNs (Virtual Private Networks)
    - EDI (Electronic Data Interchange)

Fixação

- As assinaturas digitais são importantes porque oferecem garantias de **Integridade** e **Autenticidade** da Informação transmitida. Essas duas propriedades, juntas, asseguram a **Irretratabilidade**.
- A assinatura digital simétrica possui o problema da necessidade de um **Terceiro confiável**, que conhece TODAS as chaves usadas.
- A assinatura digital assimétrica resolve isso, mas é **Lenta**, além de impor limites para o tamanho do arquivo de entrada. Para resolver isso, são usados algoritmos de **Hash**. Estes algoritmos tem as seguintes características: Dado um arquivo de tamanho qualquer, a saída sempre tem tamanho **Fixo**. A alteração de um único bit no arquivo de entrada **Altera** totalmente o Hash. Encontrar um outro arquivo que gere o mesmo HASH é possível, e chamado de **Colisão**, mas isso é computacionalmente inviável para *hashes* de 160 bits ou superiores.