

Segurança da Informação

Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Assinatura Digital;

Situação de Aprendizagem:

- Assinatura Digital.

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

- Assinaturas de Chave Simétrica
- Assinaturas de Chave Pública
- Sumários de mensagens (*Message Digests*)

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

Desvantagens

- » Idoneidade da autoridade central.
- » Autoridade central pode ler todas as mensagens.

Assinatura Digital

Chave Pública



Alice



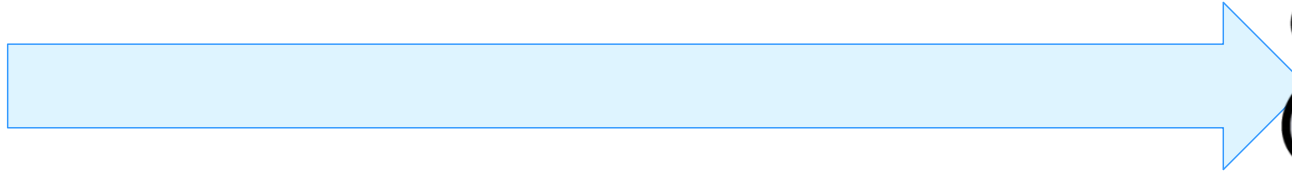
Bob

Assinatura Digital

Chave Pública



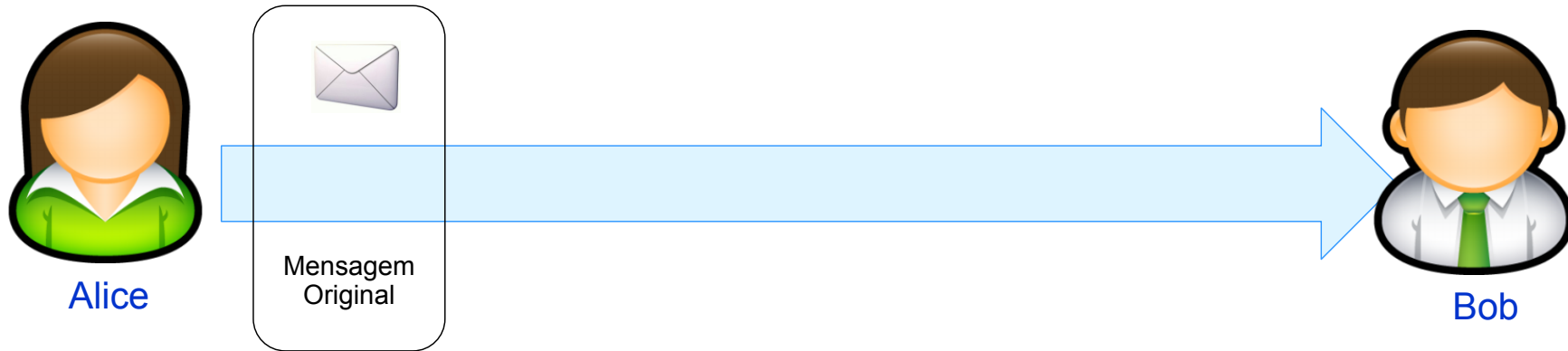
Alice



Bob

Assinatura Digital

Chave Pública



Assinatura Digital

Chave Pública



Alice



Mensagem
Original



Mensagem
Criptografada
com chave
privada
de Alice



Bob

Assinatura Digital

Chave Pública



Alice



Mensagem
Original



Mensagem
Criptografada
com chave
privada
de Alice



Mensagem
Criptografada
com chave
Pública
de Bob



Bob

Assinatura Digital

Chave Pública



Alice



Mensagem
Original



Mensagem
Criptografada
com chave
privada
de Alice



Mensagem
Criptografada
com chave
Pública
de Bob



Mensagem
Criptografada
com chave
privada
de Alice



Bob

Assinatura Digital

Chave Pública



Alice



Mensagem
Original



Mensagem
Criptografada
com chave
privada
de Alice



Mensagem
Criptografada
com chave
Pública
de Bob



Mensagem
Criptografada
com chave
privada
de Alice



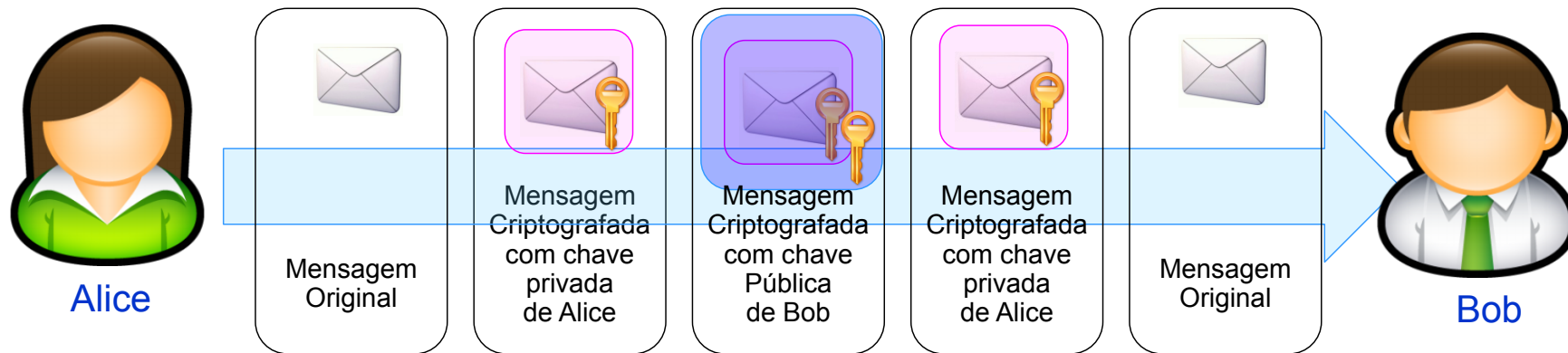
Mensagem
Original



Bob

Assinatura Digital

Chave Pública



- Reúnem **sigilo** e **autenticação**
- Em geral, o sigilo não é necessário
- Cifragem da mensagem inteira é lenta => Sumário de Mensagens

Assinatura Digital

Sumário 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 uma *string* de bits de tamanho fixo.
- **Função hash** – geralmente denominada **sumário de mensagens** (MD).

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.

Assinatura Digital

Processo



Alice



Mensagem
Original



Bob

Assinatura Digital

Processo



Alice



Mensagem
Original



Bob



Função
de hash

11010...10101

Assinatura Digital

Processo



Alice



Função
de hash

11010...10101



Cifrar
Chave
Privada
Alice

11010...10101



Bob

Assinatura Digital

Processo




Alice



Mensagem
Original



11010...10101 

Mensagem
Original
+
Assinatura



Bob

Assinatura Digital

Processo



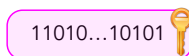
Alice



Bob



Função de hash



Decifrar usando Chave Pública Alice

Assinatura Digital

Processo



Alice



Bob



Função
de hash

11010...10101



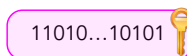
11010...10101



Assinatura
Confere



Assinatura
Não confere



Decifrar
usando
Chave
Pública
Alice

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*)
- Secure HTTP (*Secure HyperText Transfer Protocol*)

» **Aplicativos**

- SSH (*Secure Shell*)
- IPSec (*Internet Protocol Security*)
- VPNs (*Virtual Private Networks*)
- EDI (*Electronic Data Interchange*)