INE 5429
Segurança em Computação
Introdução

Prof. Ricardo Felipe Custódio, Dr.
custodio@inf.ufsc.br

19 de agosto de 2011

Definições

Autenticação (6 fatores)

Beto sabe que Alice enviou a mensagem

Integridade

A mensagem que Beto recebeu foi a que Alice enviou

Não Recusa (3 tipos)

Alice não pode negar após Beto ter recebido uma mensagem dela, que ela enviou a mensagem

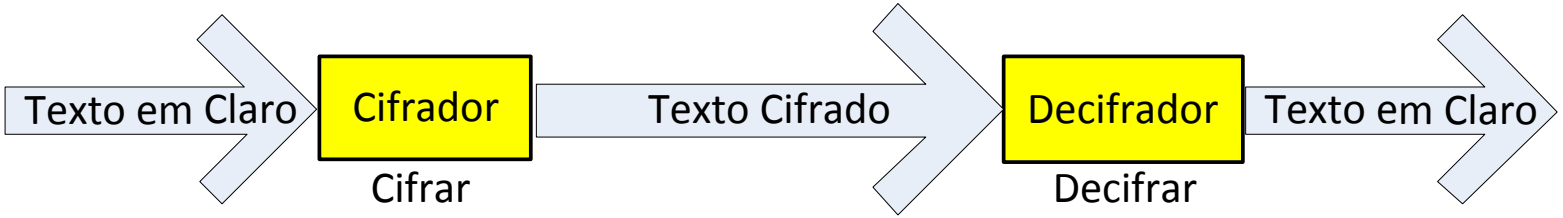
Criptografia

Estudo da Escrita (Grafia) Secreta (Cripto)

- Esconder uma informação
- Verificar a exatidão de uma informação
- Base tecnológica para problemas de segurança em comunicações e em computação

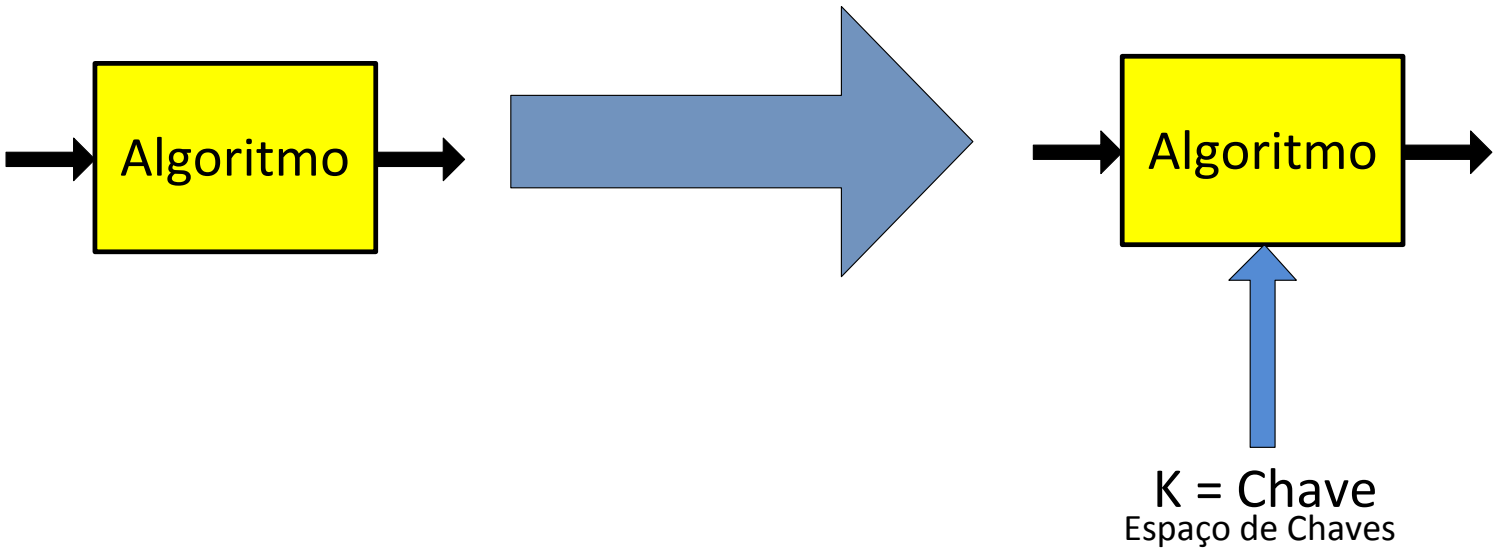
Definições e Terminologia

- Emissor (Alice) e Receptor (Beto)
- Texto Original ou Texto Limpo
- Cifrar
- Decifrar
- Criptografia X Criptoanálise = Criptologia



Algoritmos X Chaves

Princípio de Kerckhoffs



Cifradores na História

- Uma das mais antigas profissões $\approx$ 4.000 anos
- Egípcios antigos cifravão alguns de seu hieróglifos
- O barro de Phaistos (1600 a.c) ainda não decifrado
- Cifrador de Júlio César

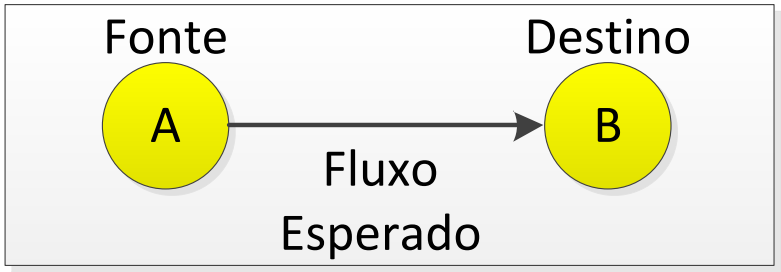
Esteganografia

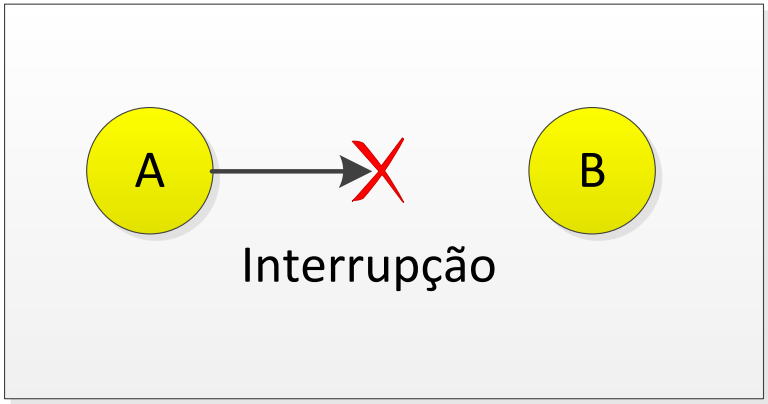
- Marcação de caracteres
- Tinta Invisível
- Pequenos furos no papel
- Moderna Esteganografia
- Uso de bits não significativos
- Área não usada

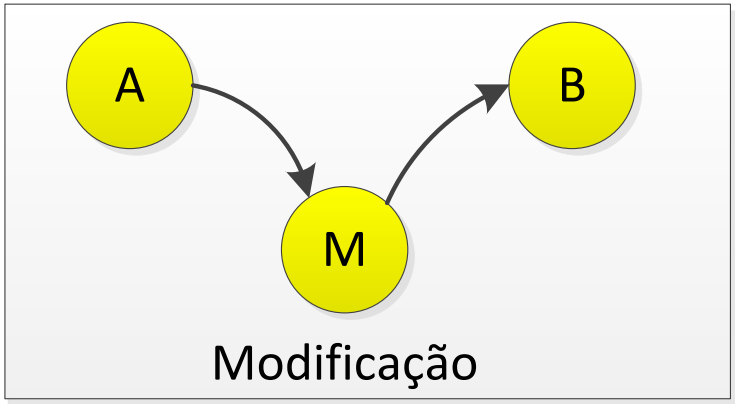
Fontes de Problemas de Segurança

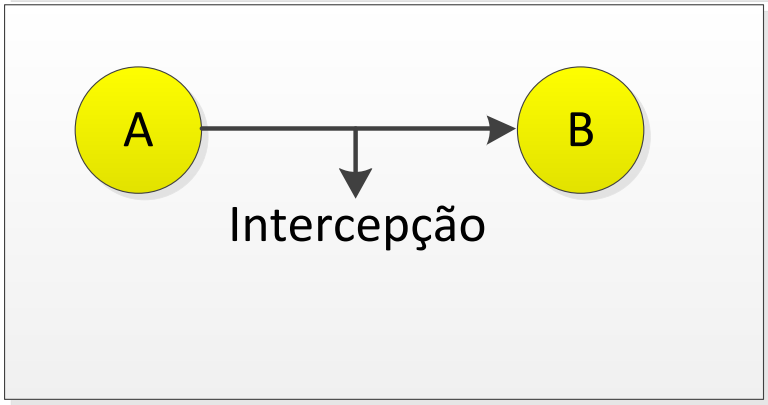
Estudante	Alterar/mandar e-mail divertido em nome de outros
Hacker	Examinar a segurança do Sistema; Roubar informação
Representante de Vendas	Dizer que representa todo o Brasil e não somente São Paulo
Empresário	Descobrir o plano de marketing estratégico do competidor
Ex-empregado	Vingar-se por ter sido despedido
Contador	Desviar dinheiro de uma empresa
Corretor	Negar uma solicitação feita a um cliente por e-mail
Inimigo	Aprender o poderio militar de um inimigo
Terrorista	Roubar segredos de guerra

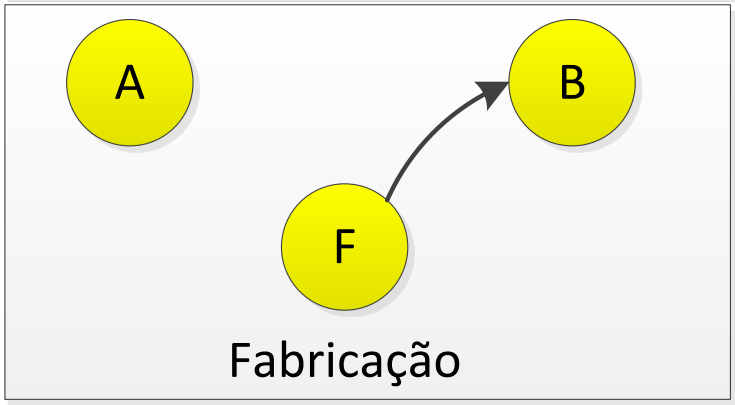
Ameaças de Segurança







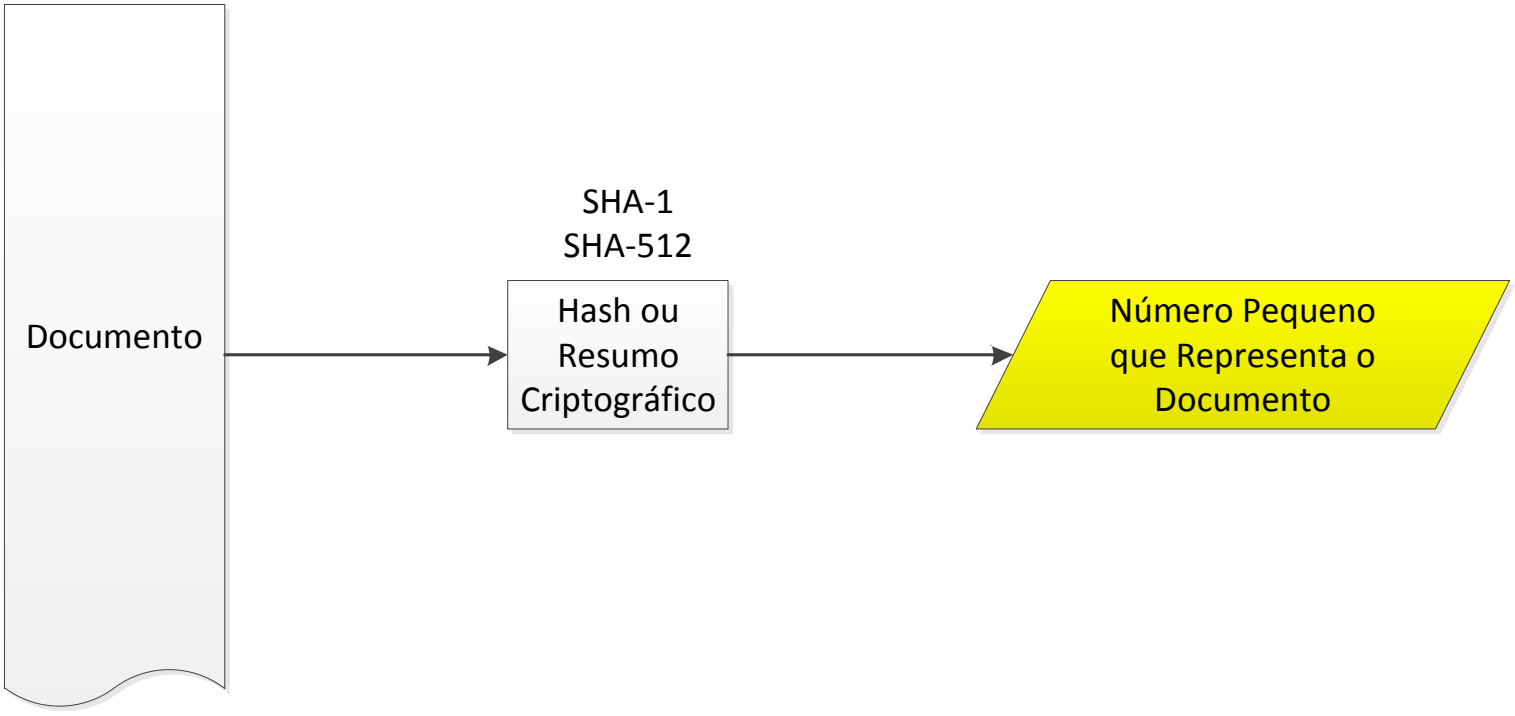




Motivações

- Segurança da Informação
- Segurança Nacional
- Restrições de Exportação de Produtos
- Comércio Eletrônico
- Internet - Caminho duplo
- Aplicação dos Conceitos de Teoria da Computação
  - Autômatos
  - Computabilidade
  - Complexidade

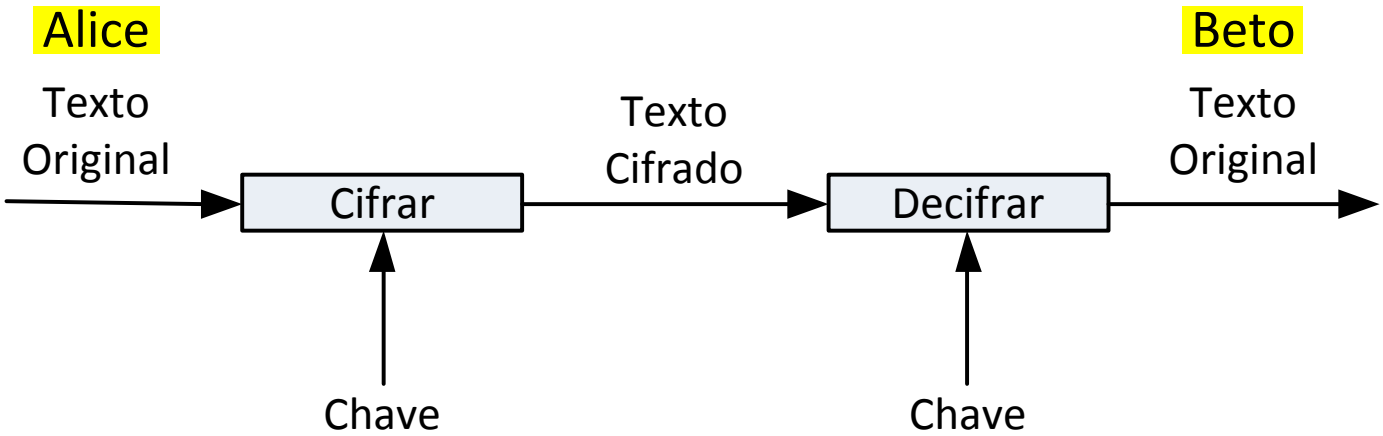
Integridade



Exemplo: Urna Eletrônica

75-AF-82-13-7B-CB-77-18-72-93-75-AF-82-13-7B-CB-77-18-72-93

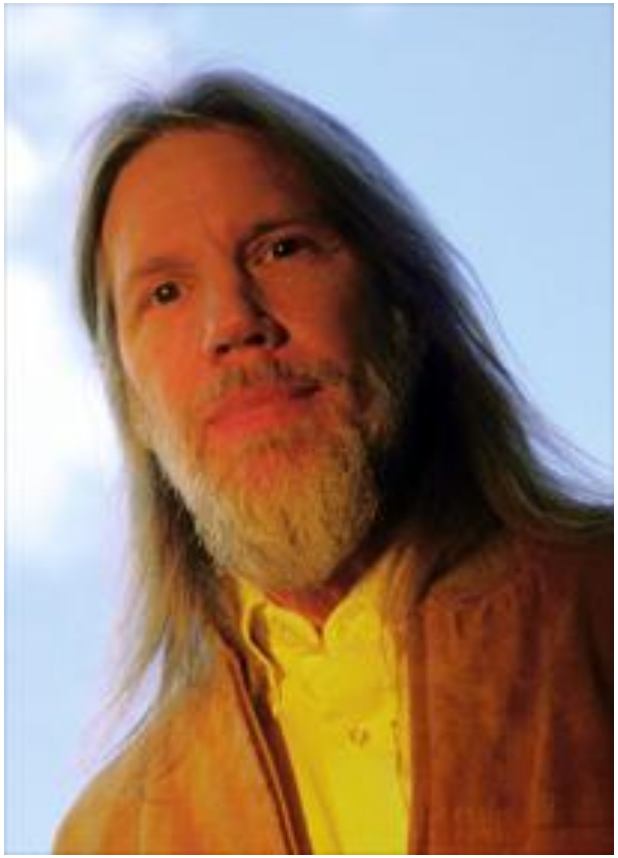
Criptografia



Diffie e Hellman

Diffie, Whitfield; Hellman, Martin E. New Directions in Cryptography. IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, p. 644-654.

Whitfield Diffie

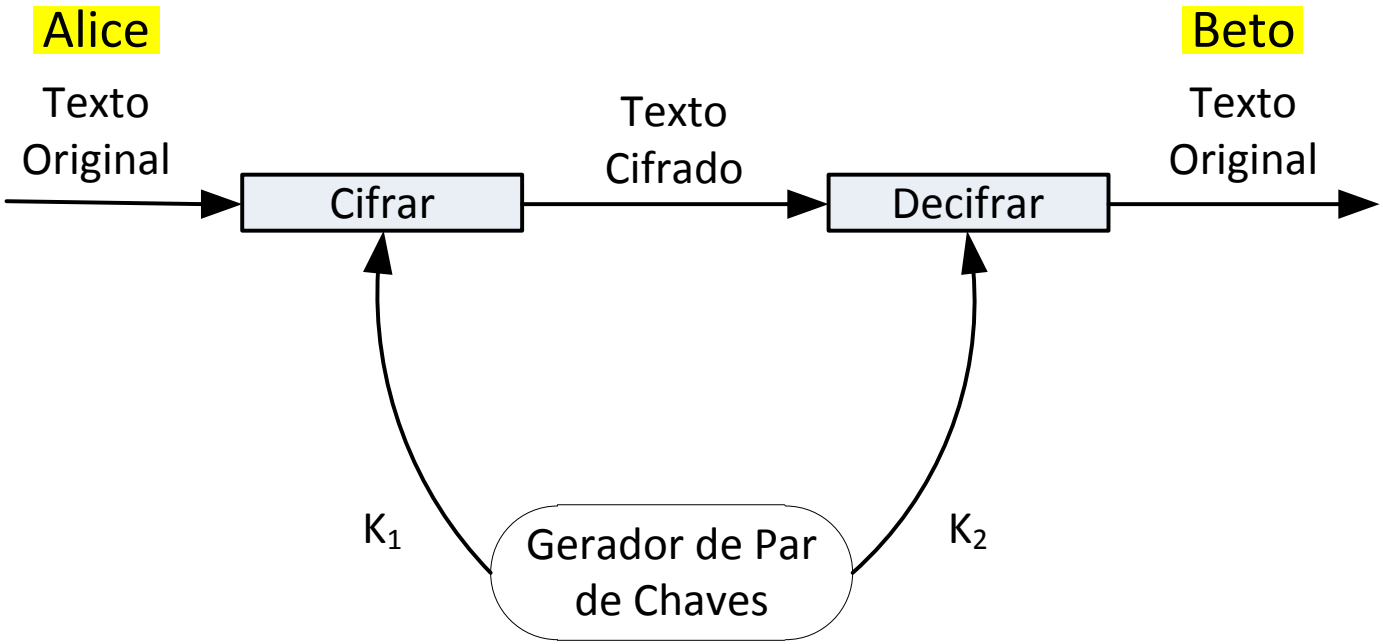


Nascimento: 05/06/1944

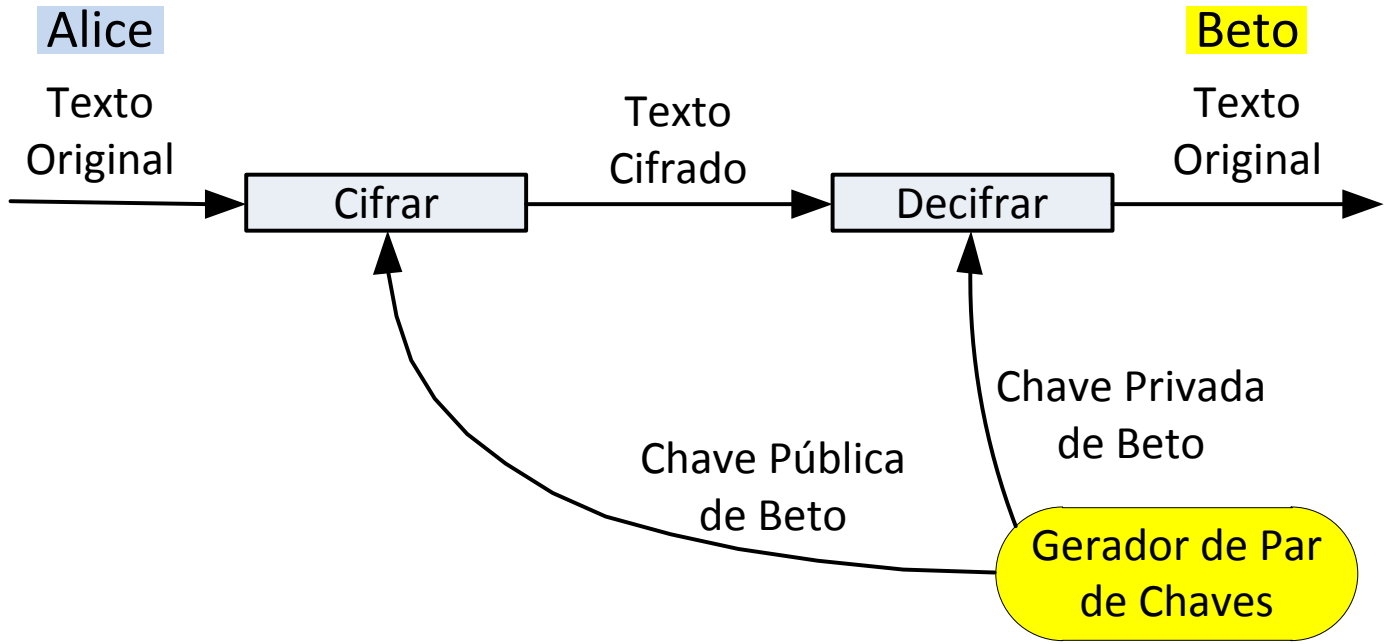
Martin Edward Hellman

Nascimento: 02/10/1945

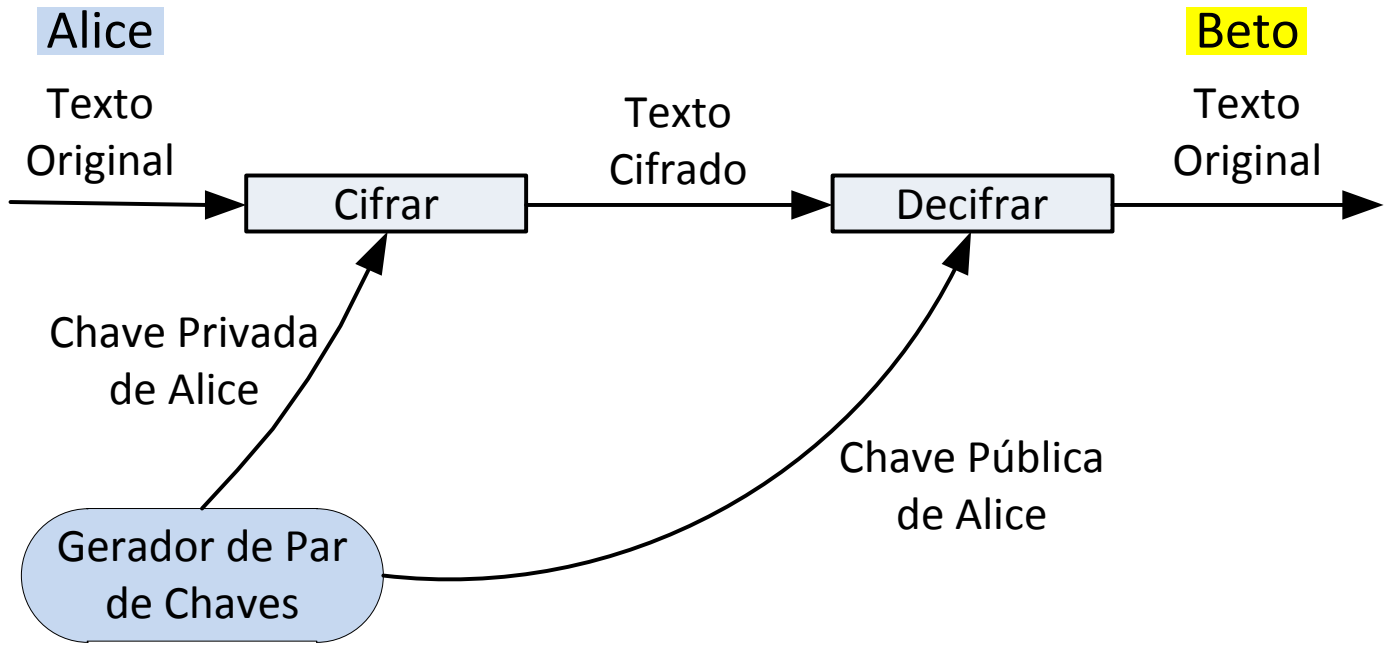
Par de Chaves Criptográficas



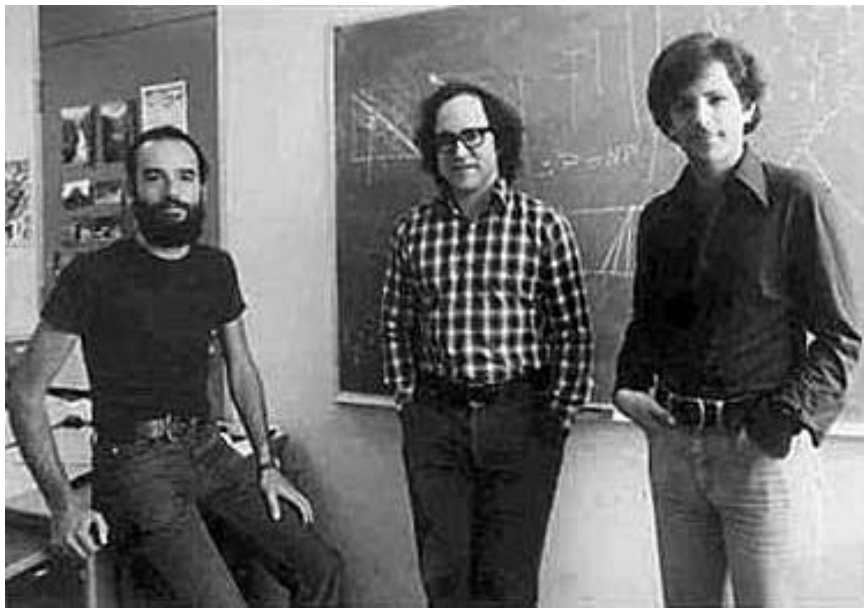
Sigilo


Alice
Texto Original
Cifrar
Texto Cifrado
Decifrar
Beto
Texto Original
Chave Pública de Beto
Chave Privada de Beto
Gerador de Par de Chaves

Autenticação



RSA - 1978



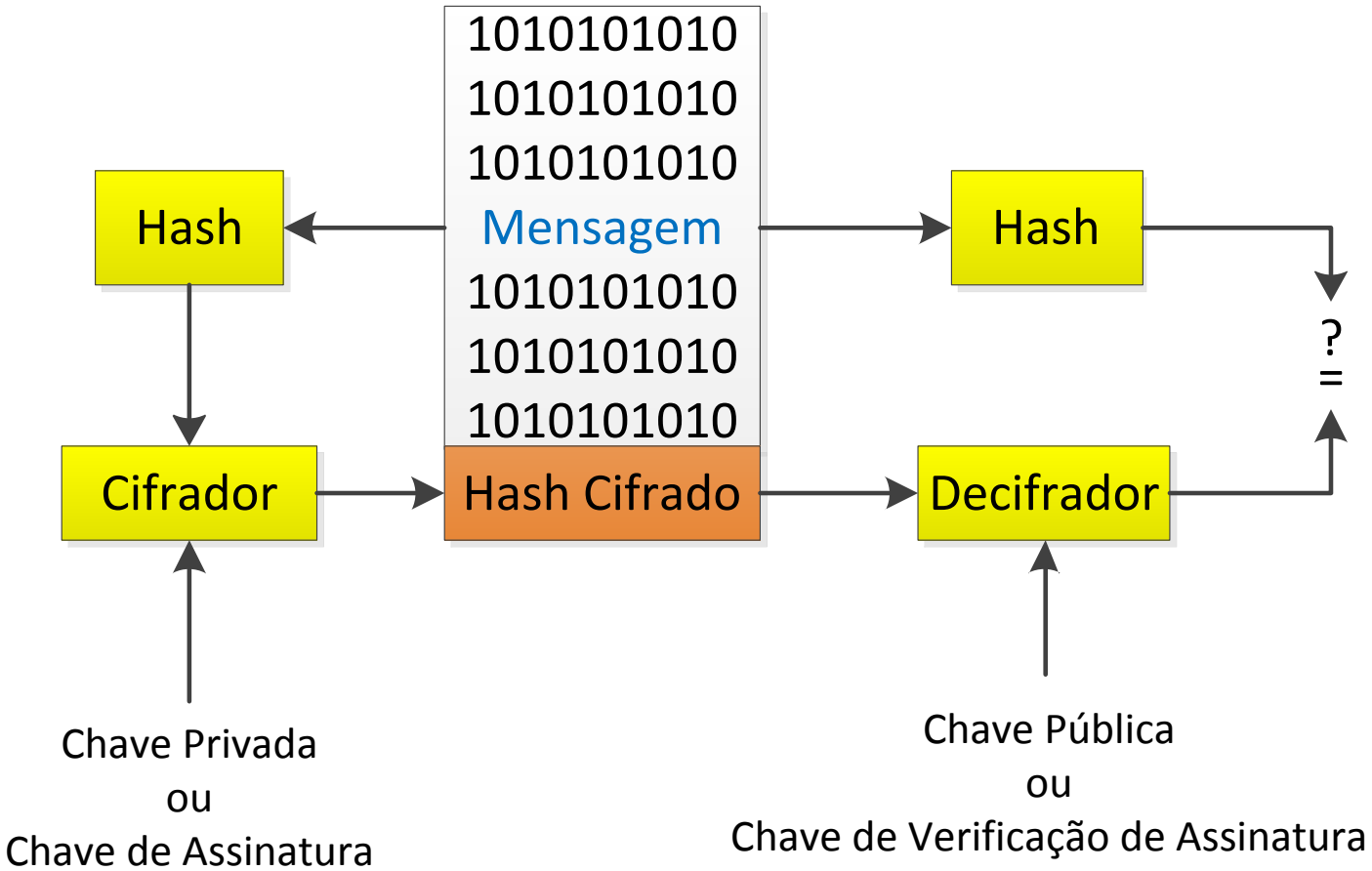
Ronaldo Linn Rivest
1947

Adi Shamir
1952

Leonard Max Adleman
1945

2010

Assinatura Digital



Aplicações da Criptografia

- Assinatura Digital
- Autenticação Descentralizada
- Confiança nos Documentos Eletrônicos
  - Documentos Papel $\rightarrow$ Documentos Eletrônicos
- Aumentar a confiança nas transações eletrônicas
- Sigilo da Informação

Exemplos de Aplicações

- Site Seguro (SSL, WTLS)
  - Cliente Web
- Entrega de Documentos pela Internet
- E-mail Seguro (Assinatura e/ou Sigilo)
- Assinatura de Documentos
- IPSec
- VPN
- Autenticação