Universidade Federal de Santa Catarina - UFSC
Centro Tecnológico - CTC
Laboratório de Segurança em Computação - LabSEC

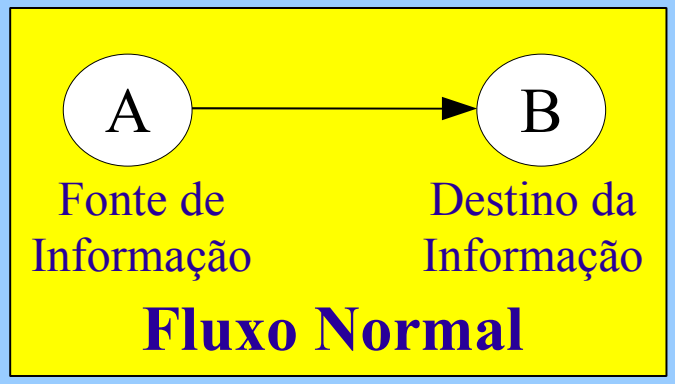
Segurança em Computação

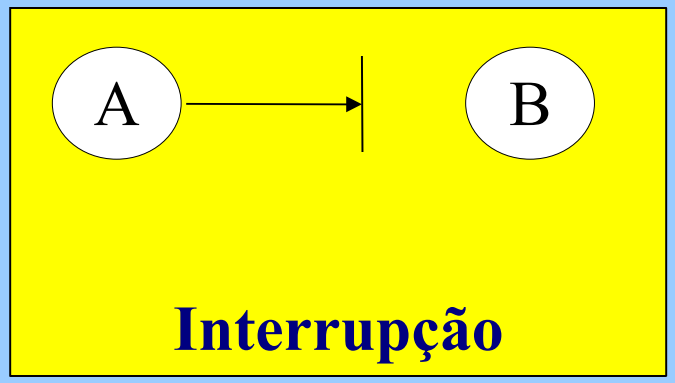
Criptografia e suas Aplicações

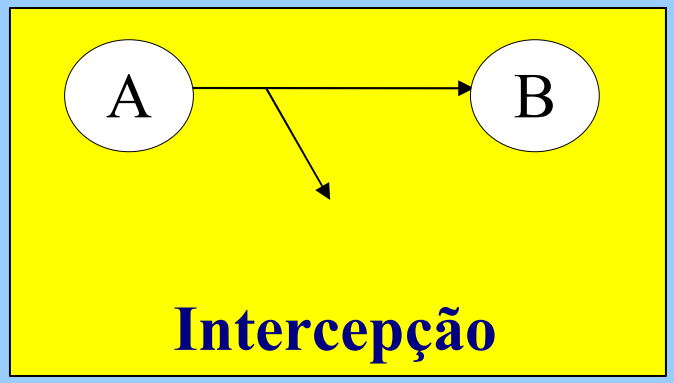
Prof. Ricardo Felipe Custódio
http://www.labsec.ufsc.br

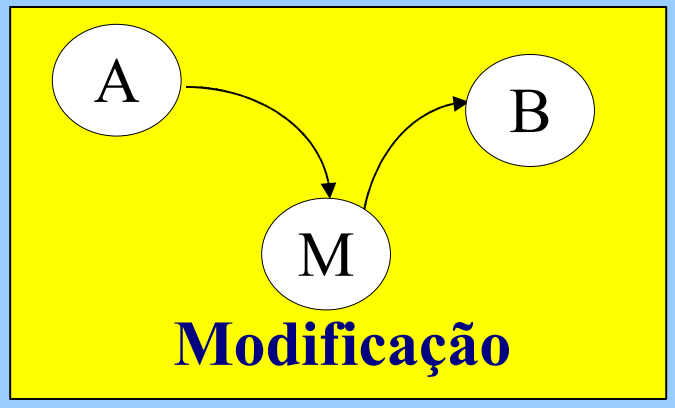
Versão 2.0070807

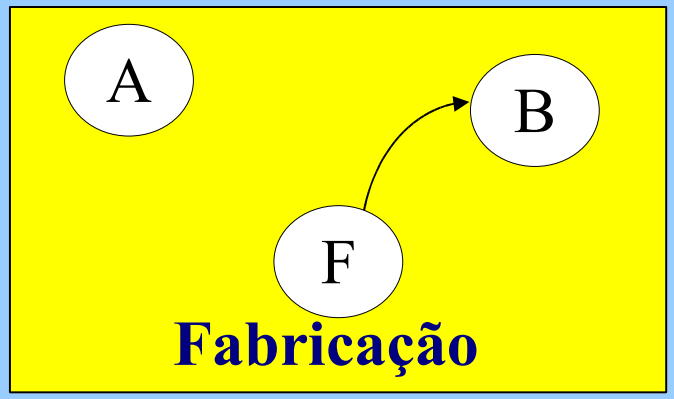
Ameaças na Segurança



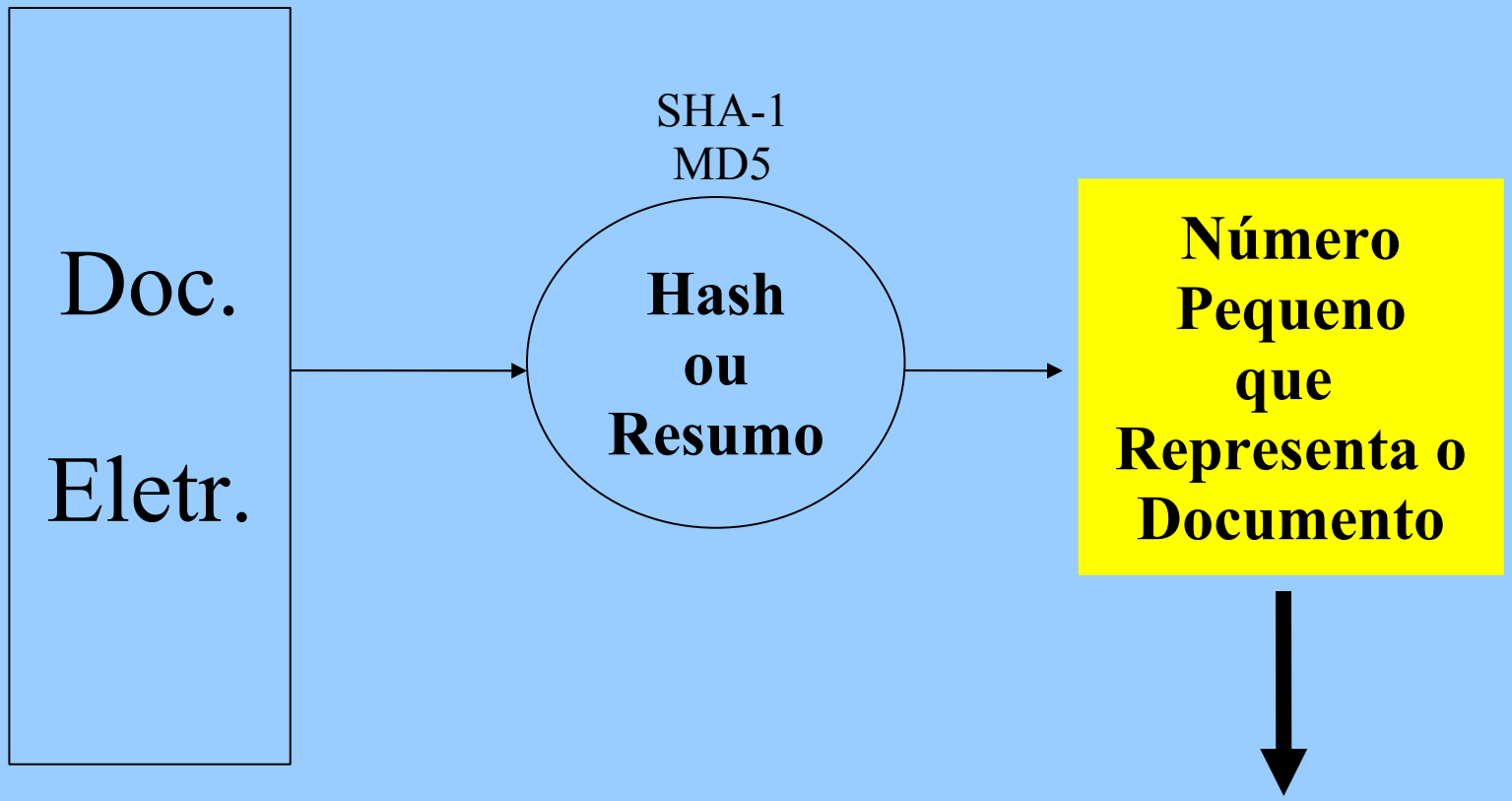






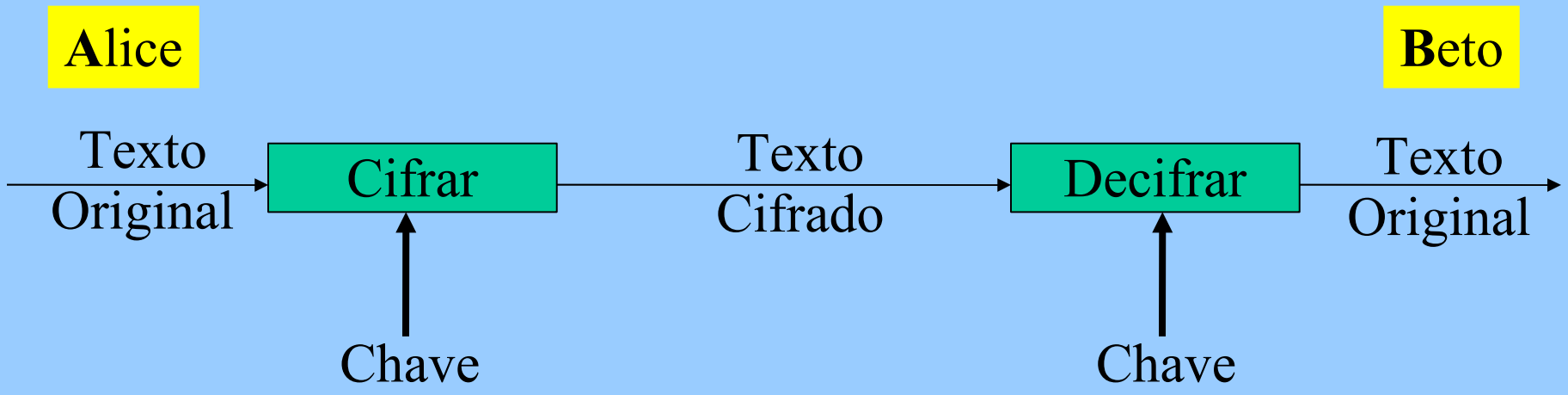


Integridade

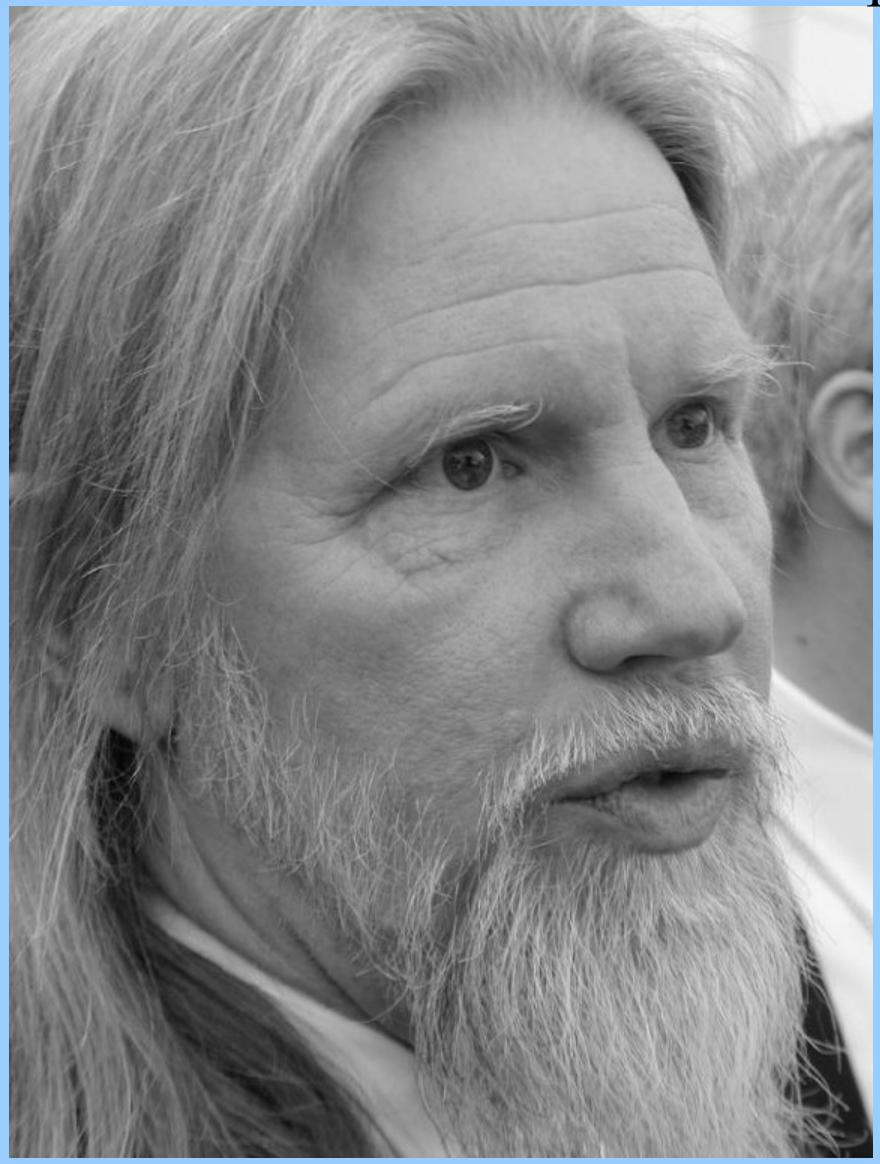


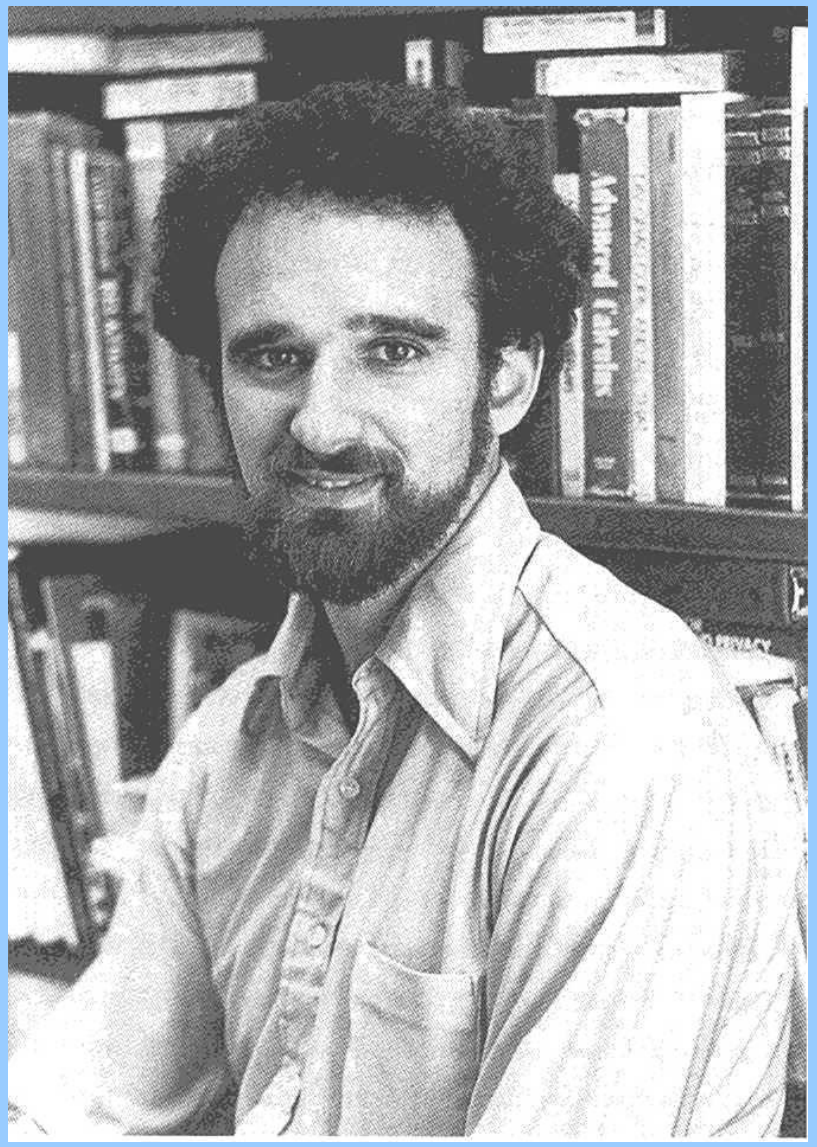
Exemplo: Urna Eletrônica
75-AF-82-13-7B-CB-77-18-72-93-75-AF-82-13-7B-CB-77-18-72-93

Criptografia

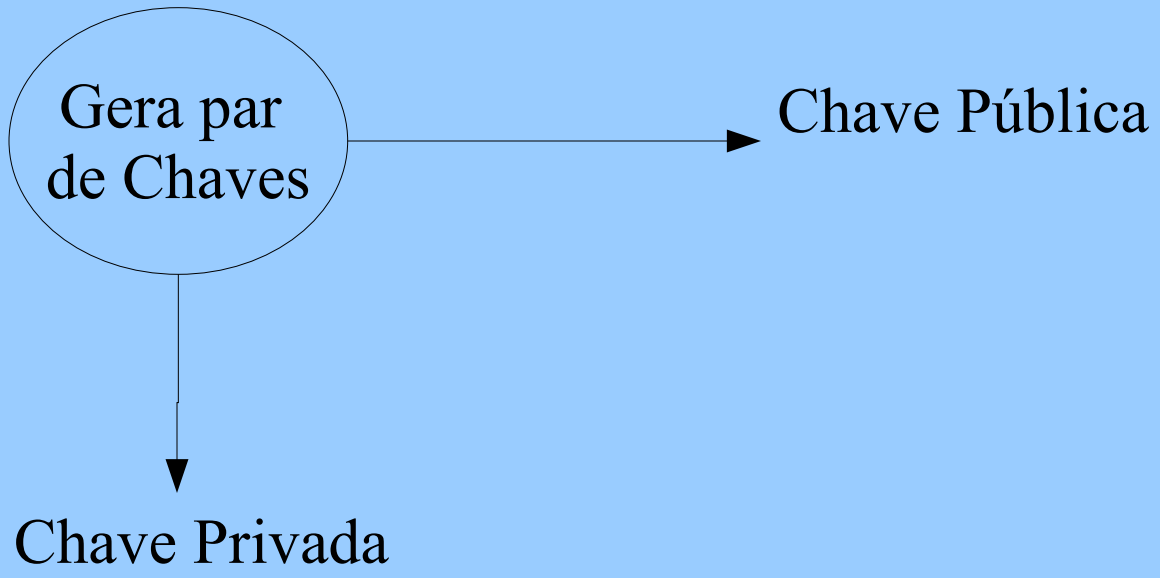


Diffie 1976 Hellman

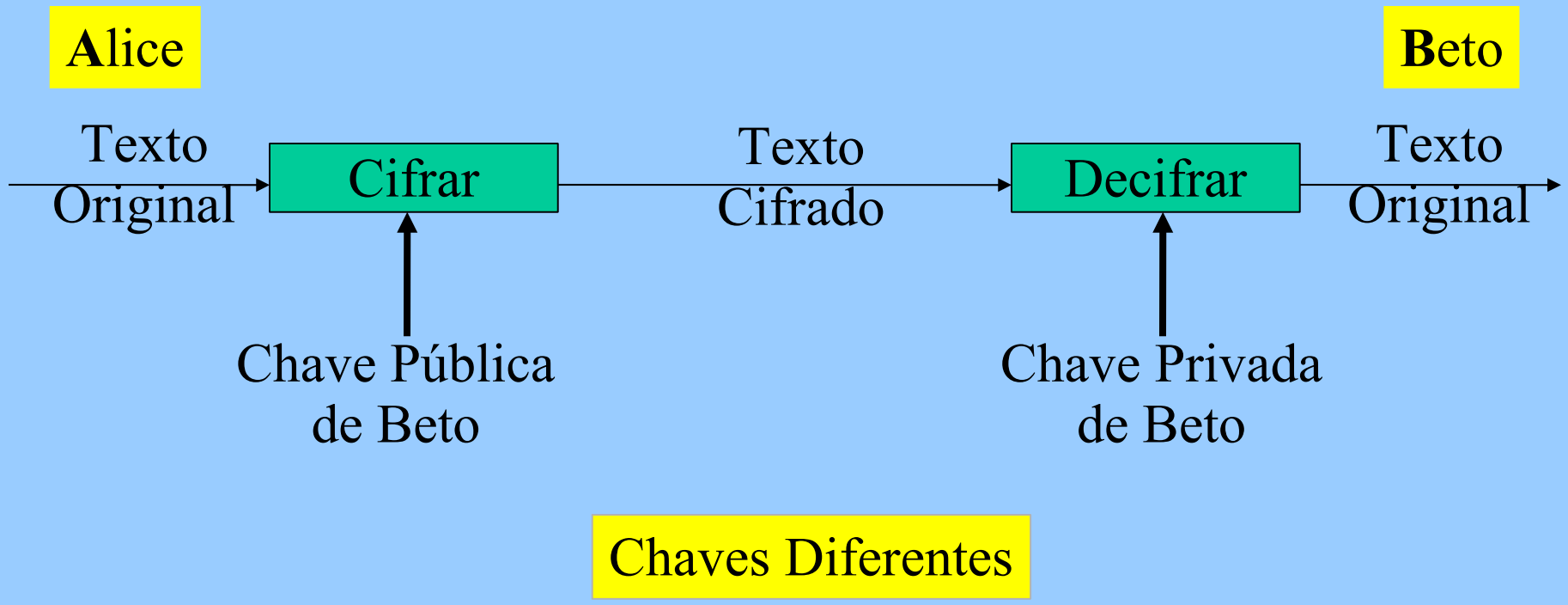




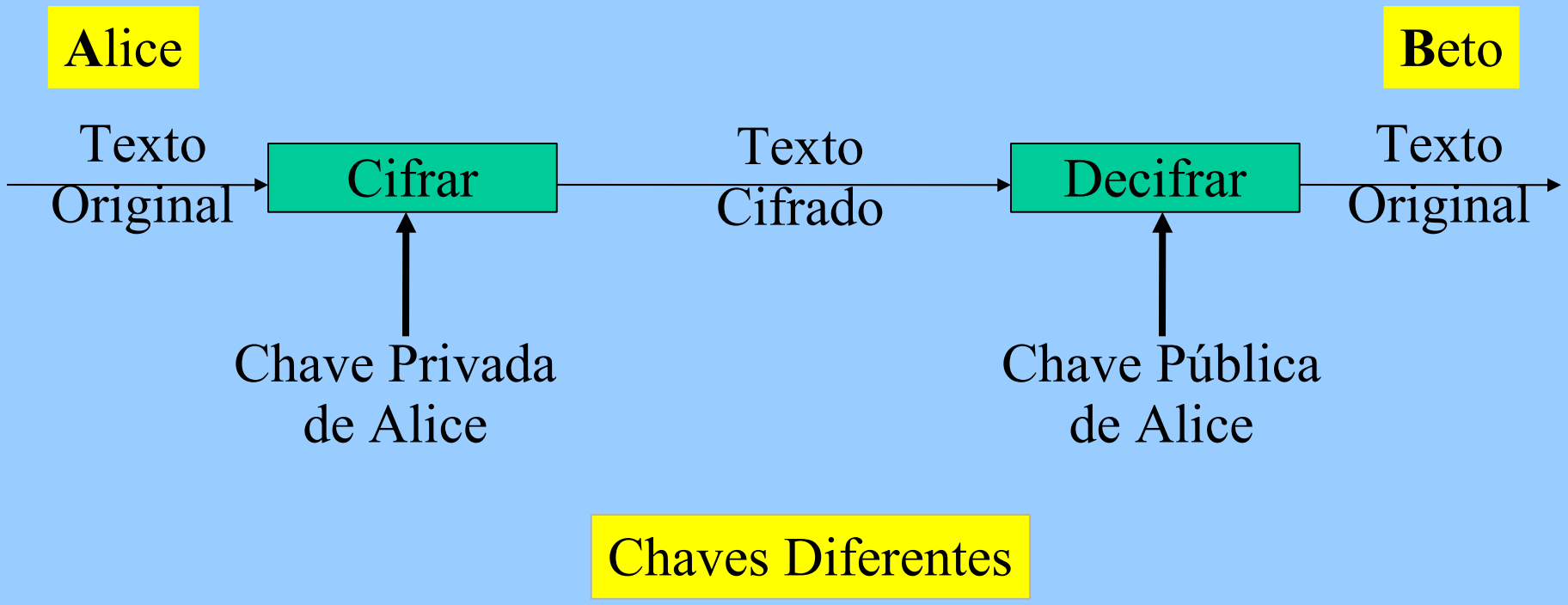
Gerador de Par de Chaves



Criptografia Assimétrica
Confidencialidade



Criptografia Assimétrica
Autenticação



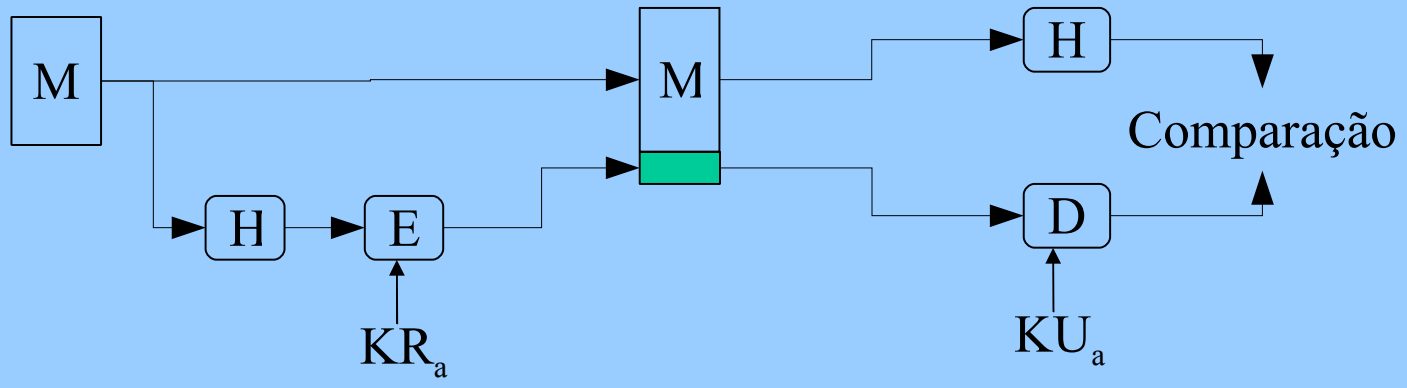
RSA - 1978

Ron Rivest

Adi Shamir

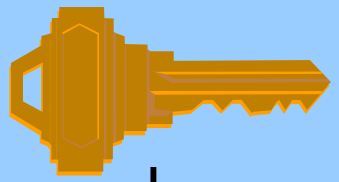
Leonard Adleman

RSA - Assinatura Digital



M - Mensagem
H - Função Resumo ou Hash
E - Cifrar
KR_x - Chave Privada de x
D - Decifrar
KU_x - Chave Pública de x

Certificado Digital = Identidade Digital



Chave Privada da AC

Identificação do Usuário

Chave Pública do Usuário

Nome da Autoridade Certificadora

Extensões

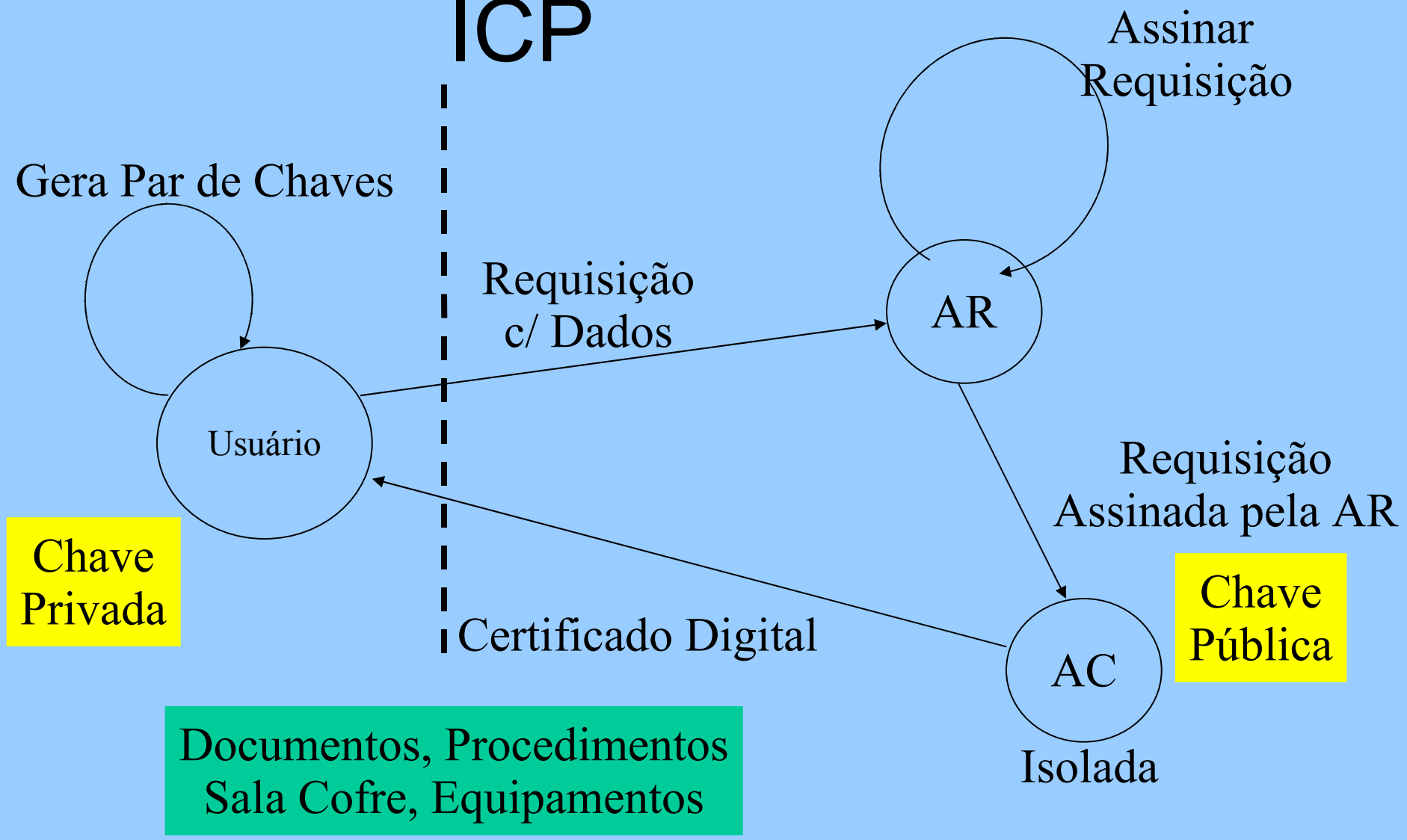
Gera Assinatura Digital

Assinatura Digital da Autoridade Certificadora

Recomendação ITUT X.509v3

Mostrar Certificado X.509

Componentes de uma ICP



Utilidade
Para que Serve?

- Assinatura Digital
- Autenticação Descentralizada
- Confiança nos Documentos Eletrônicos
  - Documentos Papel -> Documentos Eletrônicos
- Aumentar a confiança nas transações eletrônicas
- Sigilo da Informacão

Aplicações Comuns

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

Outras Aplicações

Mostrar Conexão SSL