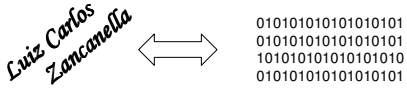
Assinatura Digital



Requisito básico da assinatura digital:

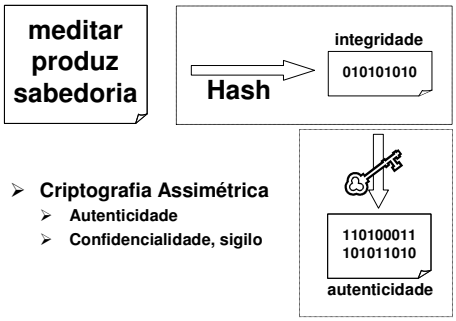
atribuir confiabilidade a um documento eletrônico, da mesma forma que uma assinatura de punho (ou firma) atribui a um documento papel.

Confiabilidade = Originalidade: → INTEGRIDADE
→ AUTORIA

Assinatura Digital

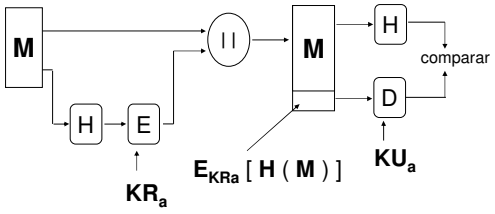
- Requisitos técnicos da assinatura digital:
  - Depender do Conteúdo;
  - Usar informação única do originador;
  - Fácil de produzir;
  - Fácil de reconhecer e verificar;
  - Inviável de forjar;
  - Deve ser prático manter uma cópia da assinatura.

Assinatura Digital



- **Criptografia Assimétrica**
  - **Autenticidade**
  - **Confidencialidade, sigilo**

Assinatura Digital com RSA



Digital Signature Standard (DSS)

1991, Digital Signature Algorithm (DSA)

NIST (National Institute Stardards and Technology)

Padrão do governo americano

- Prova de autenticidade
- Integridade
- Troca de chaves

Digital Signature Standard (DSS)

Parâmetros do DAS

p = primo, onde $2^{L-1} < p < 2^L$, $512 \le L \le 1024$, e L múltiplo de 64

q = primo divisor de p-1, onde $2^{159} < q < 2^{160}$ (q tem 160 bits)

$g = h^{(p-1)/q} \bmod p$, onde: $1 < h < (p-1)$, tal que $h^{(p-1)/q} \bmod p > 1$

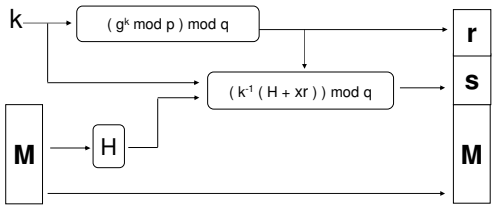
KP → **x** = número pseudorandômico com $0 < \mathbf{x} < q$

KU → $\mathbf{y} = g^x \bmod p$

k = número pseudorandômico com $0 < k < q$, por assinatura

Digital Signature Standard (DSS)

Assinatura de Mensagem



Digital Signature Standard (DSS)

Verificação da Assinatura