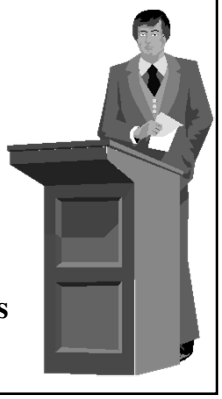


Funções *Hash*

Prof. Dr. Adilson Eduardo Guelfi[1]
Prof. Dr. Volnys Borges Bernal[2]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP



Agenda

- Introdução
- Função *hash*
- Utilização de funções *hash*
- Principais algoritmos
- Exercícios
- Referências Bibliográficas

Introdução

Introdução

- **Função hash**
  - Bloco básico para prover a integridade de dados

- **Exemplos de sistemas que apresentam mecanismos de integridade**

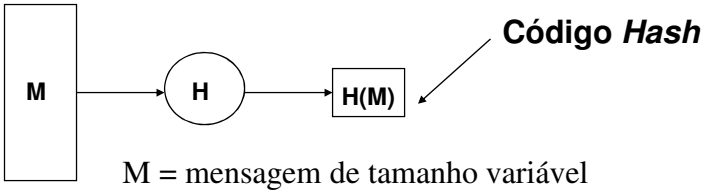
  (exemplos de situações nas quais é necessário prover integridade da informação em trânsito ou armazenada contra erros de transmissão ou armazenamento)

  - Armazenamento de informações em disco
  - Comunicação de dados

Função *hash*

Funcão *hash*

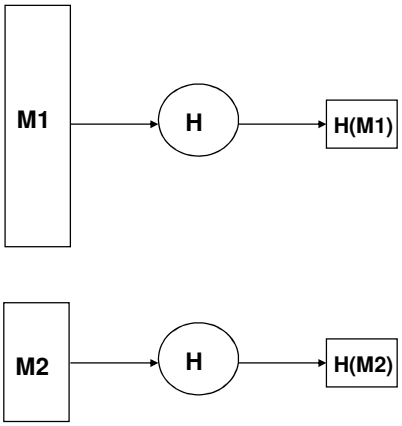
- **Função Hash Unidirecional**
  - Função matemática que envolve todos os bits da mensagem
  - Aceita como entrada uma mensagem M de tamanho variável e gera como saída um código *hash* de tamanho fixo
  - Bloco básico para implementação do serviço de integridade que depende apenas de M como entrada



M = mensagem de tamanho variável
H = função hash
H(M) = resultado *hash* de tamanho fixo (código)

Função *hash*

- **Código *hash* é de tamanho fixo independentemente do tamanho da mensagem de entrada:**



Mensagens iguais geram o mesmo código hash

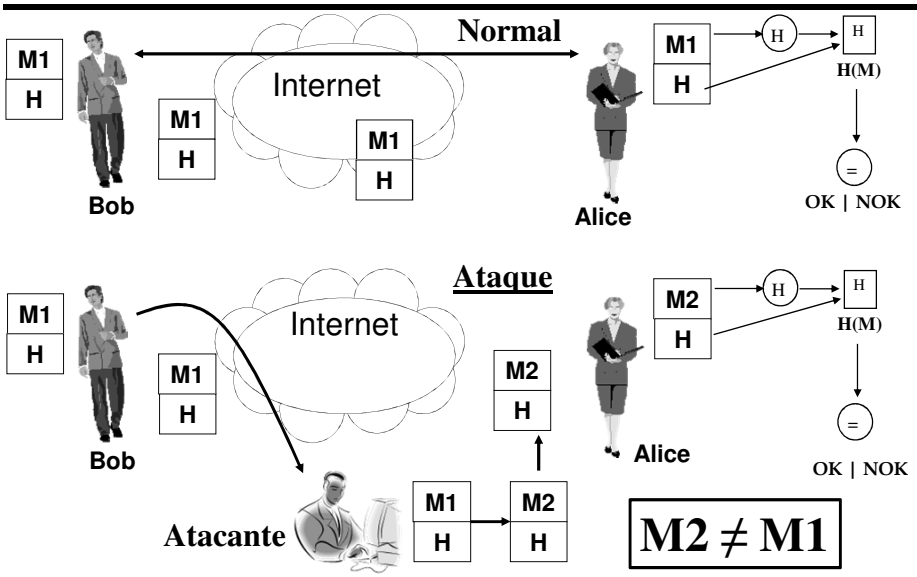
Mensagens diferentes geram códigos hash diferentes

Utilização de função *hash*

Utilização de função *hash*

- **Como visto anteriormente, a função hash é um mecanismo para a implementação do serviço de integridade.**
- **Modificações podem ocorrer de forma intencional ou não intencional**
- **<u>Isoladamente, a função hash não é suficiente para se evitar modificações intencionais!</u>**
  - Como visto nos exemplos anteriores, são necessários mecanismos adicionais para evitar as modificações intencionais
  - Neste caso, o código ou resultado *hash* deve ser protegido para impedir que seja alterado por entidades não autorizadas.
- **Existem duas formas de proteger o código *hash***
  - Criptografia simétrica
  - Criptografia assimétrica

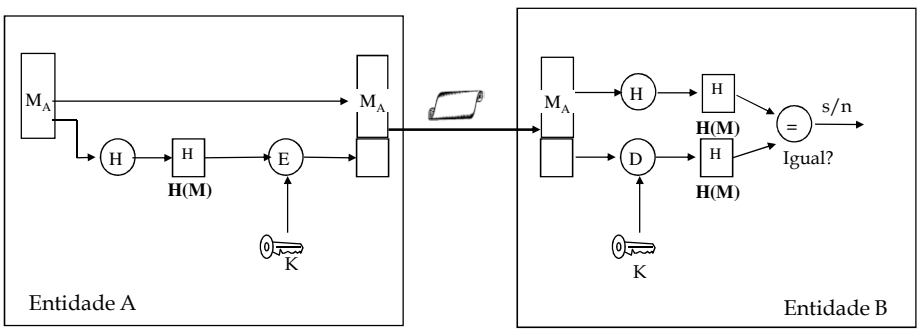
Utilização de função *hash*



Código Hash Protegido com Criptografia Simétrica

Hash protegido com criptografia simétrica

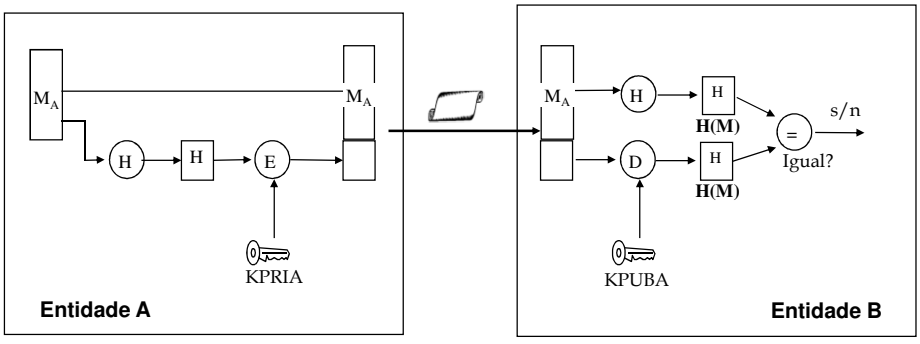
- **Proteção do código *hash* com criptografia simétrica**
- **Serviços de segurança oferecidos:**
  - baixo nível de autenticação do autor
  - integridade



Código Hash Protegido com Criptografia Assimétrica

Hash protegido com criptografia assimétrica

- **Proteção do código *hash* com criptografia assimétrica**
- **Serviços de segurança oferecidos:**
  - certo nível de autenticação do autor
  - Integridade



Principais Algoritmos de Hash

Principais algoritmos

Fonte: Applied Cryptography

Algoritmo de Hash	Compr. Hash	kbytes/s
GOST Hash	256	11
MD4 - Message Digest 4	128	236
MD5 - Message Digest 5	128	174
N-HASH (12 rounds)	128	29
N-HASH (15 rounds)	128	24
RIPE-MD	128	182
RIPE-MD-160	160	---
SHA-1 Secure Hash Algorithm	160	75
SHA-2 Family (256, 512 etc)	----	----
SNEFRU (4 passos)	128	48
SNEFRU (8 passos)	128	23
WHIRLPOOL (ISO/IEC 10118-3:2004)	512	----

Família SHA - Desenvolvida pelo NIST (FIPS PUB 180, 180-1 e 180-2)
RFC 3174 acrescenta código em linguagem C

Exercícios

Exercícios

(4) Utilize a biblioteca openssl para gerar o código hash md5 de uma mensagem

openssl dgst –md5 mensagem.txt

(5) Utilize a biblioteca openssl para gerar o código hash sha-1 de uma mensagem

openssl dgst –sha1 mensagem.txt

Exercícios

(6) Utilize a biblioteca openssl para criptografar o código hash md5 de uma mensagem utilizando criptografia assimétrica

openssl dgst –md5 –out mensagem.sign
–sign privkey.pem mensagem.txt

Referências Bibliográficas

Referências Bibliográficas

- **Criptografia e Segurança de Redes - Princípios e Práticas (4a. Edição)**
  - Willian Stallings, Pearson. 2008
- **APPLIED CRYPTOGRAPHY - PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C**
  - SCHNEIER, BRUCE, Editora: JOHN WILEY CONSUMER, Edição: 2ª, 1996
- **Sites Recomendados**
  - NIST Secure Hashing Page
  - http://www-cse.ucsd.edu/users/mihir