Funções Hash

Funçao Hash

- Uma **função hash** é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.

Função Hash

- O valor retornado por uma função hash são chamados **códigos hash**, simplesmente **hash**.

Hash

- Um **hash** é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada.

Hash

- O conceito teórico diz que "hash" é a transformação de uma grande quantidade de dados em uma pequena quantidade de informações".

Hash

- Uma função Hash aceita uma mensagem M de comprimento variável como entrada e produz uma saída de comprimento fixo conhecida por Hash de M, denotado por H(M).

Hash

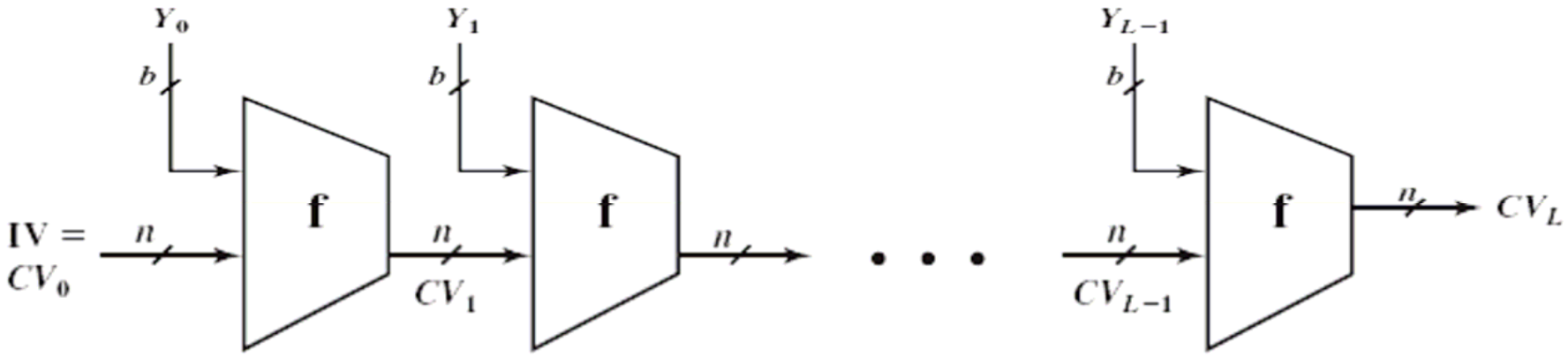
- É uma função apenas da mensagem M de entrada.

- Também chamado de:
  Resumo de Mensagem,
  Síntese de Mensagem,
  Message Digest (MD)

Hash

- É uma função de todos os bits da mensagem M.
- Tem a capacidade de detecção erros: uma mudança em qualquer bit ou bits na mensagem, resulta em uma mudança no Hash(M).
- Garante: Integridade

Estrutura do Código de Hash Seguro



IV = valor inicial
CV_i = Variável de encadeamento
Y_i = i-ésimo bloco de entrada
f = Função de compressão
L = Número de blocos de entrada
n = Comprimento do código de hash
b = Comprimento do bloco de entrada

Figura 11.9 Estrutura geral do código de hash seguro.

Função Hash

- O algoritmo de Hah envolve o uso repetido de uma função de compressão, f, que utiliza duas entradas:

  uma entrada de n bits da etapa anterior, chamada de “variável de encadeamento”,

  um bloco de b bits, proveniente de um arquivo de dados, partido em blocos.

Função Hash

- O valor final da “variável de encadeamento” é o valor da função Hash.
- Como normalmente b > n, daí o termo função de compressão.

Requisitos para uma função Hash

- H pode ser aplicada a um bloco de dados de qualquer tamanho.
- H produz uma saída de comprimento fixo.
- H(x) é relativamente fácil de ser calcular para qualquer x, tornando as implementações de hardware ou software práticas.

Requisitos para uma função Hash

- Para qualquer valor h dado, é computacionalmente inviável encontrar x tal que H(x)=h.

- “resistência à primeira inversão” ou “propriedade unidirecional”

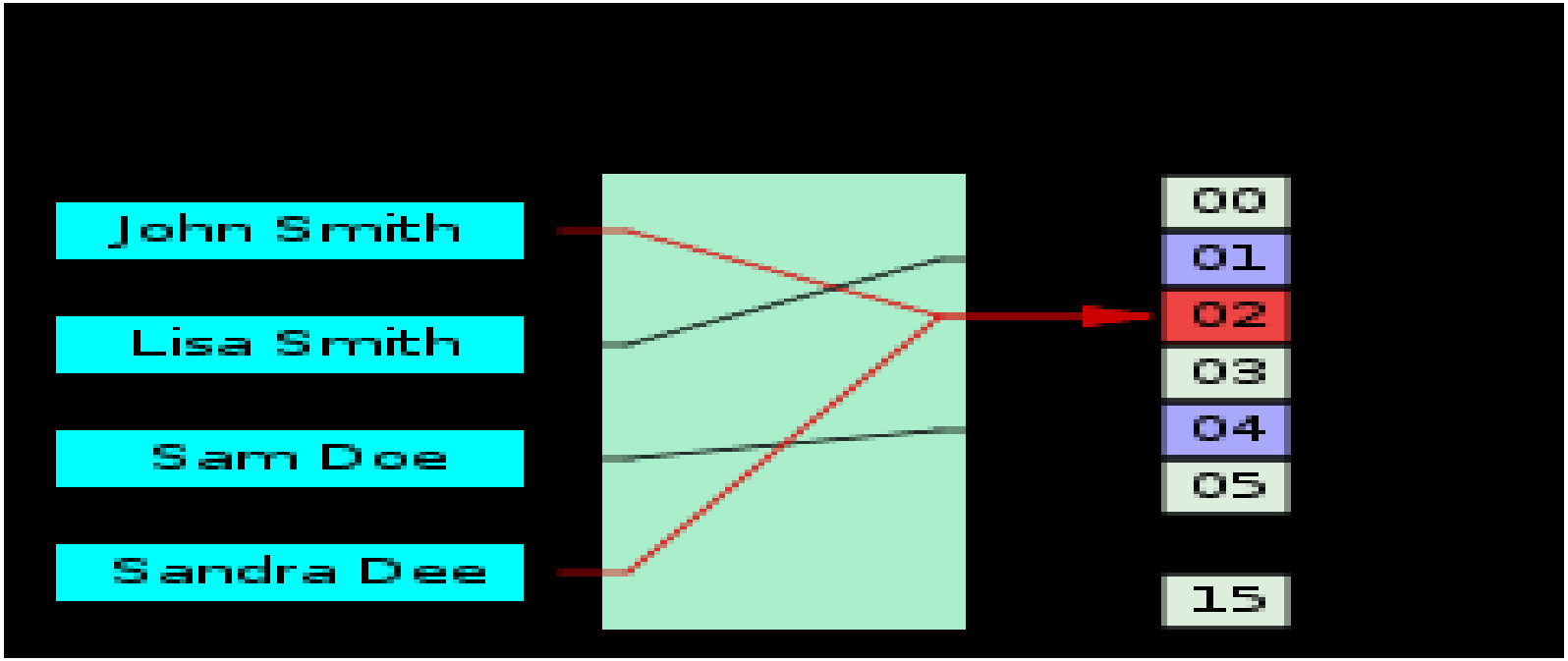
Requisitos para uma função Hash

- Para qualquer bloco de dados x, é computacionalmente inviável encontrar
  y diferente de x, tal que H(y) = H(x).

- Isto é conhecido como "resistência à segunda inversão" ou "resistência fraca à colisões".

Colisões

- Uma função hash que mapeia nomes para inteiros de 0 a 15.
- Existe um colisão entre a chaves "John Smith" e "Sandra Dee".



Requisitos para uma função Hash

- É computacionalmente inviável encontrar qualquer para (x, y) tal que H(x) = H(y) .
- Isto é conhecido como “resistência forte à colisões”.
- Resistência da função Hash a um tipo de ataque conhecido como o “ataque do aniversário”.

Ataque do Aniversário

- Uma função Hash de 64 bits é usada.
- Uma mensagem M, não criptografada, é enviada por um remetente A para um destinatário B.
- Um oponente intercepta M e o H(M).
- O oponente gera várias variações de M, substituindo várias pequenas partes, assim formando pares de texto sobre M., mas mantendo o mesmo significado de M.

Ataque do Aniversário

- O oponente precisa encontrar uma mensagem M´, adulterada, tal que:

  $$H(M') = H(M)$$

  para substituir M e enganar o receptor B.

- A probabilidade de sucesso é provado ser maior que 0,5.

- O oponente gera 2E(n/2) = 2E(64/2) =2E32 variações possíveis. Este é o esforço exigido, provado, para realizar uma ataque de força bruta num código de hash de tamanho n.

Ataque do Aniversário

- Se nenhuma combinação for encontrada, outras mensagens fraudulentas poderão ser geradas até que seja encontrada uma com o mesmo H(M).

- O oponente oferece a variação válida encontrada com o mesmo H(M), para o remetente A, para “assinatura”. Essa “assinatura” é anexada à variação fraudulenta para transmissão destinatário B.

Ataque do Aniversário

- B recebe M´ e H(M´) = H(M) e calcula o H(M´). Como H(M´) calculado é igual ao que B recebeu, B deduz que não houve alteração da mensagem, o que na realidade, é a mensagem M´ adulterada, e não a mensagem verdadeira M.

Ataque do Aniversário
Conclusão

- O tamanho do código de Hash, n bits, deve ser substancial.
- A força de uma função Hash contra ataque de força bruta deve ser proporcional ao tamanho do código de Hash produzido pelo algoritmo.

Força do Código Hash

- 64 bits é fraca.
- MD5 com 128 bits foi encontrada uma colisão em 24 dias.
- 160 bits levaria-se mais de 4000 anos para se encontrar uma colisão.
- Mesmo 160 bits é, atualmente considerado fraco.

Força do Código Hash

- Para um código Hash de tamanho de n bits, o nível de esforço exigido, para força bruta, é dado por:

- Resistência à primeira inversão: 2E(n)
- Resistência fraca à colisões: 2E(n)
- Resistência forte à colisões: 2E(n/2)

Funções Hash bem conhecidas

- MD2, MD4, MD5 (resumem 128 bits)
- SHA-1 (Standard Hash Algorithm-1) (resume 128 bits)
- SHA-2 (Standard Hash Algorithm-2) (resume 256, 384, 512 bits)
- RIPEMD
- PANAMA
- TIGER

RIPEMD-160

- **RIPEMD-160** é um algoritmo de hash de 160 bits idealizado por Hans Dobbertin, Antoon Bosselaers, e Bart Preneel.

- É usado como uma substituição segura das chaves de 128 bits MD4, MD5 e RIPEMD.

- http://pt.wikipedia.org/wiki/RIPEMD-160

Snefru (1990)

- 128 e 256 bits de saída
- http://en.wikipedia.org/wiki/Snefru

Haval (1992)

- 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits.
- http://en.wikipedia.org/wiki/HAVAL

GOST (1994)

- Função criptográfica de Hash de 256-bit.

- http://en.wikipedia.org/wiki/Gost-Hash

Tiger (1995)

- 192 bits.
- http://en.wikipedia.org/wiki/Tiger_(hash)

PANAMA (1998)

- 256 bits
- Cifra de Fluxo
- http://en.wikipedia.org/wiki/Panama_(cryptography)

SHA-2 (2001)

- **SHA-224, SHA-256, SHA-384, SHA-512,**
- Projetado por U.S. National Security Agency (NSA) and publicado em 2001 pelo the NIST como um U.S. Federal Information Processing Standard (FIPS).
- SHA significa Secure Hash Algorithm.
- SHA-2 includes a significant number of changes from its predecessor, SHA-1.
- http://en.wikipedia.org/wiki/SHA-256

Whirlpool (2000 à 2004)

- **Whirlpool** (às vezes referenciado como *WHIRLPOOL*) é uma função criptográfica de hashdesenvolvida pelo prof. Vincent Rijmen (belga) e o Prof. Paulo S. L. M. Barreto (brasileiro).

- A função foi recomendada pelo projeto *New European Schemes for Signatures, Integrity and Encryption* (NESSIE) (Europeu).

- Foi também adotada pela Organização Internacional para Padronização(ISO) e pela Comissão Eletrotécnica Internacional (IEC) como parte do padrão internacional ISO 10118-3.

Whirlpool (2005)

- Vicent Rijmen (co-autor do algoritmo Rijndael, também conhecido como AES)[1] e Paulo Barreto (pesquisador brasileiro)[2] criaram três versões do WHIRLPOOL.

- Os autores declararam que esse algoritmo "não é, e nunca será, patenteado e deve ser usado livre de custos para qualquer propósito. As referências para implementações estão em domínio público."

- Os primeiros programas de criptografia a usarem o Whirlpool foram FreeOTFE e TrueCrypt em 2005.

Calculadores Hash

- HashCalc
  http://www.slavasoft.com/hashcalc/index.htm

- ADLER 32 HASH CALCULATOR

http://www.md5calc.com/adler32