Tópicos Avançados em Computação I

Criptografia

- Funções de Hash Criptográficas

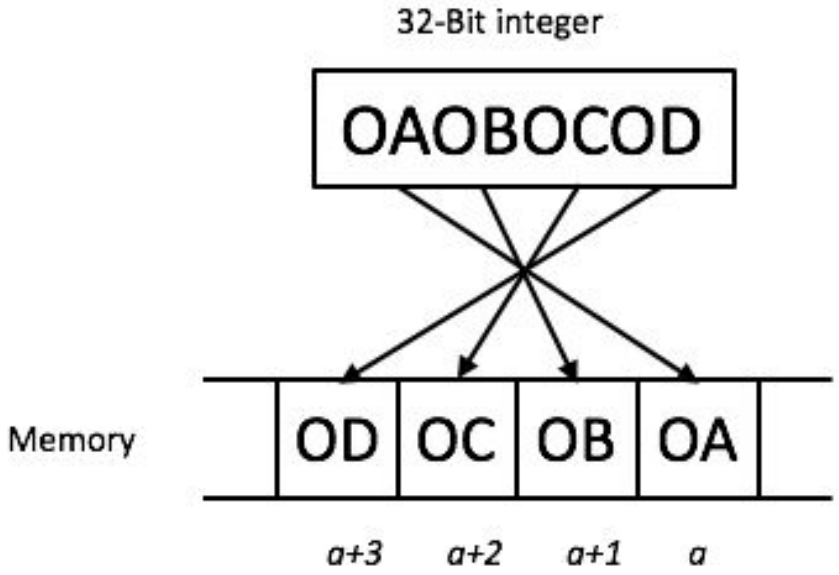
Dúvidas? *(aula anterior)*

Exercícios Anteriores *(entrega)*

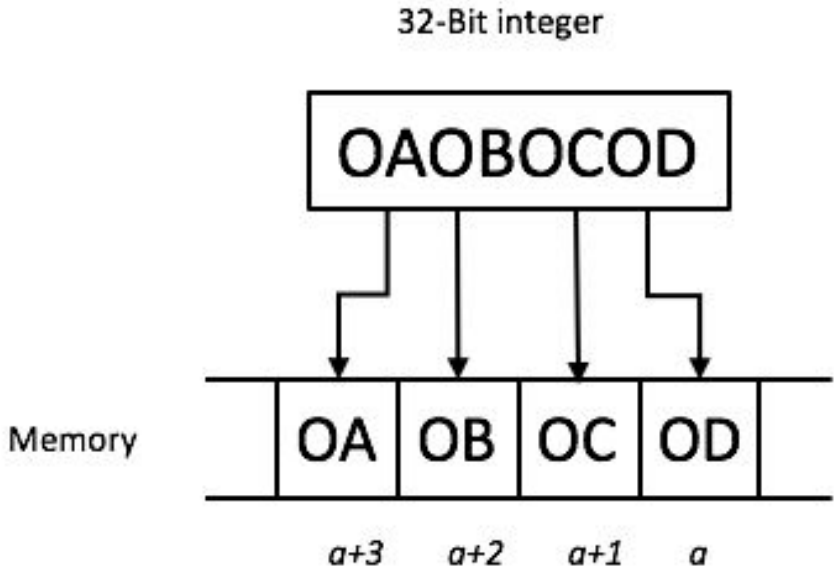
“DES simplificado”.

Dúvidas? *(exercício - aula anterior)*

Little-endian e Big-endian



Big Endian

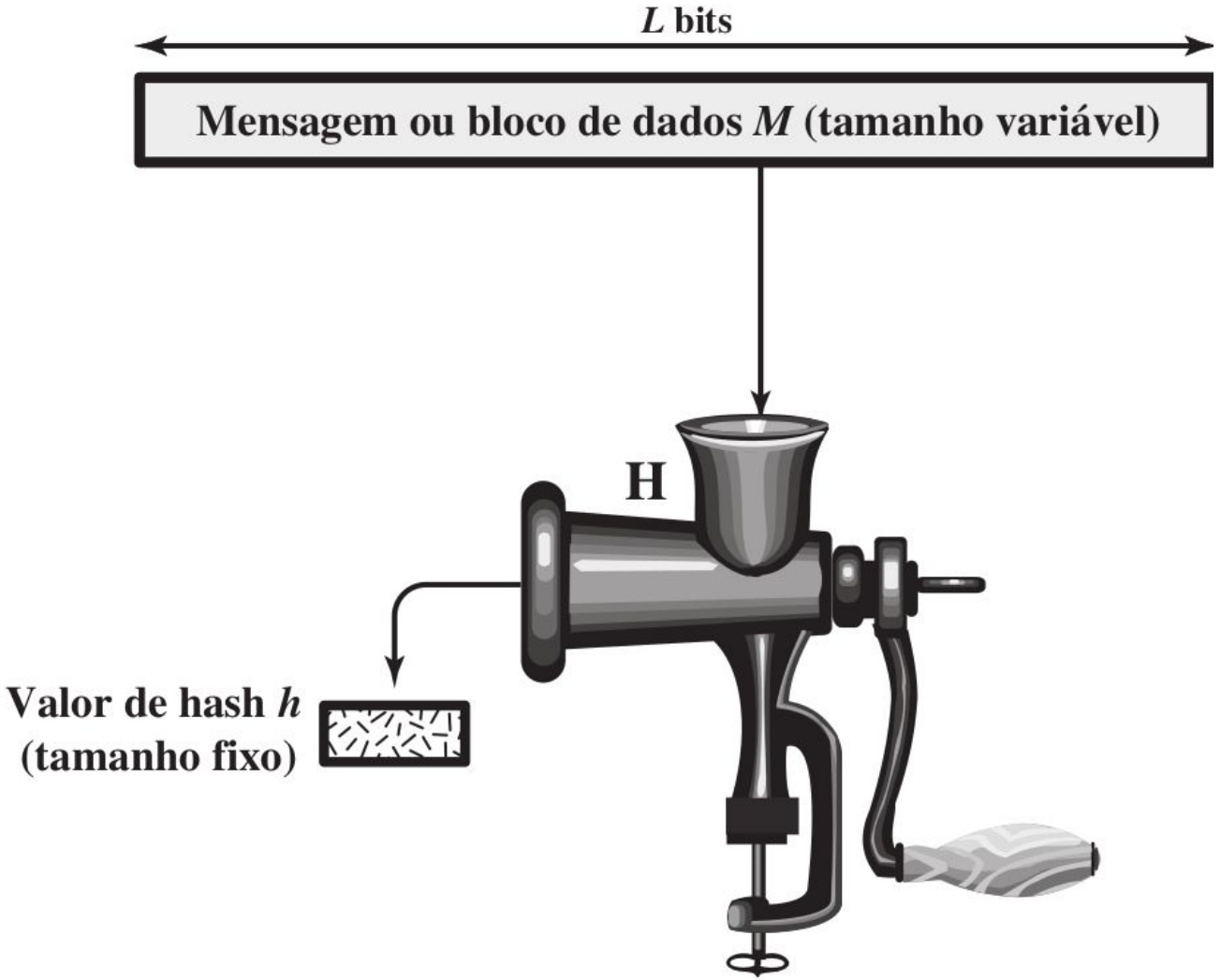


Little Endian

Funções de Hash Criptográficas

- Uma função de hash aceita uma mensagem de tamanho variável x como entrada e produz um valor de hash de tamanho fixo $y = H(x)$.

Funções de Hash Criptográficas



Formalização

Para ser considerada uma função de hash, uma função $y=E(x)$ deve satisfazer as seguintes propriedades:

- x é de comprimento variável, relativamente longo;
- y é de comprimento fixo, relativamente curto;
- dado x, $E(x)$ é fácil de ser calculada.

Propriedades

- Uma “boa” função de hash tem a propriedade de que os resultados da aplicação da função a um grande conjunto de entradas produzirá saídas que são distribuídas por igual e aparentemente de modo aleatório.
- Em termos gerais, o objeto principal de uma função de hash é a integridade de dados.
- Uma mudança em qualquer bit ou bits em x resulta, com alta probabilidade, em uma mudança no código de hash.

Formalização *(Cont.)*

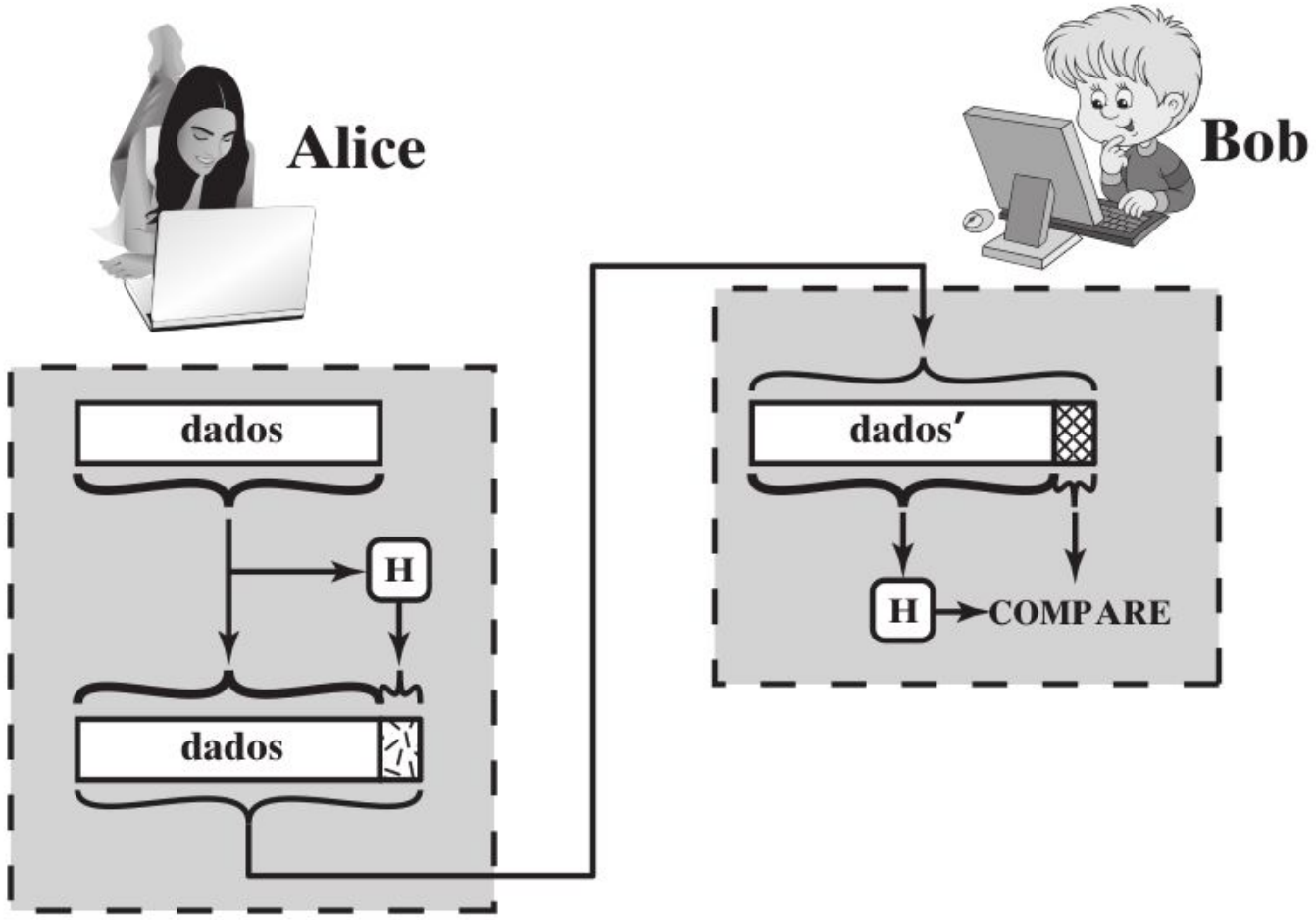
Além disso, tecnicamente, uma função de hash precisa apresentar três propriedades para ser considerada segura, e consequentemente se enquadrar como uma função de hash criptográfica. Essas propriedades são:

- **Resistência à pré-imagem**: é computacionalmente inviável ***reverter*** a função hash (ou seja, encontrar a entrada a partir de uma determinada saída).
- **Resistência à colisão**: é computacionalmente inviável ***encontrar duas entradas quaisquer*** que sejam distintas e produzam um mesmo hash como saída.
- **Resistência à segunda pré-imagem**: para uma entrada específica, é computacionalmente inviável **encontrar uma segunda entrada** que produza um mesmo hash de saída.

Aplicações

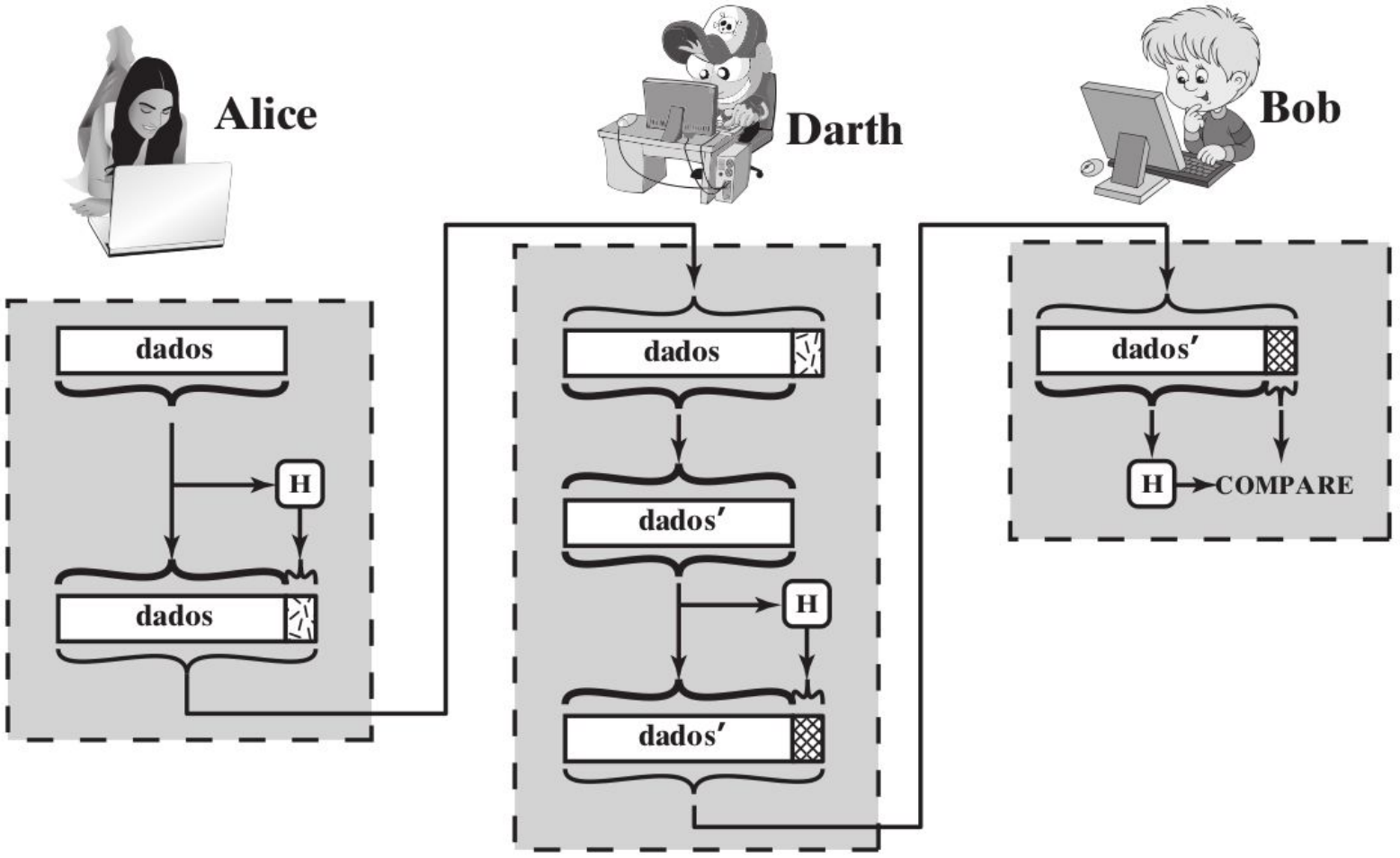
- Autenticação de mensagem
- Assinaturas digitais
- Detecção de intrusão
- Detecção de vírus
- Função pseudoaleatória (PRF)
- Gerador de número pseudoaleatório (PRNG)
- Arquivo de senha de mão única*
- …

Aplicações *(Autenticação de mensagem)*



(a) Uso da função de hash para verificar integridade de dados

Aplicações *(Autenticação de mensagem)*



(b) Ataque *man-in-the-middle*

Requisitos

Requisito	Descrição
Tamanho de entrada variável	H pode ser aplicado em um bloco de dados de qualquer tamanho.
Tamanho da saída fixo	H produz uma saída de tamanho fixo.
Eficiência	$H(x)$ é relativamente fácil de calcular para qualquer valor de x informado, através de implementações tanto em hardware quanto em software.
Resistência à pré-imagem (propriedade de mão única)	Para qualquer valor de hash h informado, é computacionalmente impossível encontrar y, de modo que $H(y) = h$.
Resistência à segunda pré-imagem (resistência à colisão fraca)	Para qualquer bloco x informado, é computacionalmente impossível encontrar $y \neq x$ com $H(y) = H(x)$.
Resistência à colisão forte	É computacionalmente impossível encontrar qualquer par (x, y), de modo que $H(x) = H(y)$.
Pseudoaleatoriedade	A saída de H atende os testes padrão de pseudoaleatoriedade.

“Novas variações”

- Funções de derivação de chaves
- Esquemas de hash de senhas
- Construção em esponja
- ...

Exercício

- Quantas variações a carta ao lado possui?

As { the / — } Dean of Blakewell College, I have { had the pleasure of knowing / known } Cherise Rosetti for the { last / past } four years. She { has been / was } { a tremendous / an outstanding } { asset to / role model in } { our / the } school. I { would like to take this opportunity to / wholeheartedly } recommend Cherise for your { school's / — } graduate program. I { am / feel } { confident / certain } { that / — } { she / Cherise } will { continue to / — } succeed in her studies. { She / Cherise } is a dedicated student and { thus far her grades / her grades thus far } { have been / are } { exemplary / excellent }. In class, { she / Cherise } { has proven to be / has been } a take-charge { person / individual } { who is / — } able to successfully develop plans and implement them.

{ She / Cherise } has also assisted { us / — } in our admissions office. { She / Cherise } has { successfully / — } demonstrated leadership ability by counseling new and prospective students. { Her / Cherise's } advice has been { a great / of considerable } help to these students, many of whom have { taken time to share / shared } their comments with me regarding her pleasant and { encouraging / reassuring } attitude. { For these reasons / It is for these reasons that } I { highly recommend / offer high recommendations for } Cherise { without reservation / unreservedly }. Her { ambition / drive } and { abilities / potential } will { truly / surely } be an { asset to / plus for } your { establishment / school }.

Exercícios

- Que características são necessárias em uma função de hash segura?
- Qual é a diferença entre resistência à colisão e resistência à segunda pré-imagem?
- Qual é a diferença entre os formatos little-endian e big-endian?
- Quais funções aritméticas e lógicas básicas podem ser utilizadas em uma função de hash?
- Descreva rapidamente a estrutura interna de uma função de iteração de uma função de hash.

Exemplo básico

Uma das funções de hash mais simples é o OR exclusivo (XOR) bit a bit de cada bloco. Isso pode ser expresso da seguinte forma:

$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im}$$

onde

$C_i = i$-ésimo bit do código de hash, $1 \leq i \leq$ n

$m =$ número de blocos de n bits na entrada

$b_{ij} = i$-ésimo bit no j-ésimo bloco

$\oplus =$ operação XOR

Exercício de Programação 01

- Especifique o restante dos passos, junte com a função de iteração descrita anteriormente, e implemente sua função de hash utilizando uma linguagem de programação de alto nível.

Obrigado!

ewerton.andrade@unir.br
http://ewerton.andrade.pro.br/