Funções de Hash Criptográficas ou one-way hash functions

1.

- Blocos construtores básicos usados em Criptografia
- Também conhecidos como "Message Digest" ou "Manipulation Detection Codes (MDC)"
- Propriedades "one-way" e resistência a colisões
- Utilização:
  - autenticação de passwords
  - preservação de integridade
  - Blockchain
- Ataques possíveis:
  - Length extension attack
  - Collision attack

Características das one-way hash function

≠ hash function

↓

Mapeiam dados arbitrários em dados de dimensão fixa

ex: $f(m) = m \mod 1000$

↓

pode ser qualquer nº

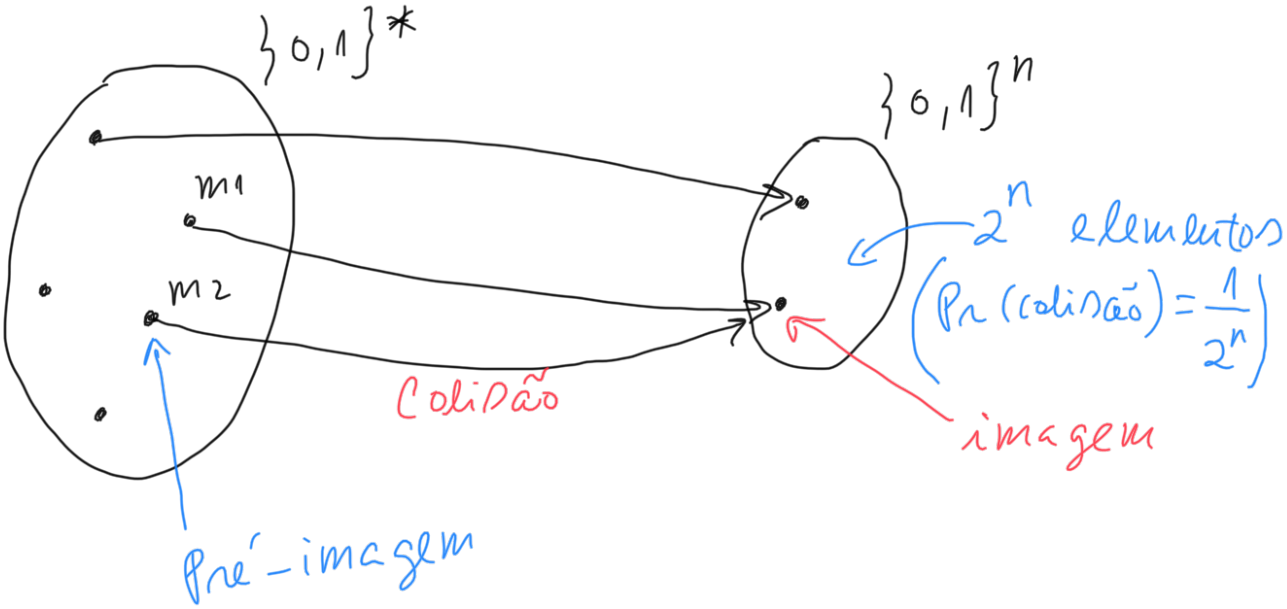
- Funções hash one-way - Propriedades:

- É computacionalmente fácil obter hash(m) dado m
- É computacionalmente difícil, dado hash(m) = h, obter m (one-way property)
- É computacionalmente difícil, dado m, obter $m' \neq m$ tal que hash(m') = hash(m) (propriedade segunda pré-imagem)

- Resistência a colisões

É computacionalmente difícil obter m_1 e m_2 tal que $hash(m_1) = hash(m_2)$

Função hash: $\{0,1\}^* \longrightarrow \{0,1\}^n$



Função $f(m) = m \bmod 1000$ é one-way?

Propriedade one-way + segunda pré-imagem:

dado o hash h é fácil obter nºs que produzem esse hash, ex: $1000 + h$, $2000 + h$, ...

Prova:

$f(m) = m \bmod 1000$

$f(m_1) = m_1 \bmod 1000 = (h)$ → público

$f(m_2 = h + 1000) = m_2 \bmod 1000$

$= (h + 1000) \bmod 1000$

$= h$ //

Propriedade resistência a colisões:

É possível encontrar dois nºs, ex: 1005 e 2005, que produzem o mesmo hash.

∴ $f(m)$ não é one-way hash function.

Funções de hash one-way (ou criptográficas) típicas:

↳ Série MD (Message Digest) de Ron Rivest

↳ Série SHA (Secure Hash Algorithm) publicado por NIST (National Institute of Standards and Technology)

MD inclui:

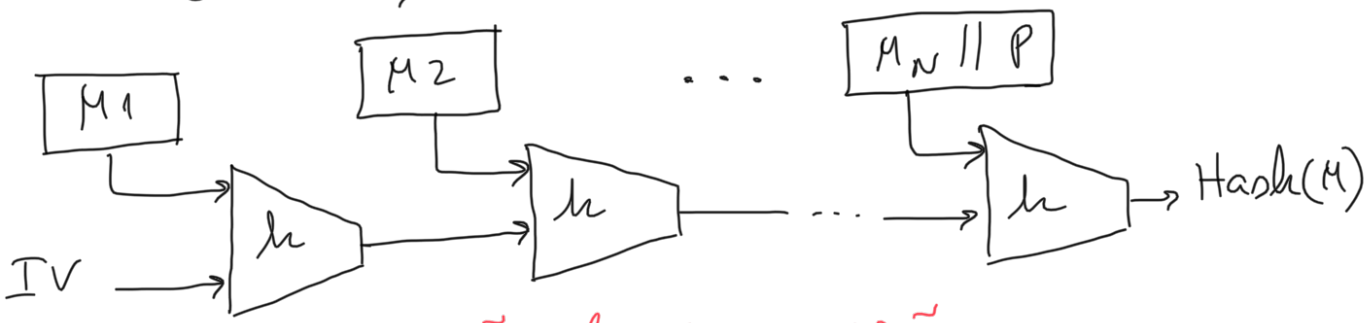
- MD2, MD4 → frágeis (obsoletos)
- MD5 → Propriedade resistência a colisões quebrada; propriedade one-way intacta
- MD6 → desenvolvida em resposta a proposta do NIST

SHA inclui:

- SHA-0: frágil (obsoleto)
- SHA-1: desenhado pela NSA (National Security Agency); collision attack encontrado em 2017
- SHA-2: NSA; SHA-256 e SHA-512 (sem ataques conhecidos)
- SHA-3 (2015): tem estrutura interna diferente dos antecessores, sendo usado como alternativa se houver ataque a SHA-2

Estrutura interna das funções de Hash MD5, SHA-1 e SHA-2

↳ Construção de Merkle-Damgard



h: função de compressão

P: padding

$\|$: concatenação

- Comandos em Linux e OpenSSL
  ↳ slides

- verificação de integridade
  ↳ slide 20 de 02-Esquemas.pdf

MAC (Message Authentication Code) revisitado

↳ usar one-way hash como tag funciona?

↳ Não, porque MITM pode recalcular o hash

↳ é necessário cifrar o hash com uma chave secreta partilhada entre emissor e recetor
↳ MITM não pode calcular hash sem saber a chave

Keyed-Hash MAC (HMAC), Krawczyk et al., 1997

↳ ver slide 5