# UNIVERSIDADE POSITIVO

CRIPTOGRAFIA E SEGURANÇA DE COMPUTADORES

Prof Escobar

# SHA-256: Um Algoritmo de Hash Seguro e sua Lógica de Funcionamento

SHA-256 (Secure Hash Algorithm 256 bits) é um algoritmo de hash criptográfico pertencente à família SHA-2, desenvolvida pela NSA (National Security Agency) e padronizada pelo NIST (National Institute of Standards and Technology). Ele gera um resumo de 256 bits (32 bytes) a partir de uma entrada de qualquer tamanho, proporcionando um valor fixo e único para cada entrada distinta.

**Utilização do SHA-256**

SHA-256 é amplamente utilizado em diversas aplicações de segurança, incluindo:

- Assinaturas digitais e certificação: Utilizado para garantir a integridade e autenticidade de documentos digitais.

- Blockchain e criptomoedas: Base do mecanismo de hashing do Bitcoin e outras criptomoedas para validação de transações

- Armazenamento seguro de senhas: Senhas podem ser armazenadas em bancos de dados em formato hash para maior segurança.

- Verificação de integridade de arquivos: Garante que um arquivo não foi alterado ao longo do tempo.

**Lógica do SHA-256**

**SHA-256 segue um processo matemático estruturado em diversas etapas**

1. **Preparação da Mensagem**

Antes do processamento, a mensagem de entrada passa por um padding (preenchimento) para garantir que seu tamanho seja um múltiplo de 512 bits:

- O bit `1` é adicionado ao final da mensagem.

- Bits `0` são adicionados até que o comprimento seja 448 bits módulo 512.

- Os últimos 64 bits armazenam o tamanho original da mensagem em bits.

**2. Inicialização dos Registradores**

SHA-256 utiliza oito registradores de 32 bits, inicializados com constantes derivadas das frações decimais das raízes quadradas dos primeiros oito números primos.

H0 = 0x6a09e667

H1 = 0xbb67ae85

H2 = 0x3c6ef372

H3 = 0xa54ff53a

H4 = 0x510e527f

H5 = 0x9b05688c

H6 = 0x1f83d9ab

H7 = 0x5be0cd19

**3. Expansão da Mensagem**

A mensagem é dividida em blocos de 512 bits e processada em partes de 32 bits, expandidas para 64 palavras de 32 bits.

W[i] = σ\_1(W[i-2]) + W[i-7] + σ\_0(W[i-15]) + W[i-16]

Onde:

σ\_0(x) = (x ROTR 7) ⊕ (x ROTR 18) ⊕ (x >> 3)

σ\_1(x) = (x ROTR 17) ⊕ (x ROTR 19) ⊕ (x >> 10)

**4. Processo de Compressão**

Cada bloco de 512 bits é processado por 64 rodadas utilizando 64 constantes derivadas das frações decimais das raízes cúbicas dos primeiros 64 números primos. O algoritmo aplica funções de mistura bitwise e operações lógicas.

Para cada rodada, são computadas duas funções principais:

Ch(x,y,z) = (x ∧ y) ⊕ (¬x ∧ z)

Maj(x,y,z) = (x ∧ y) ⊕ (x ∧ z) ⊕ (y ∧ z)

E duas operações de mistura:

Σ\_1(x) = (x ROTR 6) ⊕ (x ROTR 11) ⊕ (x ROTR 25)

As variáveis intermediárias a, b, c, d, e, f, g, h são atualizadas a cada rodada:

T1 = h + Σ\_1(e) + Ch(e,f,g) + K[i] + W[i]

T2 = Σ\_0(a) + Maj(a,b,c)

h = g

g = f

f = e

e = d + T1

d = c

c = b

b = a

a = T1 + T2

**5. Atualização dos Registradores**

Os valores intermediários são somados aos registradores originais para gerar o hash final.

H0 = H0 + a

H1 = H1 + b

H2 = H2 + c

H3 = H3 + d

H4 = H4 + e

H5 = H5 + f

H6 = H6 + g

H7 = H7 + h

**6. Geração do Hash Final**

A concatenação dos valores finais H0 || H1 || H2 || H3 || H4 || H5 || H6 || H7 resulta no hash de 256 bits.

**Atividade Prática**

Implemente o algoritmo SHA-256

Utilize o material disponibilizado, faça pesquisas e procure por mais explicações

Para verificar o funcionamento do SHA-256 acesse <https://sha256algorithm.com/>