



**FUNDAMENTOS DE
SEGURANÇA DA
INFORMAÇÃO**

Aline Zanin

Segurança em Sistemas Computacionais

Funções de hash e suas aplicações

Equipe: Lívia Faria - Lucas Faria - Wesley Júnior

Conteúdos

- O que são funções de hash?
- Características das funções de hash.
- Aplicações em integridade de dados.
- Aplicações em assinaturas digitais.
- Exemplos e conclusão.





O que são funções de hash?

Uma função de hash é um algoritmo que transforma uma entrada (ou mensagem) em uma sequência fixa de caracteres, geralmente representada como uma string hexadecimal. A saída, chamada de valor de hash ou código de hash, tem um tamanho fixo, independentemente do tamanho da entrada.

Exemplo de função de hash: SHA256 (Secure Hash Algorithm 256-bit).



Características das funções de hash

Determinística

A mesma entrada gera o mesmo hash.

Rápida de Calcular

Deve ser eficiente.

Resistência a Colisões

Difícil encontrar duas entradas com o mesmo hash.

Resistência à Pré-imagem

Difícil encontrar a entrada a partir do hash.

Resistência à Segunda Pré-imagem

Difícil encontrar uma entrada diferente com o mesmo hash.

Aplicações em Integridade de Dados

As funções de hash são amplamente usadas para garantir a integridade dos dados. Isso significa garantir que os dados não foram alterados, corrompidos ou manipulados durante o armazenamento ou a transmissão.

COMO FUNCIONA?

- **Geração do Hash:** quando os dados são criados ou recebidos, uma função de hash é aplicada para gerar um valor de hash.
- **Armazenamento/Transmissão:** o valor de hash gerado é armazenado ou transmitido junto com os dados.
- **Verificação:** quando os dados são recuperados ou recebidos, a função de hash é aplicada novamente. O valor de hash gerado é comparado ao valor de hash original. Se os dois valores corresponderem, os dados não foram alterados. Caso contrário, pode haver corrupção ou manipulação.

Exemplo de Integridade de Dados

Cenário: Transmissão de um arquivo.

- **Envio:** gerar o hash do arquivo e enviá-lo junto com o arquivo.
- **Recepção:** recalcular o hash do arquivo recebido e comparar com o hash enviado.

Aplicações em Assinaturas Digitais

As assinaturas digitais utilizam funções de hash em conjunto com criptografia para garantir a autenticidade e integridade dos dados.

COMO FUNCIONA?

- **Criação da Assinatura:** o remetente cria uma assinatura digital da mensagem. Primeiro, a função de hash é aplicada à mensagem para gerar um valor de hash. Em seguida, o valor de hash é criptografado usando a chave privada do remetente, criando a assinatura digital.
- **Envio da Mensagem:** a mensagem e a assinatura digital são enviadas ao destinatário.
- **Verificação da Assinatura:** o destinatário aplica a mesma função de hash à mensagem recebida para gerar um valor de hash. Em seguida, usa a chave pública do remetente para descriptografar a assinatura digital e obter o valor de hash original. Se o valor de hash gerado corresponde ao valor de hash descriptografado, a assinatura é válida, confirmando a autenticidade e integridade da mensagem.

Exemplo de Assinatura Digital

Cenário: Assinatura de um documento.

- **Gerar Hash:** aplicar SHA256 ao documento.
- **Criptografar:** criptografar o hash com a chave privada.
- **Verificar:** descriptografar o hash com a chave pública e comparar com o hash recalculado.

Conclusão

As funções de hash, como o SHA256, são fundamentais para garantir a integridade dos dados ao transformar entradas em valores fixos e únicos. Elas são amplamente utilizadas para verificar se os dados foram alterados e para criar assinaturas digitais que asseguram tanto a autenticidade quanto a integridade das informações. Essas funções desempenham um papel crucial na proteção contra alterações não autorizadas e na confirmação da identidade do remetente, reforçando a segurança em sistemas computacionais.

