Criptografia

Código de Autenticação de Mensagem - MAC

Roadmap

- Definição
- Estrutura de um MAC
- HMAC

Universidade Federal do Ceará
Campus de Crateús

Ciência da Computação
Sistemas de Informação

emerson@crateus.ufc.br

Código de Autenticação de Mensagem

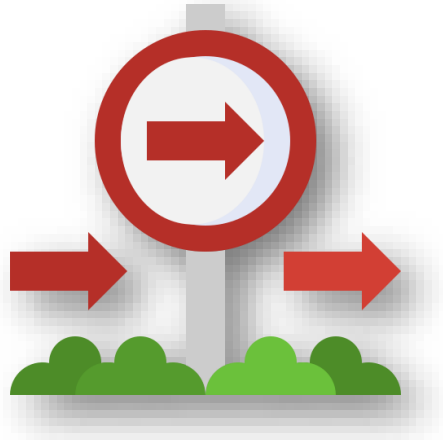
Definição

- As funções hash criptográficas são utilizadas para verificar a integridade de mensagens.
- Porém, em algumas situações, não só a **integridade** da mensagem que precisa ser verificada, mas também sua **autenticidade**.

Autenticação de mensagem *é um procedimento para verificar se a mensagem recebida provêm realmente da origem afirmada e se não foi alterada. Isso significa que o processo de autenticação garante também a integridade da mensagem.*

Código de Autenticação de Mensagem

Definição



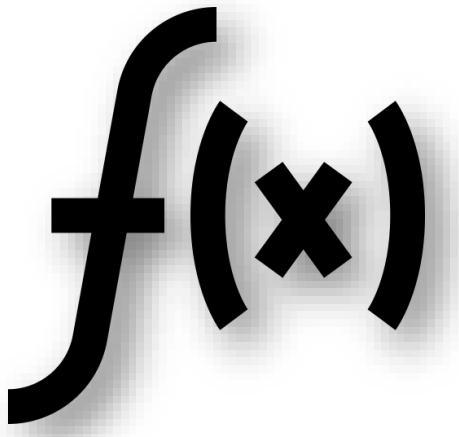
- Para autenticar uma mensagem, utiliza-se um tipo de função chamada ***Message Authentication Code*** (**MAC**)— Código de Autenticação de Mensagem.

- Essa função tem o propósito de garantir **autenticação da origem dos dados**

- **MAC** pode ser entendido como uma técnica de **autenticação** que envolve o uso de uma **mensagem** e uma **chave secreta**, para gerar um pequeno bloco de dados de **tamanho fixo**, que é transmitido juntamente com a mensagem.

Código de Autenticação de Mensagem

Definição



- Formalmente, MAC é uma função

$$\boldsymbol{MAC}: \{\mathbf{0},\mathbf{1}\}^{*} \times \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{s}} \rightarrow \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}},$$

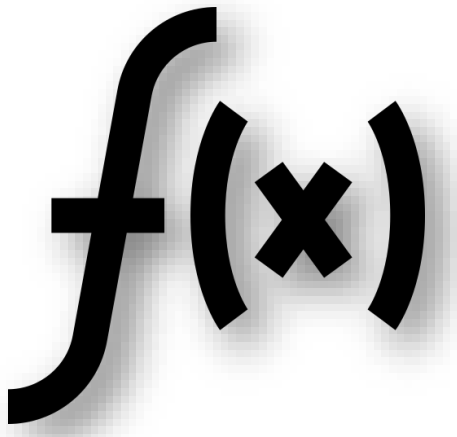
- que mapeia uma mensagem $\boldsymbol{m} \in \{\mathbf{0},\mathbf{1}\}^{*}$ de comprimento arbitrário e uma chave secreta $\boldsymbol{k} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{s}}$ em uma saída de comprimento fixo $\boldsymbol{t} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ semelhante a um valor hash.

- Tal função pode ser denotada por

$$\boldsymbol{MAC_s(m) = t}$$

Código de Autenticação de Mensagem

Estrutura de um MAC



- Um MAC baseado em **funções hash** pode ser descrito genericamente da seguinte forma:

1. Uma mensagem $\boldsymbol{m}$ de qualquer tamanho é utilizada como entrada para uma função hash $\mathcal{H}$,
2. Além da mensagem $\boldsymbol{m}$, uma chave secreta $\boldsymbol{k}$ também é utilizada para compor a entrada da função.
3. A função hash será aplicada à mensagem $\boldsymbol{m}$ juntamente com a chave secreta $\boldsymbol{k}$, esse processo resultará em uma *string*

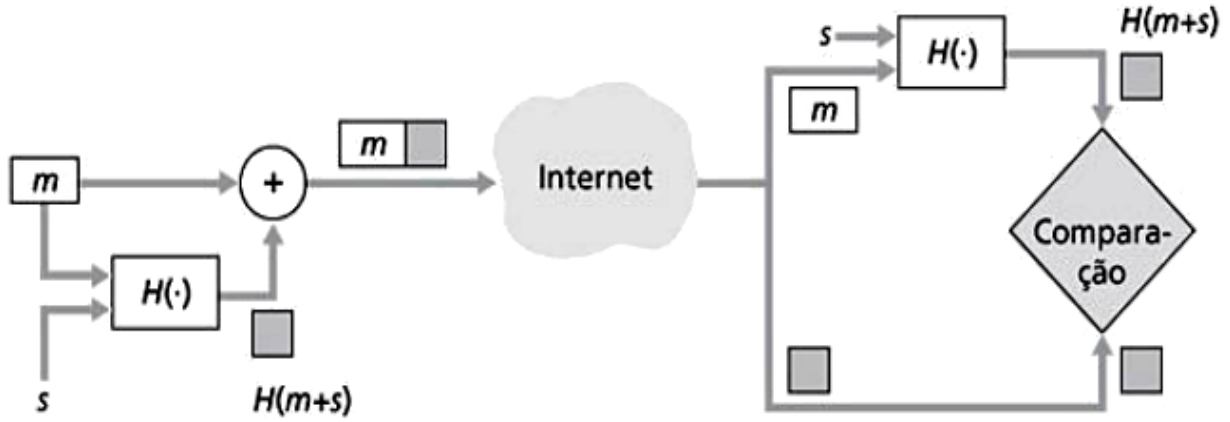
$$\boldsymbol{MAC_s(m) = t.}$$

4. A valor MAC será enviado juntamente com a mensagem.

Código de Autenticação de Mensagem

Estrutura de um MAC

- A função hash $\mathcal{H}$ recebe como entrada a mensagem e a chave secreta ($\boldsymbol{m} + \boldsymbol{s}$), em que o sinal de " + " representa uma operação de **concatenação**.



Código de Autenticação de Mensagem

Estrutura de um MAC

- Para que o destinatário **autentique** a mensagem recebida, basta aplicar a mesma função hash $\mathcal{H}$ à mensagem juntamente com a chave secreta s.
- Se a etiqueta hash obtida for exatamente a mesma recebida significa que a mensagem está intacta e a autoria da mensagem também está comprovada.
- Uma vez que apenas o **legítimo remetente** conhecia a chave secreta.

Código de Autenticação de Mensagem

Estrutura de um MAC

- A chave secreta precisa ser previamente compartilhada com o destinatário da mensagem.
- A diferença da valor **MAC** para a valor *hash* fica por conta de que o *hash* pode ser obtida simplesmente aplicando a mesma função hash à mensagem.
- Enquanto que para obter o valor MAC é necessário a **mensagem original** e a **chave secreta**.
- Sendo assim, aplicando-se a função somente à mensagem resultará em um valor hash totalmente diferente.

Código de Autenticação de Mensagem

Construção de MAC baseado em função hash – HMAC

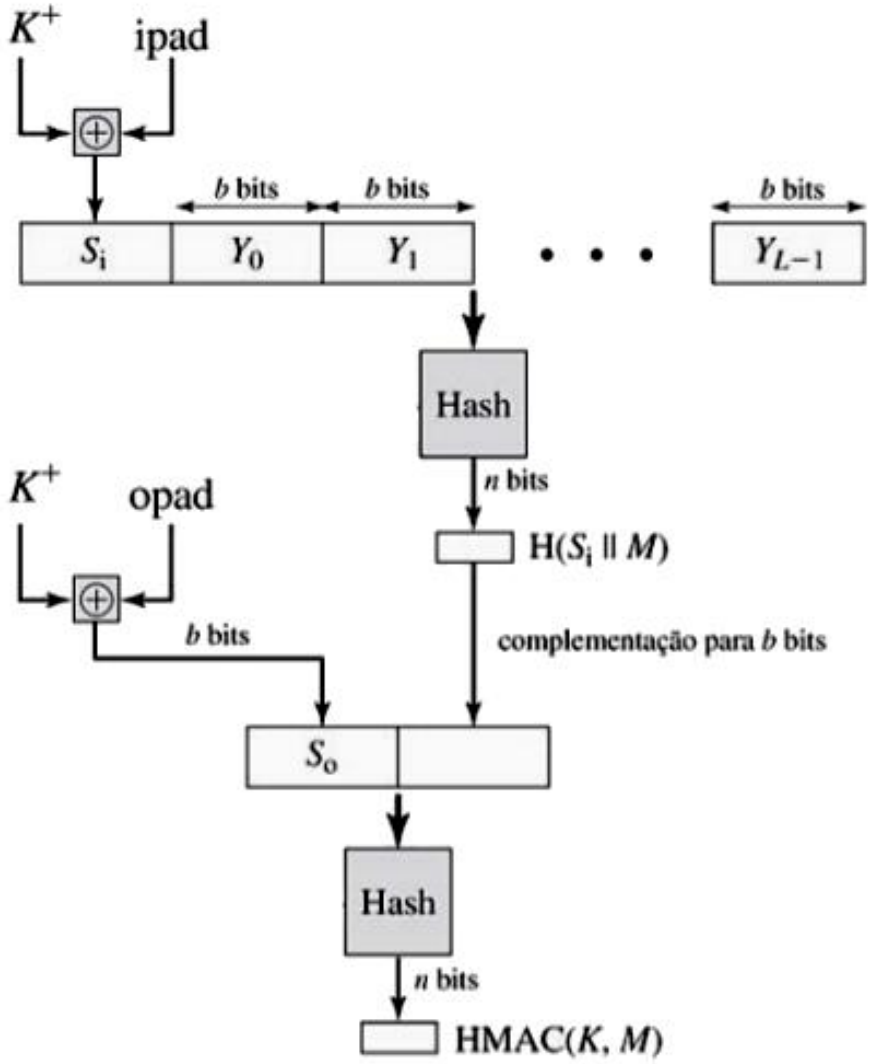
- ***O algoritmo HMAC é um esquema de autenticação de mensagens construído a partir de funções hash criptográficas.***
  - Uma função de hash segura pode ser utilizada como núcleo do algoritmo de MAC.
  - Portanto, **HMAC** pode ser usado com qualquer função de hash criptográfica iterativa em combinação com uma chave secreta compartilhada.

Construção de MAC baseado em função hash – HMAC

- A construção do HMAC tem os seguintes objetivos:

1. Usar, sem modificações, as funções de hash disponíveis.
2. Preservar a performance original da função hash sem incorrer em uma degradação significativa.
3. Permitir facilmente a substituição da função hash embutida, caso sejam encontrada funções de hash mais rápidas ou mais seguras.

Construção de MAC baseado em função hash – HMAC



M	Mensagem a ser autenticada
H	Função hash criptográfica
K	Chave secreta
K^+	Sequencia de bits formada pela chave K acrescentada de zeros à direita
$\|\|$	Denota concatenação
$\oplus$	Denota ou exclusivo (XOR)
b	Tamanho do bloco da função de compressão
$ipad$	Constante 00110110 (36 em hexadecimal) repetido $b/8$ vezes
$opad$	Constante 01011100 (5C em hexadecimal) repetido $b/8$ vezes
S_i	Bloco formando por K^+ XOR $ipad$
Y_i	i-ésimo bloco de M

$$HMAC(K,M) = H((K \oplus opad) \| H((K \oplus ipad) \| M))$$

Construção de MAC baseado em função hash – HMAC

- Uma função hash iterativa **quebra** uma mensagem em **blocos de tamanho fixo** e utiliza cada um desses blocos como entrada para a função de compressão.
  - O tamanho do bloco, b bits, varia de acordo com a função de compressão utilizada.
- A chave K será preenchida com zeros extras à direita até atingir o tamanho do bloco b, ou será usando o hash da chave original se esta for maior que o tamanho do bloco.

Código de Autenticação de Mensagem

Segurança do HMAC

- A segurança do HMAC está diretamente relacionada com a **segurança da função hash** usada internamente.
- Um algoritmo de MAC utiliza a função hash como uma **caixa preta**, não há necessidade de modificar o código da função para implementar a algoritmo de MAC.
- Se o HMAC falhar como um MAC seguro, é porque há fraqueza suficiente na função hash embutida que precisa ser descartada.

Código de Autenticação de Mensagem

Segurança do HMAC

- O **ataque do aniversário**, que é a base para encontrar colisões em funções hash criptográficas, pode ser aplicado para atacar também o esquemas HMAC.
- Porém, encontrar colisões pelo ataque do aniversário no HMAC é mais difícil que encontrar colisões em uma função hash.
- Em uma função hash o atacante pode gerar $\mathbf{2}^{n/2}$ operações e armazenar as mensagens testadas juntamente com as respectivas etiquetas hash encontradas.
- No HMAC, o atacante não pode simplesmente gerar pares de **mensagem/MAC**, já que ele não conhece a chave K.

Segurança do HMAC

- Sendo assim, para que o MAC seja considerado seguro, basta que a função hash tenha as propriedades de segurança necessárias, principalmente que seja livre de colisão.
- Portanto, a única maneira do HMAC falhar é se a função hash utilizada internamente falhar.

Fim!

[Aula 15] Código de Autenticação de Mensagem