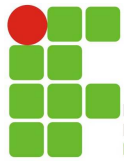
Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 07
Função Hash

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"O futuro dependerá daquilo que fazemos no presente." (Mahatma Gandhi)



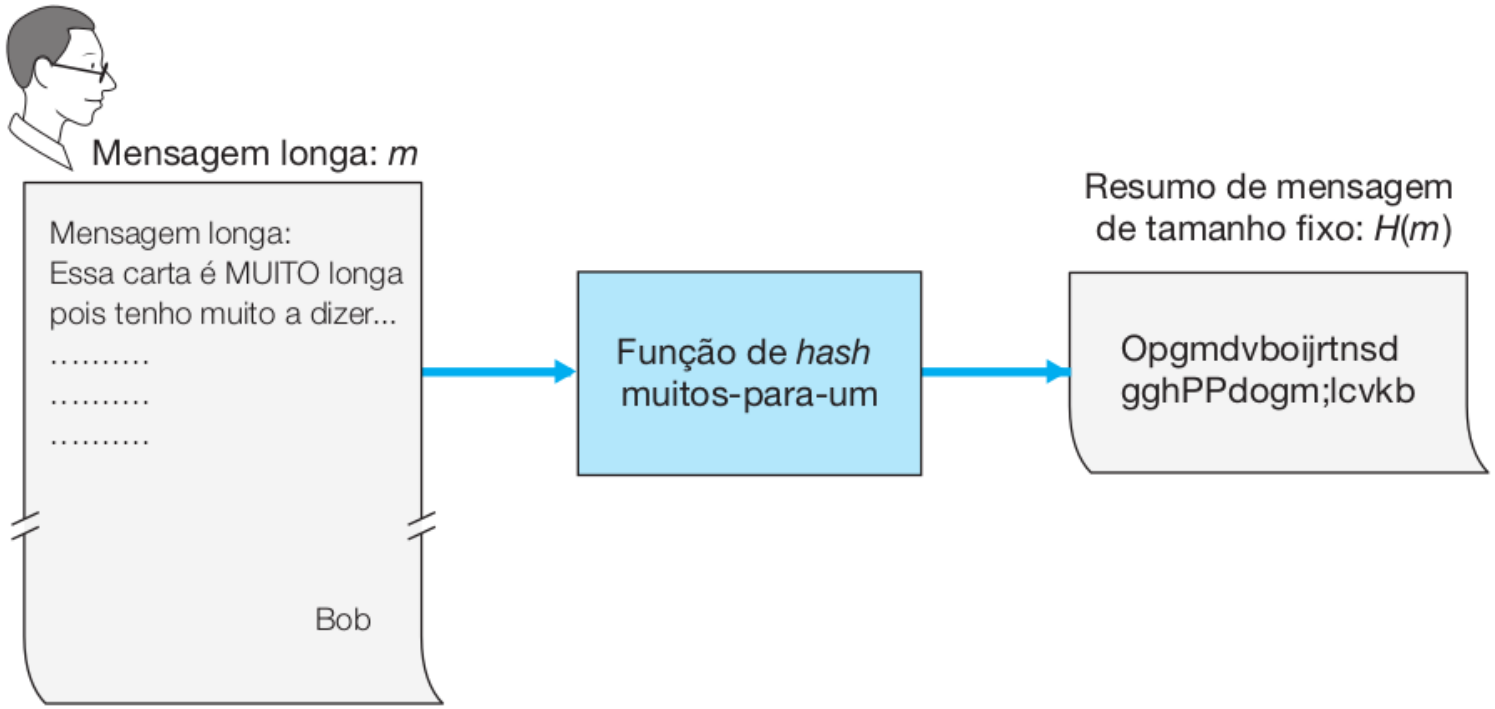
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender a função hash;
- Compreender suas características e propriedades;
- Conhecer algoritmos de hash;
- Aprender o funcionamento do MAC (código de autenticação de mensagens).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

A função *hash* é uma função matemática que recebe uma mensagem de tamanho variável, e produz uma saída de tamanho fixo (chamada de resumo da mensagem ou *digest*). O objeto principal é buscar garantir a **integridade** de um documento e/ou mensagem. Uma mudança em qualquer *bit* resultaria, com alta probabilidade, em uma mudança no código de *hash*. A função *hash* também é utilizada para armazenamento de senhas, comparar arquivos e assinaturas de vírus.



Propriedades

São propriedades de um algoritmo de *hash*:

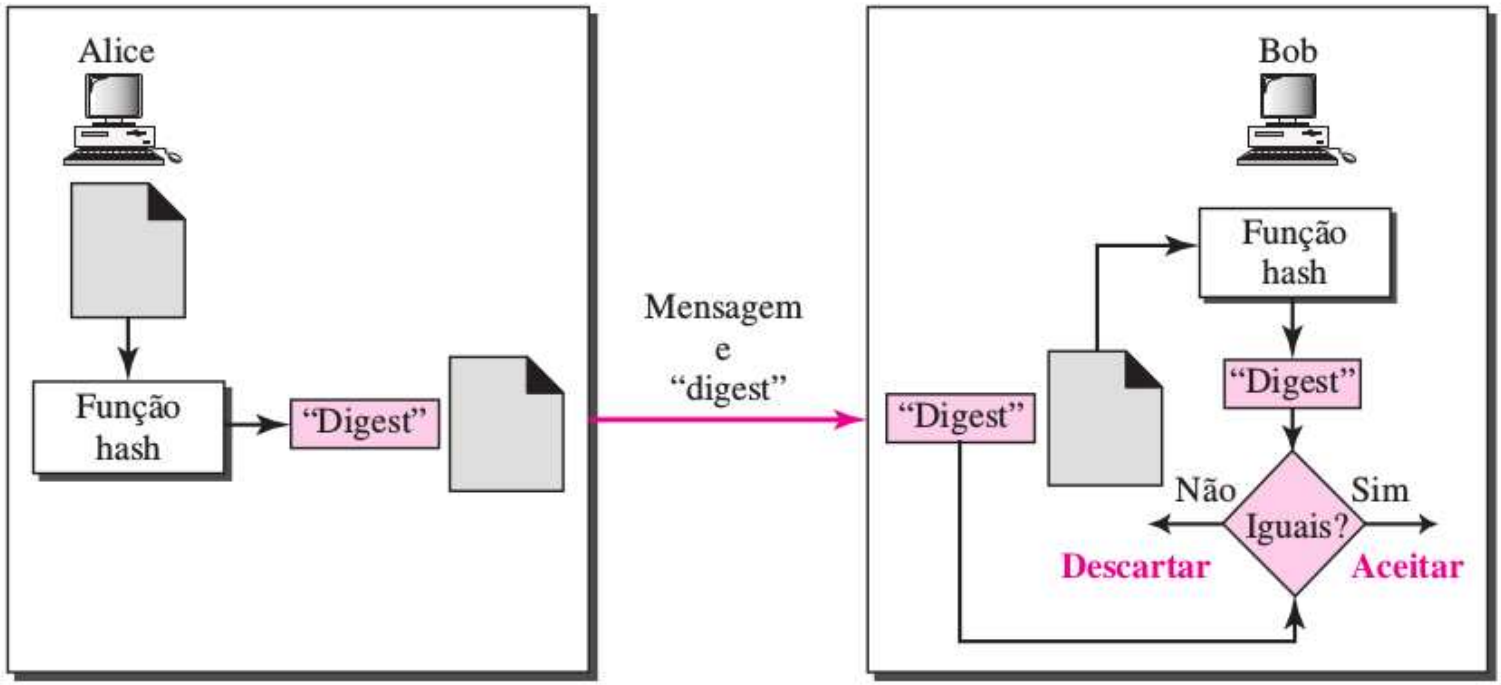
- Consistência: mesma entrada produz sempre a mesma saída.
- *One-way* (mão única): a saída não deve permitir descobrir informações de entrada (mensagem original).
- Único: quase impossível duas mensagens produzirem *hashes* iguais.

Uma função *hash* é semelhante à encriptação. Uma diferença é que o algoritmo de *hash* não precisa ser reversível, como para a decriptação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Hash Para Integridade dos Dados

O *hash* da mensagem é criado no emissor e enviado juntamente com a mensagem para o receptor. Para verificar a integridade da mensagem, o receptor calcula a função *hash* novamente e compara o resultado com aquele recebido. Se ambos forem o mesmo, o receptor tem certeza de que a mensagem original não foi alterada.



Os principais algoritmos de Hash seguros, atualmente, são uma família de algoritmos publicadas pelo Instituto Nacional de Padrões e Tecnologia (NIST) americano e Agência de Segurança Nacional (NSA) americano, são elas:

- SHA-0 : processa a entrada em blocos de 512 e produz uma saída de 160 bits. Surgiu falhas de segurança e não é mais recomendado o uso;
- SHA-1 : também possui o mesmo tamanho de entrada e saídas, mudando apenas alguns pontos no algoritmo. Fraquezas criptográficas foram descobertas e ele não foi mais aprovado para a maioria dos usos criptográficos;
- SHA-2 : processa blocos de 512 e 1024 e possui saída de 224, 256, 384 e 512 bits;
- SHA-3: processa blocos de entrada de 576 à 1152, e possui saída de 224, 256, 384 e 512 bits, O algoritmo difere significativamente do restante da família SHA.

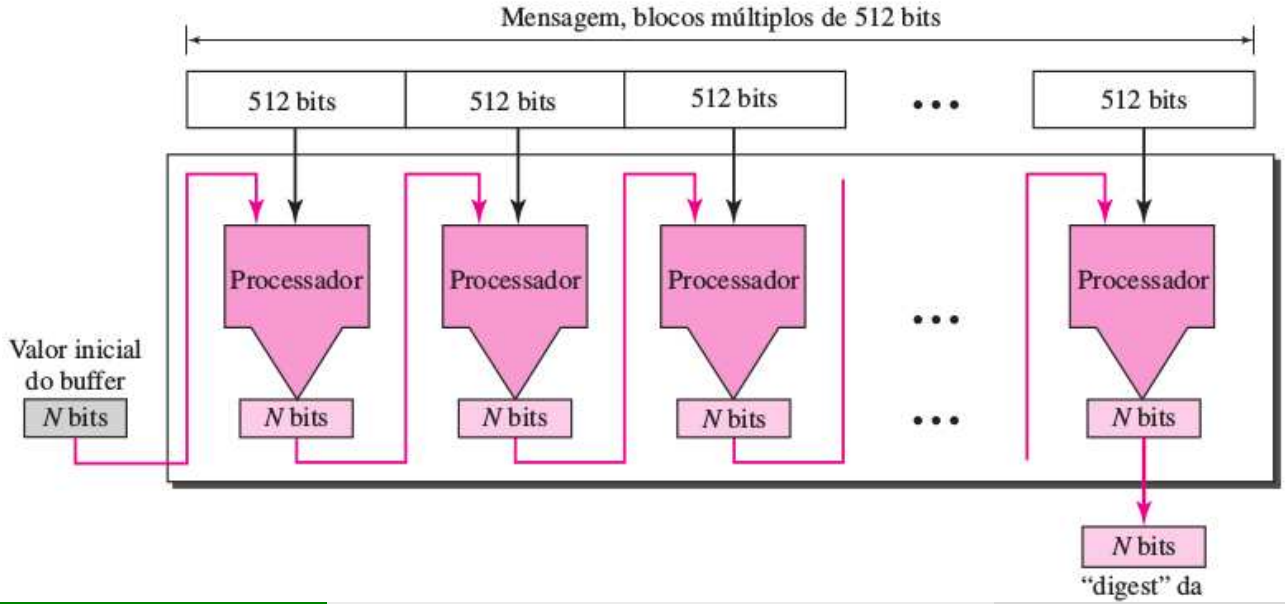
Exemplos

Mensagem Original: "**Curso de Redes de Computadores no IFRN**"
SHA-1: aae724d3c22188f8e40bfa1041f0f194ef387609

Mensagem Alterada: "**Curso de Redes de Computadores no IFRN.**"
SHA-1: 3cc2582ec28503e7e37bcb3cbc45e08c7c5018b1

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Por exemplo, no algoritmo SHA, a mensagem original é dividida em blocos de 512 bits. Um *buffer* de N *bits* é inicializado com um valor predeterminado. O algoritmo utiliza esse *buffer* com os 512 primeiros *bits* da mensagem para criar o primeiro resultado intermediário de 160 *bits*. Esse "digest" é então utilizado com o segundo bloco de 512 bits para criar o segundo resultado intermediário. E assim sucessivamente. Se um bloco não for de 512 bits, é usado preenchimento (0s) para que esse chegue ao comprimento. Quando o último bloco for processado, o "digest" resultante é o da mensagem original.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

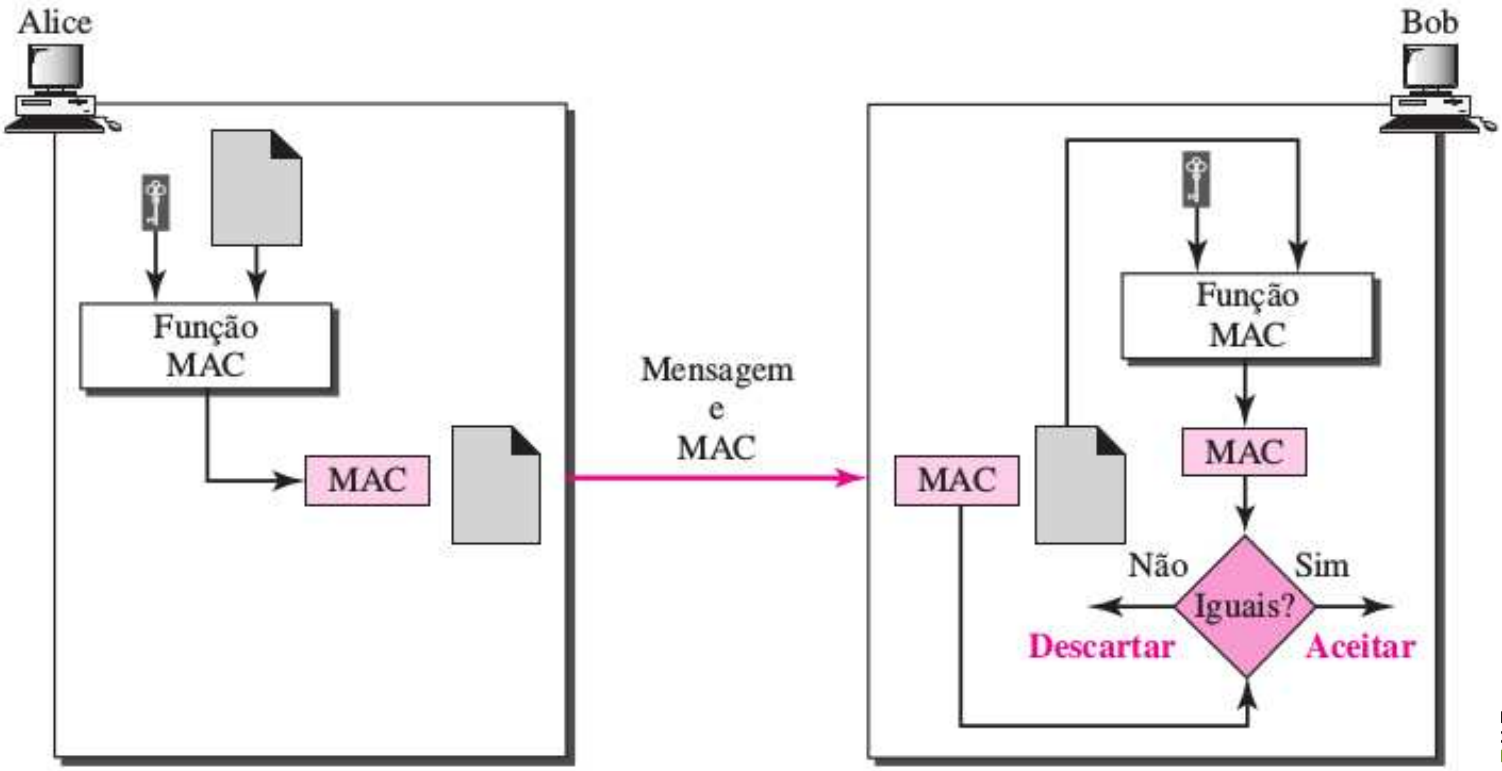
MAC

Uma função hash garante a integridade de uma mensagem. Essa abordagem é, obviamente, errônea, pois um atacante poderia criar uma mensagem m falsa, passar-se por Alice, calcular $H(m)$ e enviar $(m, H(m))$ a Bob.

Para garantir a integridade e autenticidade, ou seja, não ocorreu alteração dos dados e que quem enviou foi realmente a pessoa que se diz ser é utilizado a função hash com chaves simétricas criando o chamado MAC (Código de Autenticação de Mensagens).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

No MAC pode ser utilizado qualquer função hash padrão sem chaves, como o SHA-1, apenas acrescentando a chave (chave de autenticação). Desta forma, é calculado o hash do documento original + chave e enviado para o destinatário. O destinatário recebe o documento e calcula o hash acrescentando a mesma chave. Se os resultados do MAC forem iguais a mensagem será aceita, caso contrário, será descartada.



Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE