Segurança da Informação: Integridade

Prof. Renato da Costa

Integridade

“Propriedade de salvaguarda da exatidão e completeza de ativos ”

[ABNT NBR ISO/IEC 27001:2006]

BRB

No contexto da segurança da informação, há três pilares essenciais que devem ser considerados: confidencialidade, integridade e disponibilidade. Acerca desse assunto, assinale a alternativa que indica a medida que reforça o pilar de integridade.

a)Implementar um plano de recuperação de desastres em caso de perda de dados importantes.

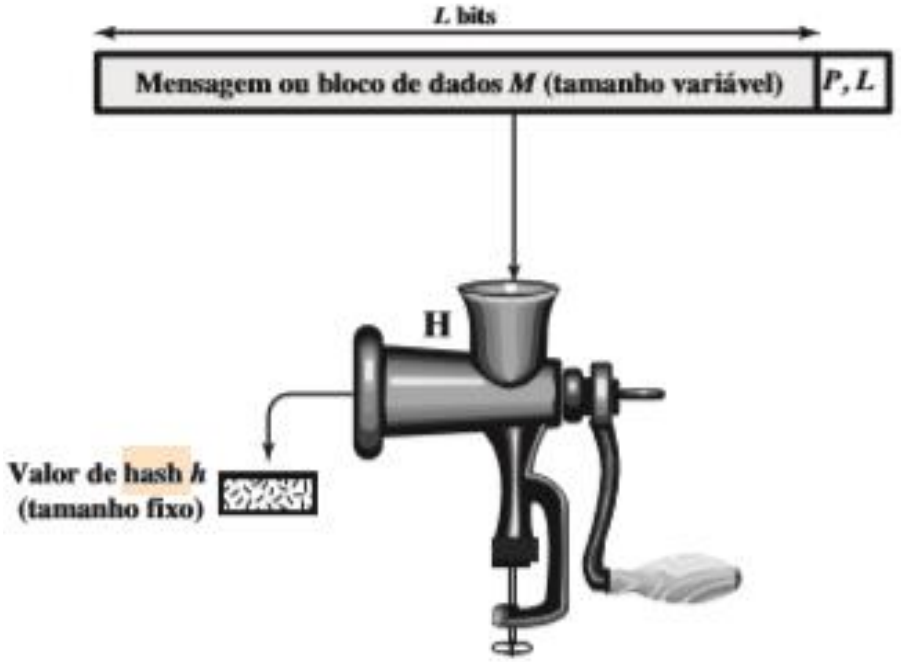
b)Definir acesso a informações somente para pessoas autorizadas.

c)Implementar processos de manutenção rápida de hardware.

d)Conscientizar os funcionários para que não violem regras e para que sigam os procedimentos de sigilo de dados.

e)Permitir a reversão de arquivos para versões anteriores, para casos de edições acidentais.

HASH



P, *L* = preenchimento mais campo de tamanho

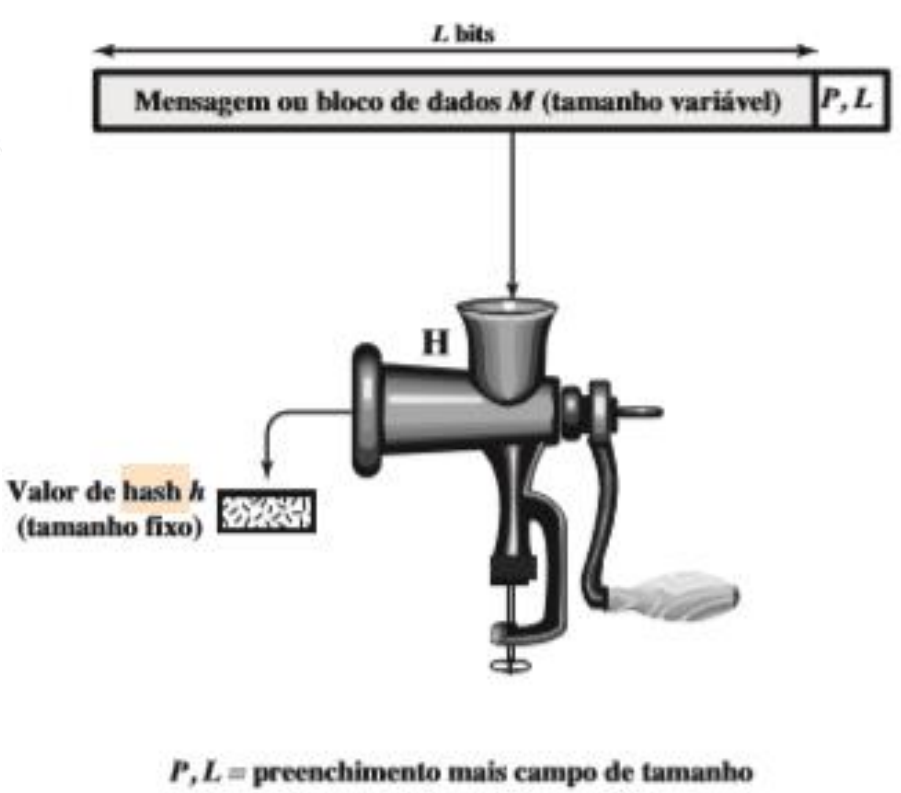
No caso do CPF, o DV módulo 11 corresponde ao resto da divisão por 11 do somatório da multiplicação de cada algarismo da base respectivamente por 9, 8, 7, 6, 5, 4, 3, 2, 1 e 0, a partir da unidade. O resto 10 é considerado 0. Veja, abaixo, exemplo de cálculo de DV módulo 11 para o CPF nº 280012389:

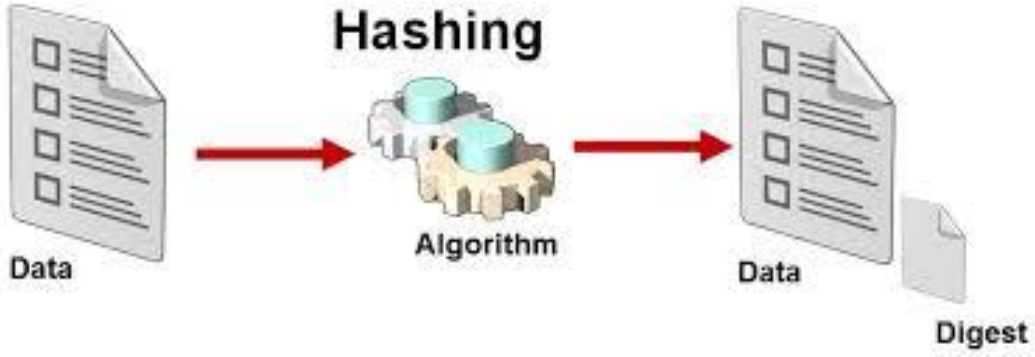
```
2  8  0  0  1  2  3  8  9 = 3
x  x  x  x  x  x  x  x  x
1  2  3  4  5  6  7  8  9
-------------------------
2+16+ 0+ 0+ 5+12+21+64+81 = 201÷11=18, com resto 3

2  8  0  0  1  2  3  8  9  3 = 8
x  x  x  x  x  x  x  x  x  x
0  1  2  3  4  5  6  7  8  9
----------------------------
0+ 8+ 0+ 0+ 4+10+18+56+72+27 = 195÷11=17, com resto 8

Portanto, CPF+DV = 280012389-38

Nota:
O resto 10 será sempre considerado 0.
```

CPF 9 dígitos: 069157127 | Calcular | DV: 98 | Reiniciar

A **Região Fiscal** onde emitido o **CPF** (definida pelo nono dígito) tem a seguinte abrangência: **1** (DF-GO-MS-MT-TO), **2** (AC-AM-AP-PA-RO-RR), **3** (CE-MA-PI), **4** (AL-PB-PE-RN), **5** (BA-SE), **6** (MG), **7** (ES-RJ), **8** (SP), **9** (PR-SC) e **0** (RS). Mas, inexplicavelmente, já vi CPF válido, emitido no DF (Região 1) com o nono dígito = 5 (Região BA-SE), o que me faz imaginar que o nono dígito foi incorporado para ampliar a capacidade de cadastros (de 100 milhões, a capacidade passou para 1 bilhão de números possíveis).

"Uma função de hash aceita uma mensagem de tamanho variável M como entrada e produz um valor de hash de tamanho fixo h = H(M). Uma "boa" função de hash tem a propriedade de que os resultados da aplicação da função a um grande conjunto de entradas produzirá saídas que são distribuídas por igual e aparentemente de modo aleatório. Em termos gerais, o objeto principal de uma função de hash é a integridade de dados. Uma mudança em qualquer bit ou bits em M resulta, com alta probabilidade, em uma mudança no código de hash."
(STALLINGS, Criptografia e Segurança de Redes, pág. 247)




Hashing
Data
Algorithm
Data
Digest

UFR - 2021

Método criptográfico que, quando aplicado sobre uma informação (arquivo), independentemente do tamanho que ela tenha, gera um resultado único (valor) e de tamanho fixo. Trata-se de

A) Assinatura Digital.
B) Certificado Digital.
C) Chave Mestra.
D) Função de Resumo.

Eletrobrás

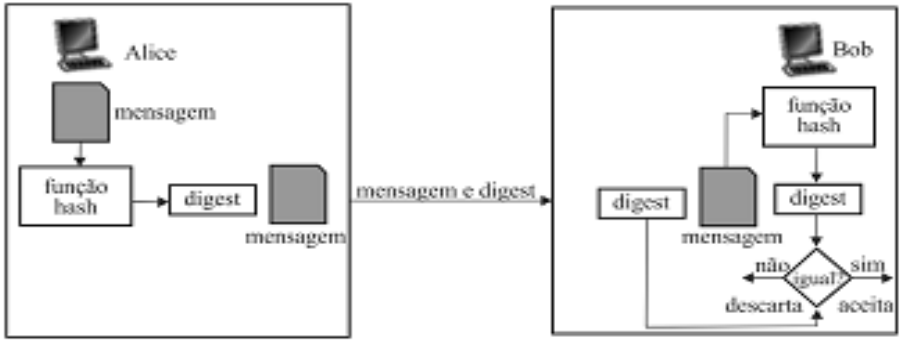
Ao se enviar arquivos pela internet há um método criptográfico que permite verificar se o arquivo foi alterado, ou seja, se teve sua integridade violada. Esse método, quando aplicado sobre as informações do arquivo, independente do seu tamanho, gera um resultado único de tamanho fixo. Assim, antes de enviar o arquivo pode-se aplicar esse método no conteúdo do arquivo, gerando um resultado A. Quando o arquivo é recebido pelo destinatário, pode-se aplicar novamente o método gerando um resultado B. Se o resultado A for igual ao resultado B significa que o arquivo está íntegro e não foi modificado; caso contrário, significa que o arquivo teve sua integridade violada.

...

Eletrobrás

O método criptográfico citado é conhecido como

a) função de hash.
b) criptografia simétrica.
c) esteganografia.
d) criptografia assimétrica.
e) certificação digital.



A figura precedente ilustra o esquema do serviço de segurança de redes denominado

a) autenticação de mensagens.
b) não repúdio.
c) integridade.
d) confidencialidade.
e) identificação de usuário.

MS

Função de *hashing* é uma função criptográfica mediante a qual sempre é gerada uma saída de tamanho fixo diferente para entradas diferentes, o que impossibilita a existência de mensagens diferentes para o mesmo hash.

( ) CERTA ( ) ERRADA

MS

Função de *hashing* é uma função criptográfica mediante a qual sempre é gerada uma saída de tamanho fixo diferente para entradas diferentes, o que ***impossibilita*** a existência de mensagens diferentes para o mesmo hash.

( ) CERTA (X) ***ERRADA***

Suframa

Para averiguar a integridade de um arquivo de computador a ser transmitido por um meio inseguro, pode-se gerar um hash antes da transmissão e verificar o hash após a transmissão.

( ) CERTA ( ) ERRADA

Abin

As funções hash são utilizadas em diversos meios computacionais, sendo uma de suas aplicações a verificação de integridade dos dados de uma transmissão.

( ) CERTA ( ) ERRADA

STJ

Uma função hash criptográfica é um algoritmo de encriptação de mão única, ou seja, muito difícil de inverter.
( ) CERTA ( ) ERRADA

UFAL

Quais técnicas asseguram, respectivamente, confidencialidade, integridade e autenticidade na troca de informações?

a) VPN, algoritmos de Hash e firewall.
b) Firewall, algoritmos de Hash e VPN.
c) Assinatura digital, criptografia e VPN.
d) Algoritmos de Hash, IDS e criptografia.
e) Criptografia, algoritmos de Hash e assinatura digital.

Informática
Prof. Renato da Costa