Criptografia

Algoritmos de Hash

Algoritmos de Hash

O problema

- Garantir que os arquivos tivessem o equivalente a uma impressão digital, o que permitiria saber identificar se o arquivo não foi modificado;

Algoritmos de Hash

Dificuldades

- O algoritmo não pode ser uma função reversível;
- Precisa ser rápido;
- O resultado não pode ser do tamanho do arquivo;

Algoritmos de Hash

Funções digest

- Função não reversível que não permite obter o valor de entrada;
- Exemplo 1: somar os valores de um código de barras:
- 12000. 34000. 01200.x.3920
- 3+7+3+14=27 =7
- 12000. 34000. 01200.7.3920

Algoritmos de Hash

Personalidade do nome

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Algoritmos de Hash

Soma das letras

- NELSON =14+5+12+19+15+14 = 79
- ALVES =1+12+ 22+5+19 = 59
- PINTO= 16+9+14+20+15=74
- 79+59+74=212
- 2+1+2 = 5

Algoritmos de Hash

Resultados

Resultado	Virtude
1	Alegria
2	Paciência
3	Caridade
4	Bondade
5	Fidelidade
6	Fé
7	Esperança
8	Temperança
9	Honestidade

Algoritmos de Hash

Características

- Entrada: tamanho variável;
- Saída: tamanho fixo;
- Colisão:
  - Duas entradas tem uma mesma saída;

Algoritmos de Hash

Exemplo de Colisão

- 123456 = 21
- 654321= 21

Algoritmos de Hash

Algoritmo MD5

- Fluxo de bits deve ser divisível por 512;
- Inicializado um Buffer:
  - word A: 01 23 45 67
  - word B: 89 ab cd ef
  - word C: fe dc ba 98
  - word D: 76 54 32 10

Algoritmos de Hash

Operações lógicas

- F(X,Y,Z) = (X and Y) or (not(X) and Z)
- G(X,Y,Z) = (X and Z) or (Y and not(Z))
- H(X,Y,Z) = X xor Y xor Z
- I(X,Y,Z) = Y xor (X or not(Z))

Algoritmos de Hash

Rodadas

```
                Rodada 1
  ----------------------------------
  F(a,b,c,d, X[ 0], 7, 0xd76aa478)
  F(d,a,b,c, X[ 1],12, 0xe8c7b756)
  F(c,d,a,b, X[ 2],17, 0x242070db)
  F(b,c,d,a, X[ 3],22, 0xc1bdceee)
  F(a,b,c,d, X[ 4], 7, 0xf57c0faf)
  F(d,a,b,c, X[ 5],12, 0x4787c62a)
  F(c,d,a,b, X[ 6],17, 0xa8304613)
  F(b,c,d,a, X[ 7],22, 0xfd469501)
  F(a,b,c,d, X[ 8], 7, 0x698098d8)
  F(d,a,b,c, X[ 9],12, 0x8b44f7af)
  F(c,d,a,b, X[10],17, 0xffff5bb1)
  F(b,c,d,a, X[11],22, 0x895cd7be)
  F(a,b,c,d, X[12], 7, 0x6b901122)
  F(d,a,b,c, X[13],12, 0xfd987193)
  F(c,d,a,b, X[14],17, 0xa679438e)
  F(b,c,d,a, X[15],22, 0x49b40821)
```

Algoritmos de Hash

Fraquezas

- Quebrado em 2005;
- Não é criptografia!

Algoritmos de Hash

Uso

- Verificação de arquivos;
- Armazenamento de senhas na web;
- Verificador de mensagens;
- Verificador de links.