Criptografia

Grupo de Resposta a Incidentes de Segurança

OLÁ,

Eu sou Sidney

Aluno de Ciência da Computação na UFRJ, Diretor do GRIS e membro do Laboratório de Redes e Multimídia(Labnet).

Sumário

- **O que é criptografia?**
- **Por que criptografar?**
- **Tipos de criptografia**
- **Hash**
- **base64, MD5 (básico)**
- **RSA, Diffie-Hellman (Intermediário)**
- **Criptografia Quântica(?)**
- **Tag**

O que é criptografia?

- **Consiste em técnicas cuja a finalidade destina-se a tornar informações sigilosas em mensagem que aparentam não ter sentido**
- **Esteganografia ≠ Criptografia**

Por que?

Tipos de Criptografias

Simétrica

- um algoritmo
- uma chave de segurança

Exemplo:

Cifra de césar e AES

Assimétrica

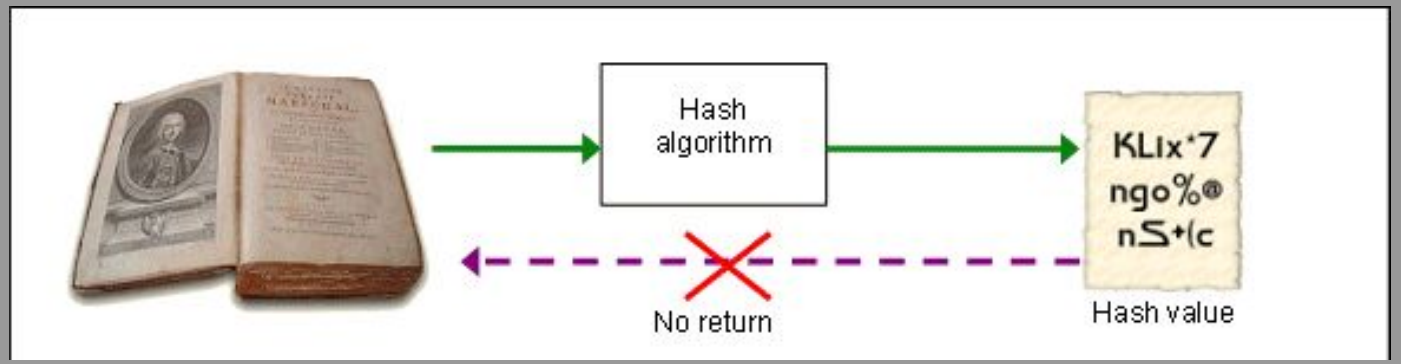
- um algoritmo
- uma chave pública (para encriptar)
- uma chave privada (para decriptar)

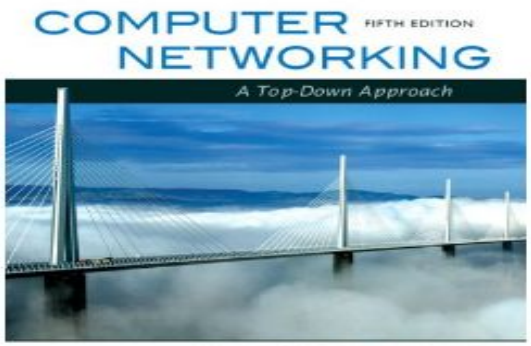
Exemplo:

RSA e curvas elípticas

Hash

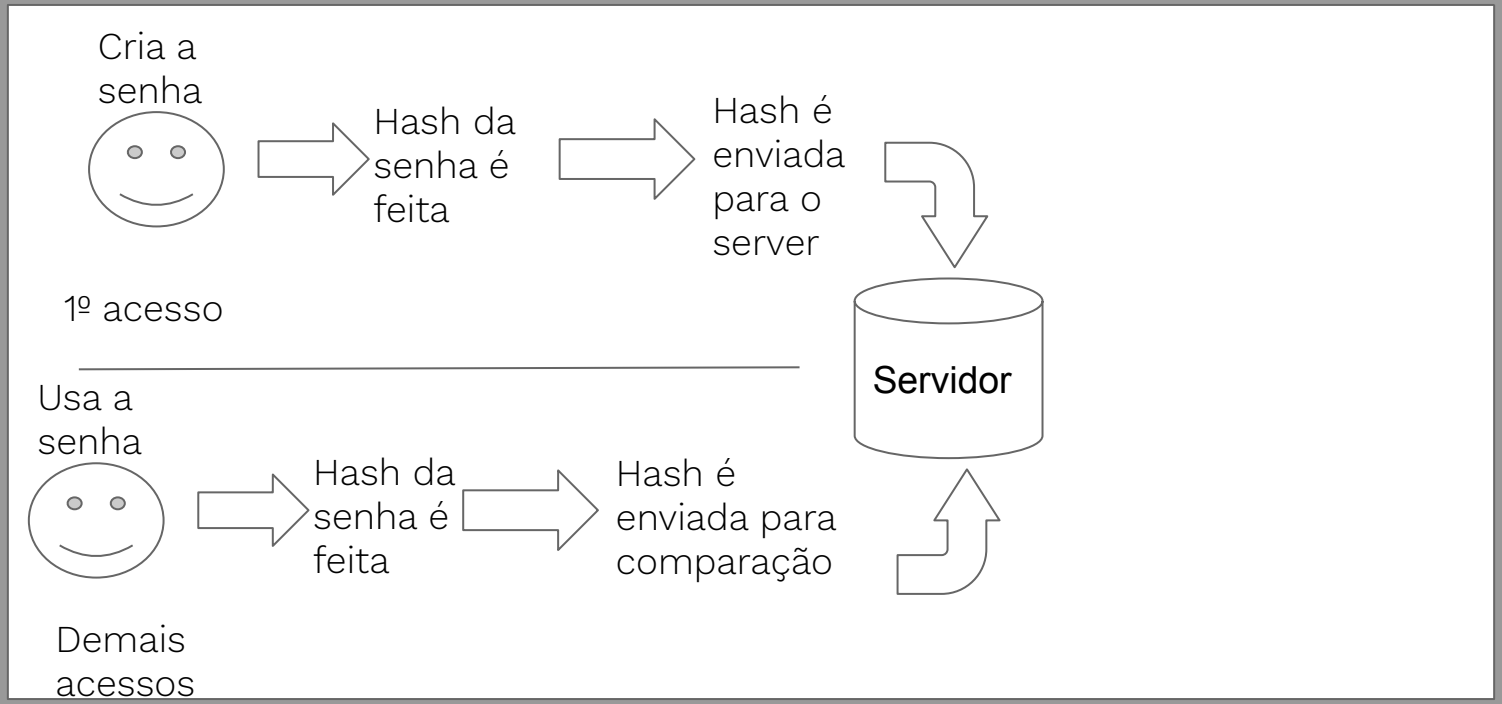
- **Uma função hash criptográfica é um algoritmo que pega uma informação de tamanho qualquer e mapeia para uma informação de tamanho fixo, além disso é praticamente impossível de inverter**
- **Pode ser usado para comparar e validar senhas ou validar a integridade de arquivos**

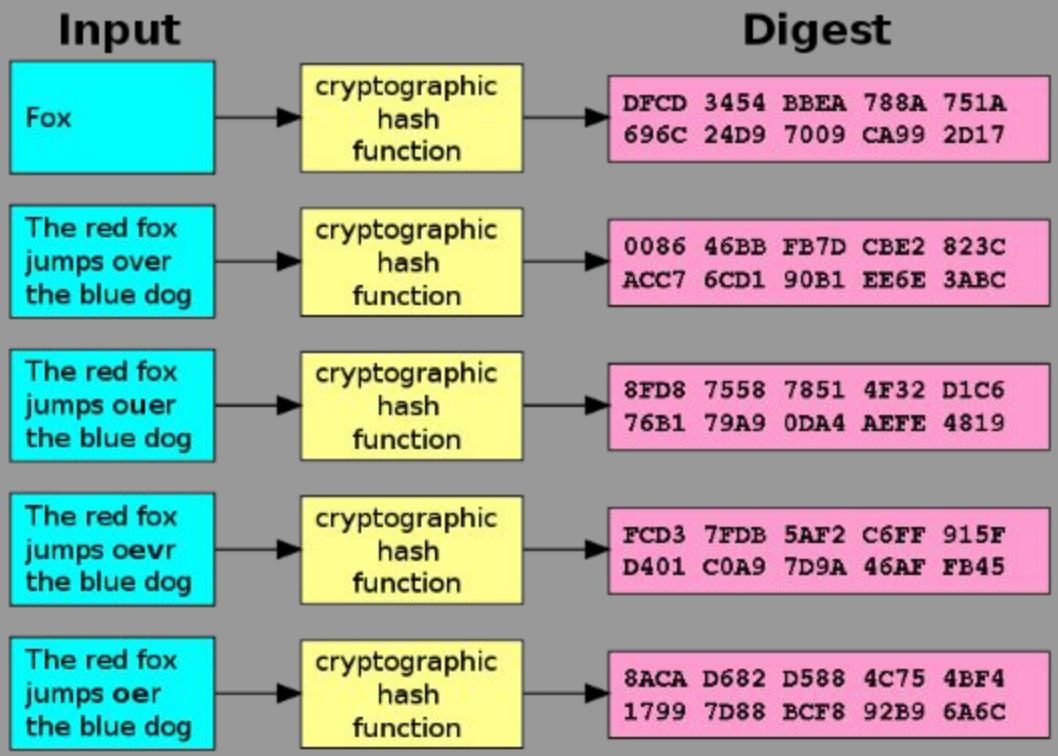

Hash
algorithm
KLIx*7
ngo%@
n≤+(c
No return
Hash value



Hashes:

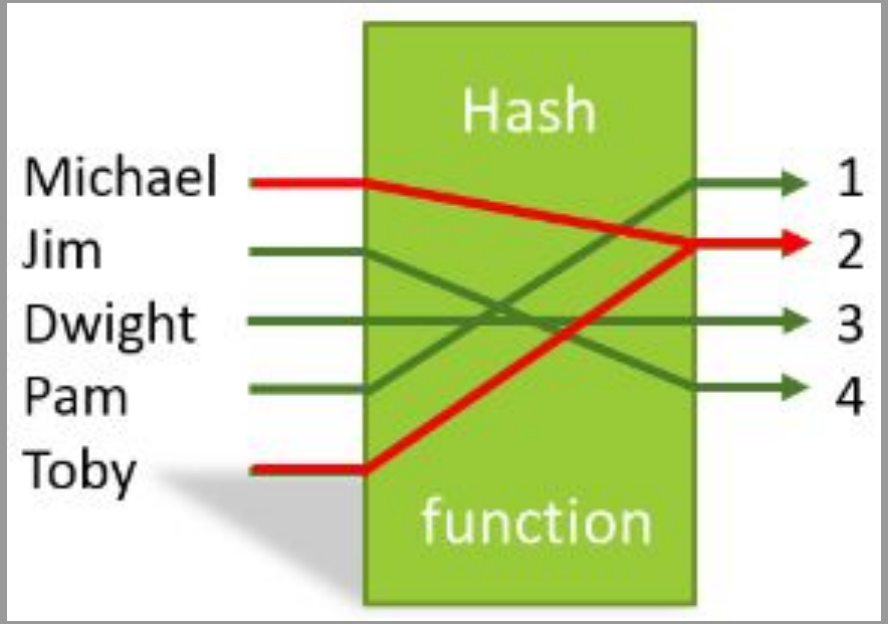
AICH	YDIFAZKS6NAXN6KIY5SVTXN667HD7PY3
CRC32	B6764D7C
eDonkey	92794EFFD6E32EF7790DEE770A4CB6A5
MD5	B29D6ECA58B6B460D11AD68F224EDD02
SHA1	2610CED2F8C4181898419DEA6CED5DC6407D0749
SHA256	80E5CF17E8A5CBB1D2168912FCB2A2BF 906898648469F51FB2930726324DF854
TTH	G2SJCBMF2IU6HEHJ6NPMEVBXQWCMOF4H7PFSXKI


Cria a senha
Hash da senha é feita
Hash é enviada para o server
1º acesso
Servidor
Usa a senha
Hash da senha é feita
Hash é enviada para comparação
Demais acessos


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

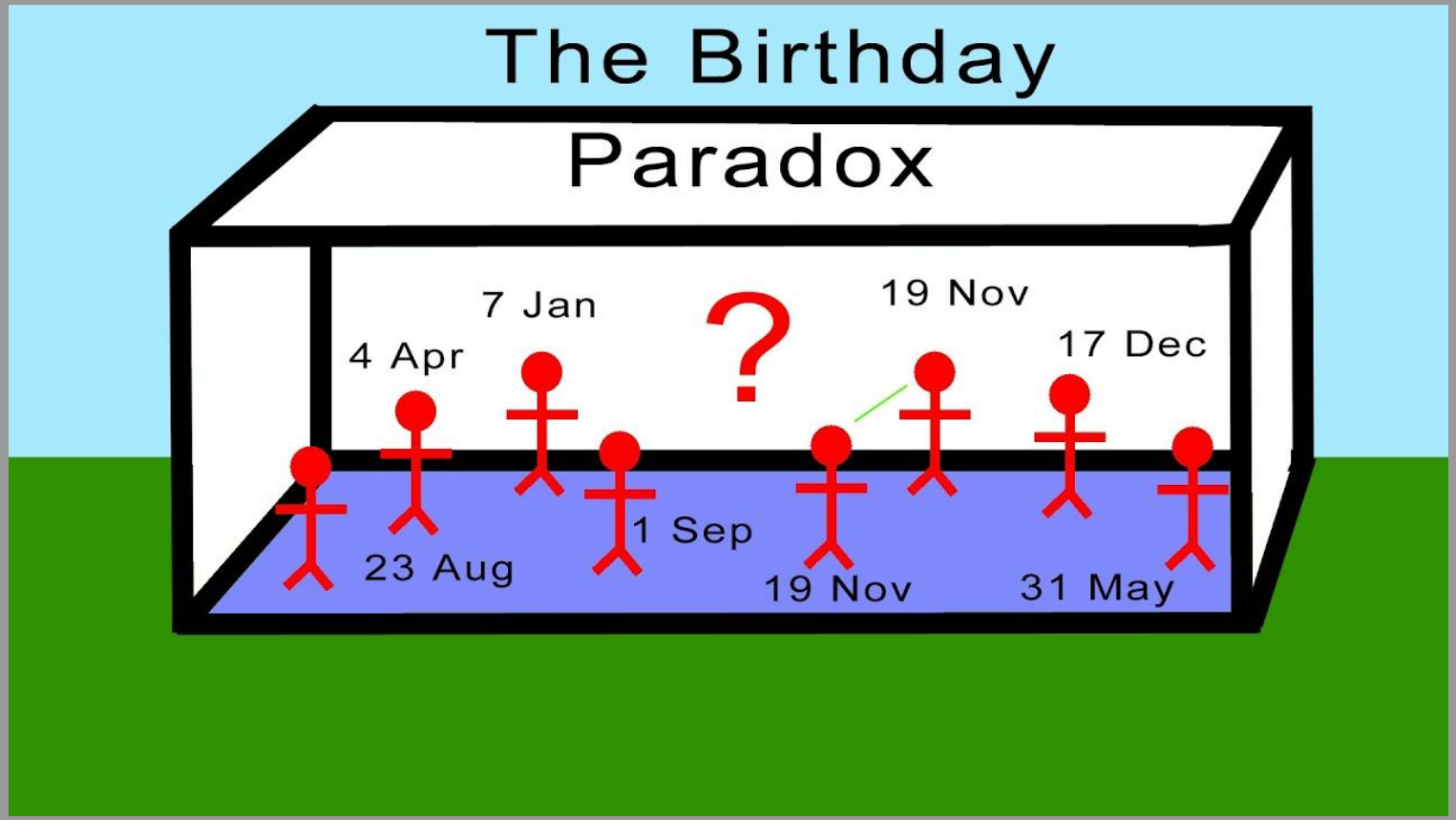
Colisão de Hash

- Quando duas entradas distintas são processadas por uma função hash e geram um mesmo resultado, isso se chama uma colisão de hash
- Todas as funções Hash tem potenciais colisões
- Uma função Hash é considerada boa, quando há poucas ocorrências de colisões


Hash
Michael
Jim
Dwight
Pam
Toby
function
1
2
3
4

Birthday attack

- **Baseado em um paradoxo usaremos a teoria da probabilidade para tentar encontrar uma colisão**
- **Um ataque de força bruta em que podemos estipular o quão seguro é uma função hash antes de executar**


The Birthday
Paradox
7 Jan
?
19 Nov
4 Apr
17 Dec
23 Aug
1 Sep
19 Nov
31 May

Para formar um par em que uma das partes seja especificamente uma pessoa:

Precisamos de 253 só para ter 50% de chance

Para formar um par qualquer:

Basta 23 pessoas para ter 50% de chance

Um pouco de Combinatória mostra o porquê

$$C_{23,2} = 253$$

Base64

- **É uma técnica de codificação usada para transferir dados binários por transmissão que aceitam texto**
- **Constituído por 64 caracteres ([a-z],[A-Z],[0-9],”/” e “+”), que deu origem ao nome**

source ASCII (if <128)	M								a								n							
source octets	77 (0x4d)								97 (0x61)								110 (0x6e)							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22				5				46							
Base64-encoded	T								W				F				u							
encoded octets	84 (0x54)								87 (0x57)				70 (0x46)				117 (0x75)							

MD5

- **Message Digest algorithm 5**
- **É um função hash criptográfica de 128 bits**
- **Fraco contra rainbow tables e não é seguro pela facilidade em gerar colisões**

MD5 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
md5_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
md5_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect
md5_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB	Perfect Non-perfect	Perfect Non-perfect
md5_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	690 GB 864 GB	Perfect Non-perfect	Perfect Non-perfect
md5_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB	Perfect Non-perfect	Perfect Non-perfect
md5_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	316 GB 396 GB	Perfect Non-perfect	Perfect Non-perfect

RSA

- **Encriptação a partir de um par de primos**
- **Sua força deriva-se da ausência de um algoritmo de fatoração eficiente**

1º passo: Escolha 2 números primos P e Q. Com isso, N = P x Q e F = (P-1)x(Q-1)

2º passo: Escolha um número ‘e’ qualquer maior que 3 e que o MDC entre ‘e’ e F seja 1

3º passo: Encontre um “d” inteiro que satisfaz a equação ed + fg = 1, sendo g um número inteiro qualquer

Chave pública: (n,e)

Chave privada: (n,d)

Ex:

Suponha P = 11 e Q = 13, então N e F são respectivamente 143(8 bits) e 120

Agora com e = 23, como o MDC(e,F) = 1, basta encontrar o ‘d’

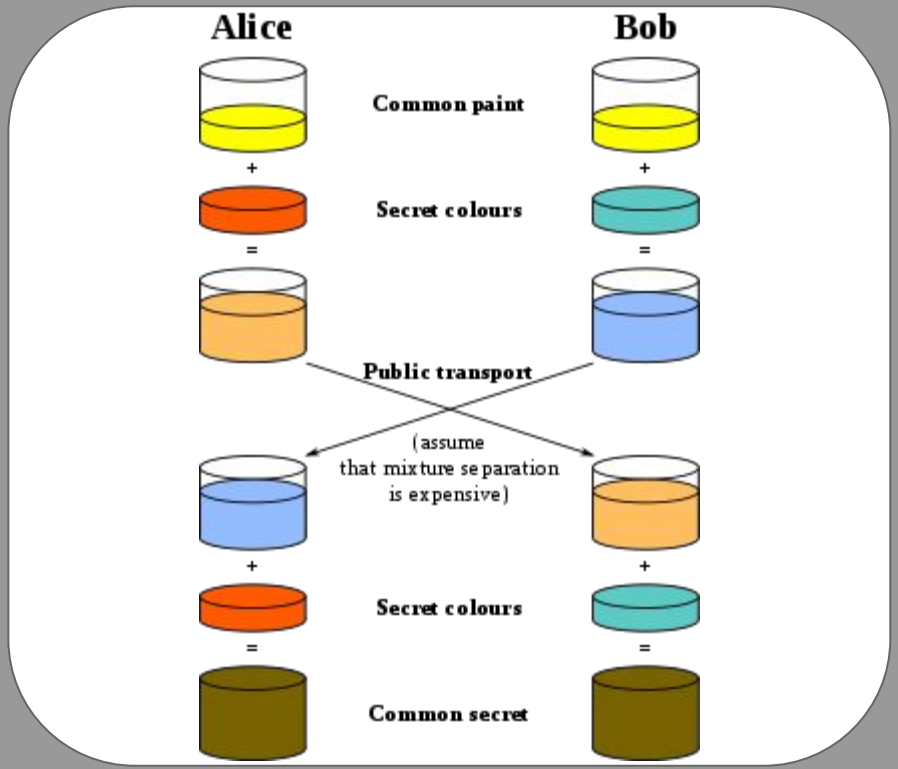
Usando um algoritmo que se chama Euclidiano estendido podemos encontrar 47 como valor apropriado para d

$$M^{e} \equiv C \pmod{N}$$

$$C^{d} \equiv M \pmod{N}$$

Diffie-Hellman

- **Algoritmo de troca de chaves ideal de ser usado quando pretende-se usar uma criptografia simétrica**


Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

Sid	**Membro do Gris**
2 números em comum é definido: **191 & 19**	2 números em comum é definido: **191 & 19**
O próprio número secreto é escolhido: **4**	O próprio número secreto é escolhido: **7**
$19^4 \equiv X \pmod{191}$	$19^7 \equiv Y \pmod{191}$
$\mathbf{Y^4} \equiv \mathbf{Z} \pmod{191}$	$\mathbf{X^7} \equiv \mathbf{Z} \pmod{191}$

A troca de chaves foi um sucesso e a chave é **Z**

Criptografia Quântica

- **Quantum proof**
- **BB84 & “coin tossing”**

Tag: Cryptopals

- **Fazer 3 desafios do site cryptopals.com (recomendo os três iniciais) e entregar um relatório explicando as questões selecionadas e suas respostas**
- **Pode ser feito em qualquer linguagem**
- **Entrega: daqui a 3 semanas**

OBRIGADO


sid@dcc.ufrj.br


@outeirosid