Criptografia Aplicada

Funções de Hash

Dênio Mariz
denio@ifpb.edu.br

Função de hash

- Função de Hash
  - É uma função criptográfica que recebe como entrada uma sequência de bits de qualquer tamanho e produz uma saída determinística tamanho fixo.
  - A saída é chamada de "valor hash" ou "hash" da entrada.
  - Outros termos também usados: "impressão digital" ou "resumo da mensagem" (message Digest)
- Entrada pode ser um string ou um arquivo
  - Arquivo=imagem, video ou o disco inteiro
- Exemplos:
  - saida=Hash("texto de entrada")
  - digest=hash(file.jpg)

Função de hash

- Colisão
  - Duas entradas diferentes geram a mesma saída
- Características Desejáveis
  - Probabilidade[colisão] --> 0
  - Mudança de 1 bit na entrada altera completamente a saída
- Número de mensagens de entrada é infinito, mas o número de hashes é finito (tamanho fixo)
  - Exemplo: hash de 160 bits gera 2^{160} hashes diferentes

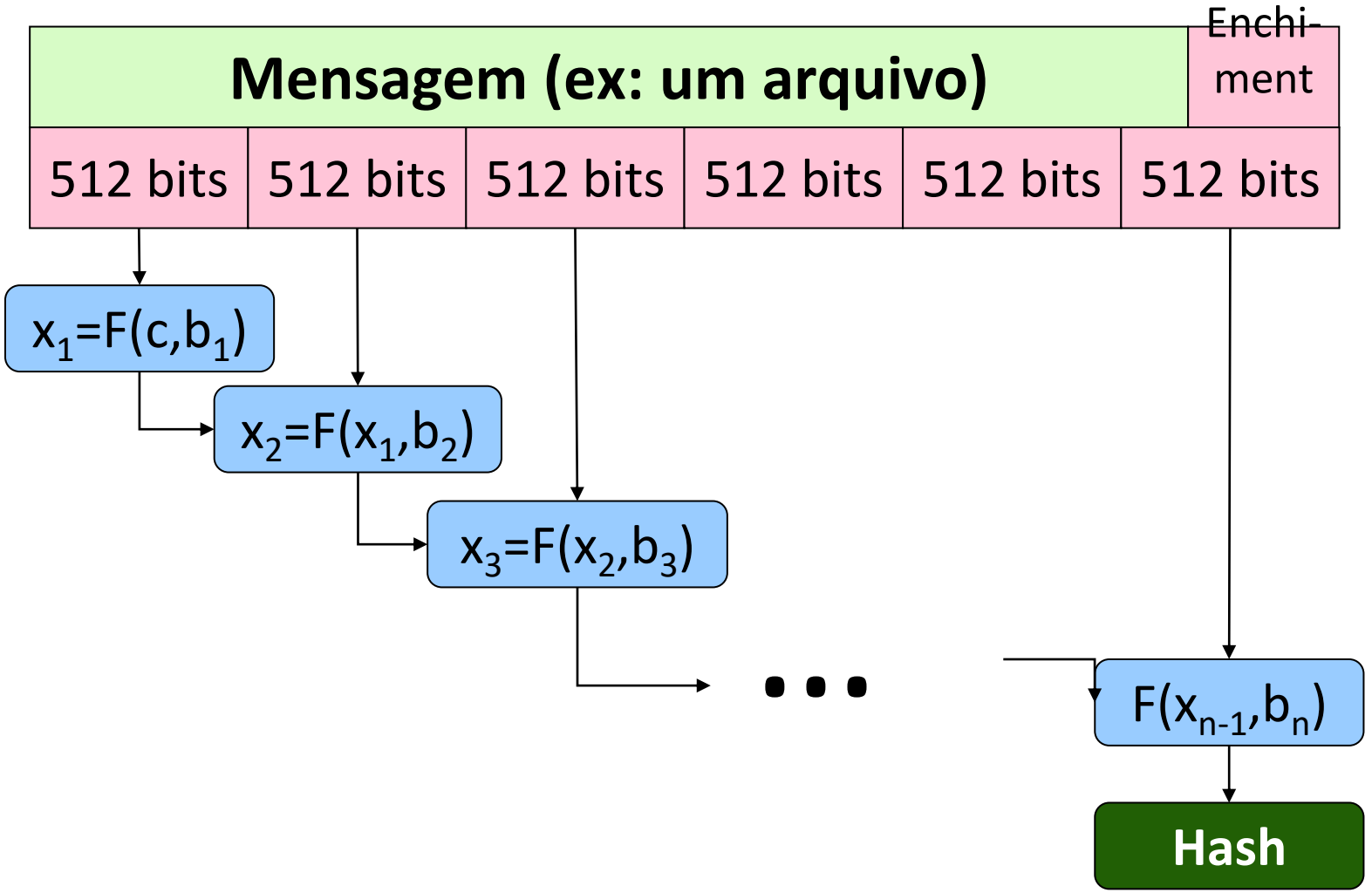
Requisitos de uma função de Hash

- Viabilidade computational
  - É "barato" computar o hash **y**=**H**(**x**)
- Pre-image resistance
  - É difícil encontrar uma mensagem de entrada **x** tal que **y**=**H**(**x**) conhecendo apenas a saída **y**
- Collision resistance
  - É difícil encontrar duas entradas $\mathbf{x_1}$ e $\mathbf{x_2}$ tal que $\mathbf{x_1} \neq \mathbf{x_2}$ e $\mathbf{H}(\mathbf{x_1}) = \mathbf{H}(\mathbf{x_2})$
- Além disso
  - A saída deve ter tamanho fixo
  - A função **H()** não PODE ter inversa (one-way function)

Aplicações de uma função de Hash

- Verificação de integridade de uma mensagem M
  - Calcule $\mathbf{h_1}$=H(M)
  - Guarde $\mathbf{h_1}$
  - Calcule h_2=H(M) a qualquer hora. Se $h_1 \neq h_2$ então M foi alterada
- Armazenamento de senha S
  - Guarde h_1=H(S) ao invés da senha S
  - Na autenticação, solicite a senha S_u do usuário
  - Calcule h_2=H (S_u). Se $h_1 = h_2$ então S_u = S

Algoritmo de Hash: Funcionamento Básico



Algoritmos de Hash

- MD5 (Message Digest 5)
  - Derivado da família MD2, MD3, MD4, MD5 (MD2-4 não usados atualmente)
  - Projetado por Ron Rivest, descrito na RFC 1321 (1992)
  - Entrada de tamanho arbitrário
  - Gera hash de 128 bits (chamado de "message digest")
  - Exemplo:
    - MD5 ("message digest") = f96b697d7cb7938d525a2f31aaf161d0

Veja detalhes do MD5 em en.wikipedia.org/wiki/MD5

Algoritmos de Hash

- SHA (Secure Hash Algorithm)
  - Desenvolvido pelo National Institute of Standars and Technology (NIST) & NSA

Função	Descrição
SHA-0	Versão original (1993), substituído pelo SHA-1 devido a falhas
SHA-1	Projetado pela National Security Agency (NSA). Saída de 160 bits.
SHA-2	Uma família de hashes com diferentes tamanhos de saída: SHA-256 e SHA-512. Existem versões com tamanhos diferentes de saída: SHA-224, SHA-384
SHA-3	Escolhida em 2012 por competição pública. Suporta mesmos tamanhos do SHA-2, mas com estrutura de cálculo diferente (usa função antes conhecida como Keccak).

  - Exemplo:
    - SHA256(“message digest") = 3520b54ccec750d15256ada5b3d51cfddcec7fad1482f6bde2ea1c31a2c5b3a5

Colisão MD5

```
d131dd02c5e6eec4693d9a0698aff95
c2fcab58712467eab4004583eb8fb7f
8955ad340609f4b30283e4888325714
15a085125e8f7cdc99fd91dbdf28037
3c5bd8823e3156348f5bae6dacd436c
919c6dd53e2b487da03fd02396306d2
48cda0e99f33420f577ee8ce54b6708
0a80d1ec69821bcb6a8839396f9652b
6ff72a70
```

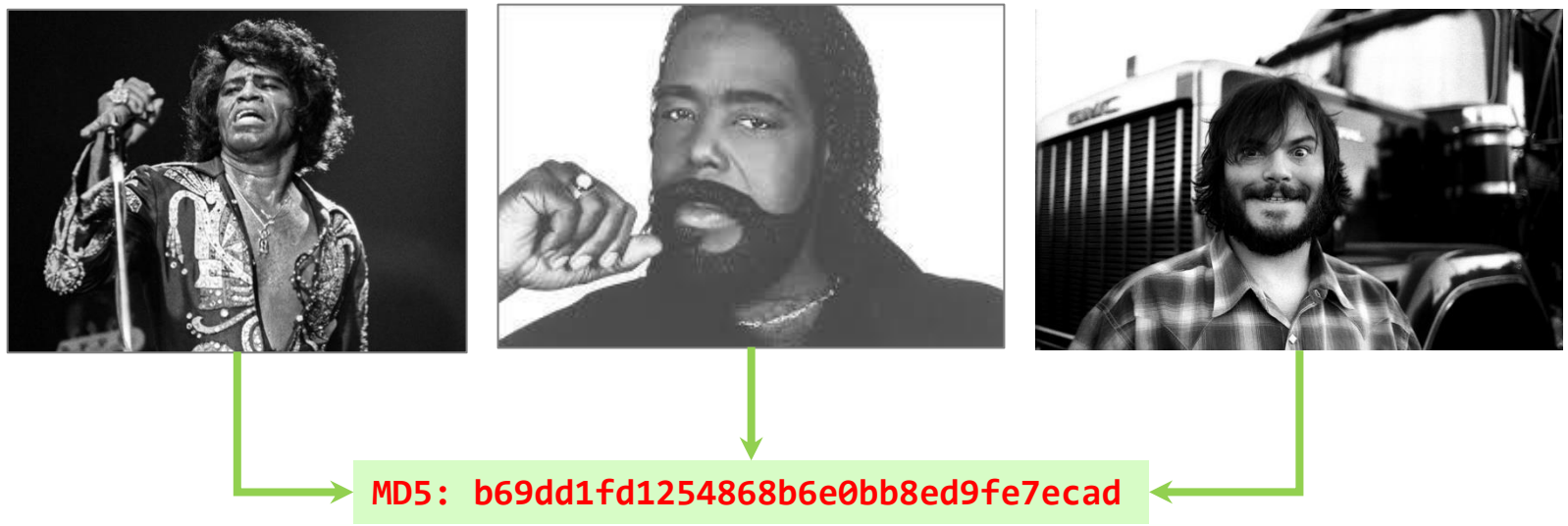
```
d131dd02c5e6eec4693d9a0698aff95
c2fcab50712467eab4004583eb8fb7f
8955ad340609f4b30283e4888325f14
15a085125e8f7cdc99fd91dbd728037
3c5bd8823e3156348f5bae6dacd436c
919c6dd53e23487da03fd02396306d2
48cda0e99f33420f577ee8ce54b6708
0280d1ec69821bcb6a8839396f965ab
6ff72a70
```

Ambas as sequencias de bits acima possuem o
mesmo hash md5=79054025255fb1a26e4bc422aef54eb4

Fonte: http://www.mscs.dal.ca/~selinger/md5collision/

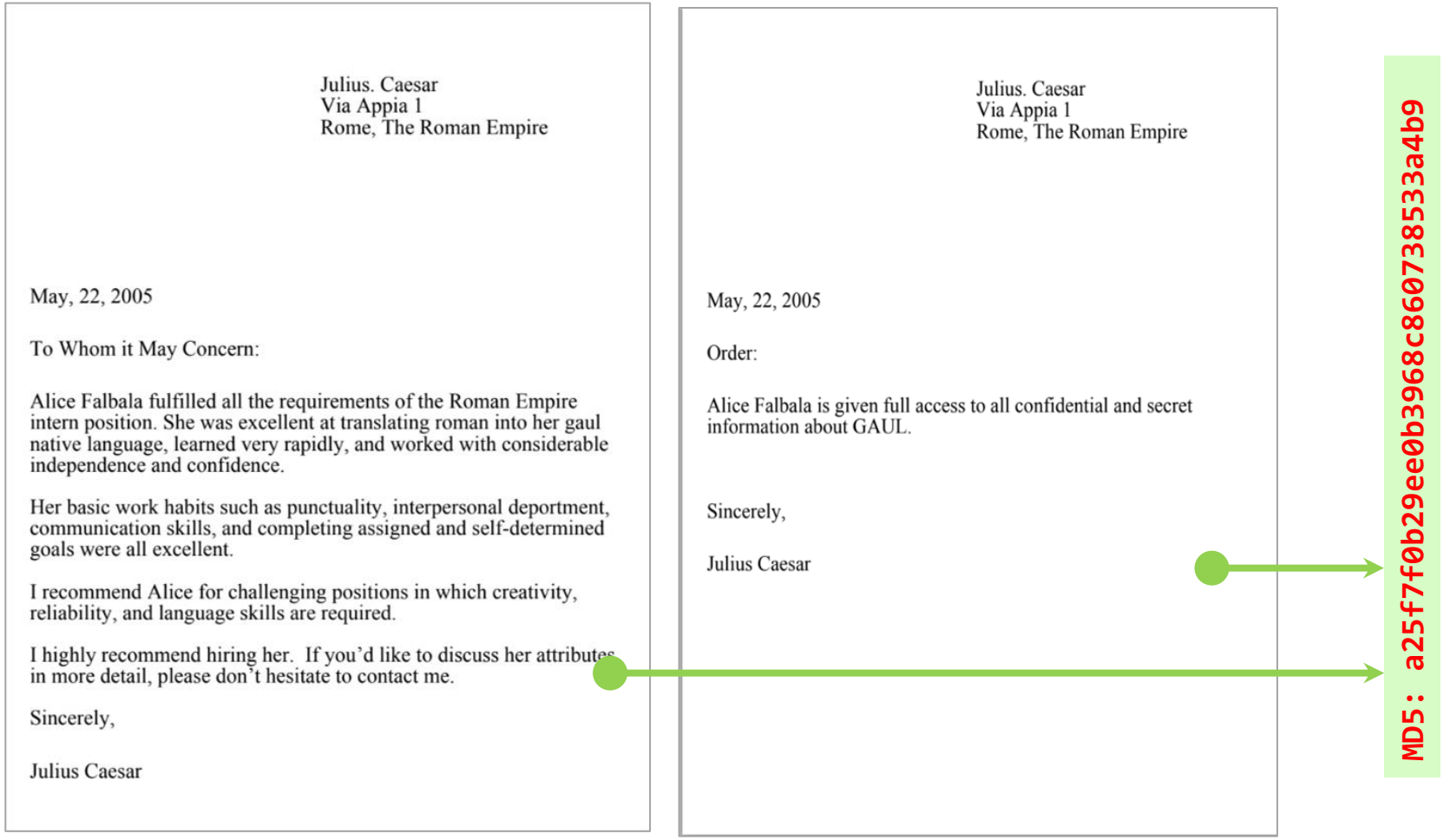
Colisão no MD5 (com significado!)

- Figuras abaixo possuem **o mesmo MD5**



Fonte: https://natmchugh.blogspot.com.br/2014/11/three-way-md5-collision.html

Colisão no MD5 (com significado!)



Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

MD5: a25f7f0b29ee0b3968c860738533a4b9

http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/MD5-Collisions/CITS-MD5-Collisions.html

Colisão no SHA-1

- Arquivos PDF abaixo possuem **o mesmo SHA-1**
- Técnica desenvolvida pelo Google e CWI: apenas 2^{63} cálculos
- Custo estimado de calcular a colisão SHA-1 é de ~US$120 mil usando Amazon EC2 cloud por alguns meses

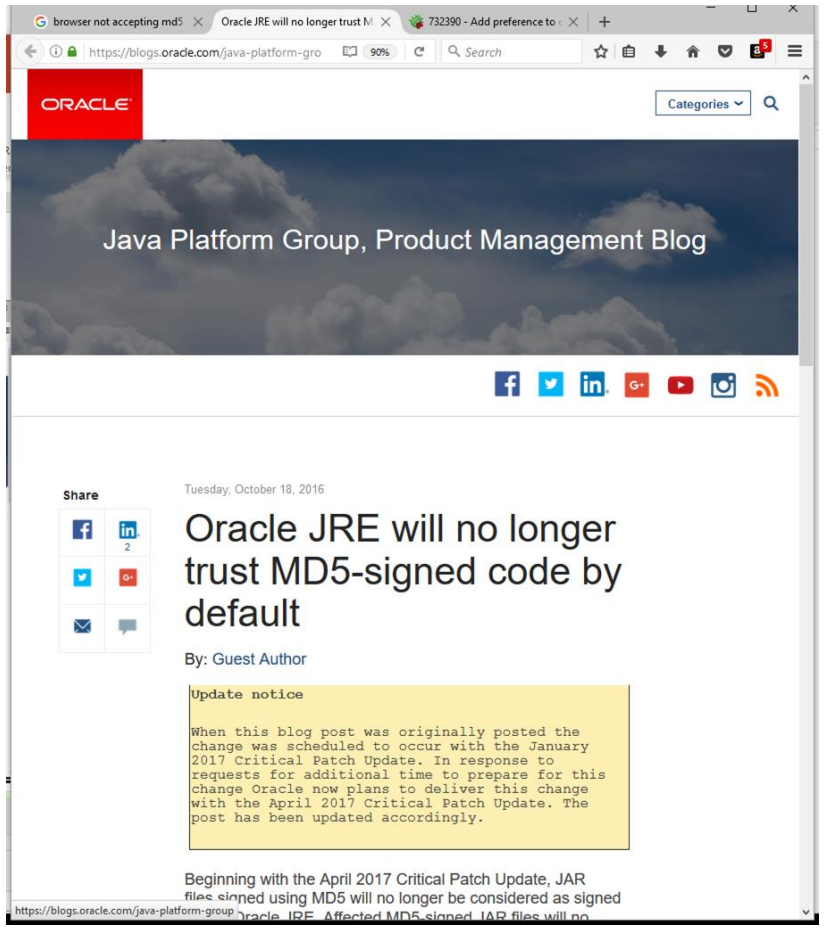
Fonte: http://thehackernews.com/2017/02/sha1-collision-attack.html
https://shattered.io/

Impacto de colisões de hash

- Assinaturas Digitais de documentos
- Falsificação de certificados digitais X.509
- Quebra de Passwords
- Sistema de controle de versões (Git)
- Sistemas de backup

- Exemplo em:
  - https://www.win.tue.nl/hashclash/rogue-ca/

SHA-0/1, MD5 encerram a carreira



Demonstração

- SHA
- MD5