



1



2




GRADUAÇÃO

Cognitive Cybersecurity

Prof. Leonardo Orabona
E-mail: profleonardo.orabona@fiap.com.br

Prof. Dr. Noris Junior
E-mail: profnoris.junior@fiap.com.br

3



I Agenda

- Recap da aula anterior
- Certificado digital
- Hash
- Assinatura digital

4

I Princípios da segurança

FIAP

- Confidencialidade (C)
- Integridade (I)
- Disponibilidade (A)

1 Confidencialidade



Garante que as informações estão corretas, autênticas e não sofreram qualquer alteração

2 Integridade



Garante que as informações estão disponíveis quando desejado

3 Disponibilidade



Garante que apenas pessoas de posse da chave tenham acesso ao conteúdo das informações

5

I O problema da confiança no mundo digital

FIAP

- Você recebe uma carta dizendo que ganhou um prêmio milionário. No envelope, há um selo de cera, mas... **como saber se a carta é legítima?**
- O mundo digital tem o mesmo problema:
 - Como saber se um site realmente pertence a um banco e não a um golpista?
 - Como garantir que um documento digital enviado por um juiz não foi alterado?
 - Como provar que um e-mail veio de um remetente autêntico?
- A resposta: **certificado digital, hash e assinatura digital.**

6

I

FIAP

HASH

7

I O que é um hash?

FIAP

- **RESUMO**
- Suponha que preciso criar um **resumo** de um livro de **1000 páginas**
- Ou um **resumo** de um livro de **100 páginas**
- Porém, **o resumo deve ter sempre o mesmo tamanho,** independentemente do número de páginas

Isso é um **hash**

8

I Hash

FIAP

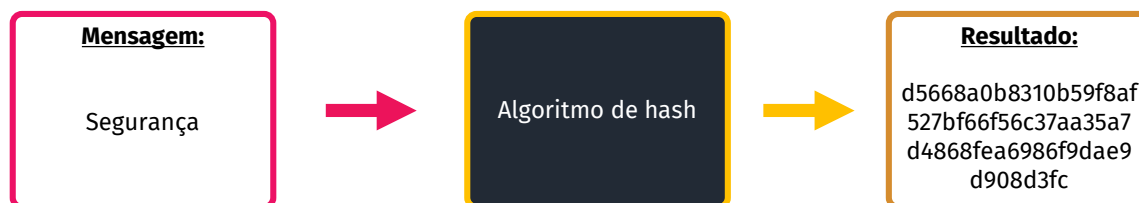
- Um algoritmo que transforma qualquer informação em uma sequência fixa de caracteres.
- Pequenas **mudanças** (um único caracter, por exemplo) no conteúdo resultam em um **hash completamente diferente**.

9

I Hash

FIAP

- Exemplo:
 - Preciso garantir que a mensagem “Segurança” chegue ao destinatário sem modificação.
 - Envio a mensagem “Segurança” e o hash da mensagem.

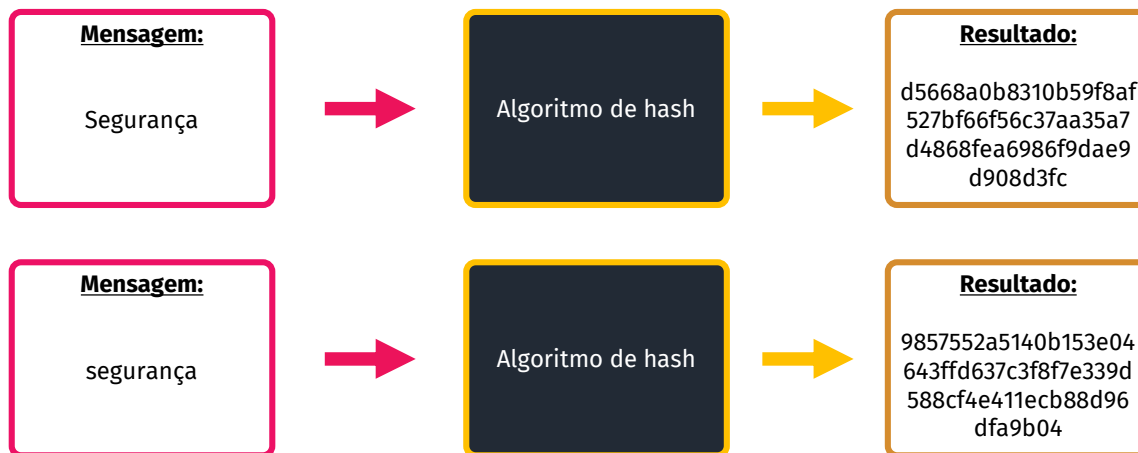


10

I Hash

FIAP

- Apenas uma pequena mudança...

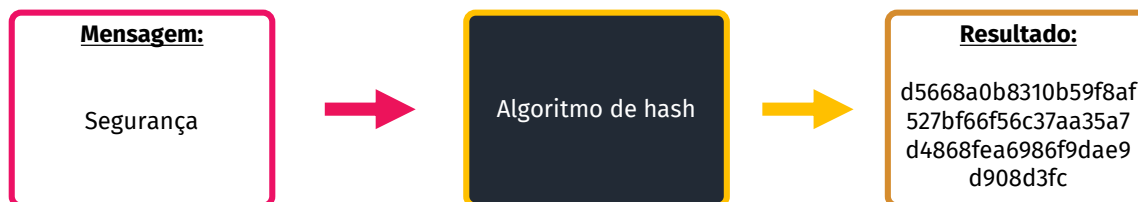


11

I Hash

FIAP

- O que o destinatário precisa fazer?
 - Usar o mesmo algoritmo de hash para a mesma mensagem



- **Hash é igual** = mensagem **íntegra**
- **Hash é diferente** = mensagem foi **modificada**

12

I Hash

FIAP

- Algoritmos mais conhecidos:

- MD5:

- Uma das funções antigamente mais usadas
 - Gera um valor de 128 bits (16 Bytes)
 - Suscetível a colisões: duas mensagens diferentes (muito grandes!) podem gerar o mesmo hash
 - Não deve ser mais usado

- SHA-256

- Uma função de hash muito usada
 - Gera um valor de 256 bits (32 Bytes)
 - Usado em certificados digitais
 - Já existe o SHA-384 e o SHA-512

13

I Hash

FIAP

- Palavra: Security (8 letras, 8 caracteres). Supondo 8 Bytes:

- Em português: Security

- Em binário: 01010011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

- Em hexadecimal: 53 65 63 75 72 69 74 79

14

I Playground

FIAP

- Conversões e algoritmos:
 - <https://gchq.github.io/CyberChef>
- Hash usando SHA em python:
 - <https://colab.research.google.com/drive/1sPl8SnHvfdQ1XNOiHqtmUzn4ZYvvwFqG?usp=sharing>

15

I

FIAP

HANDS ON!

16

I Hash

FIAP

- A partir do hash não é possível obter a mensagem
- Mas é possível que o destinatário confira se a mensagem “bate” com o hash
- Hash é determinístico:
 - A mesma entrada gerará o mesmo resultado
- **Em quais aplicações/cenários podemos aplicar hash?**

17

I Hash

FIAP

- Aplicações de hash na prática:
 - Verificar a integridade de arquivos
 - Armazenar senhas de forma segura
 - Criar assinaturas digitais confiáveis

18