Lição 9

Message Digest

Objetivos

Ao final desta lição, o estudante será capaz de:

- Conhecer os principais algoritmos de *Message Digest*
- Identificar os principais usos da utilização de *Message Digest*
- Empregar a classe *MessageDigest* em um aplicativo

Algoritmos de Message Digest

- *Message Digest 5* (MD5)
- *Secure Hash Algothm* (SHA)

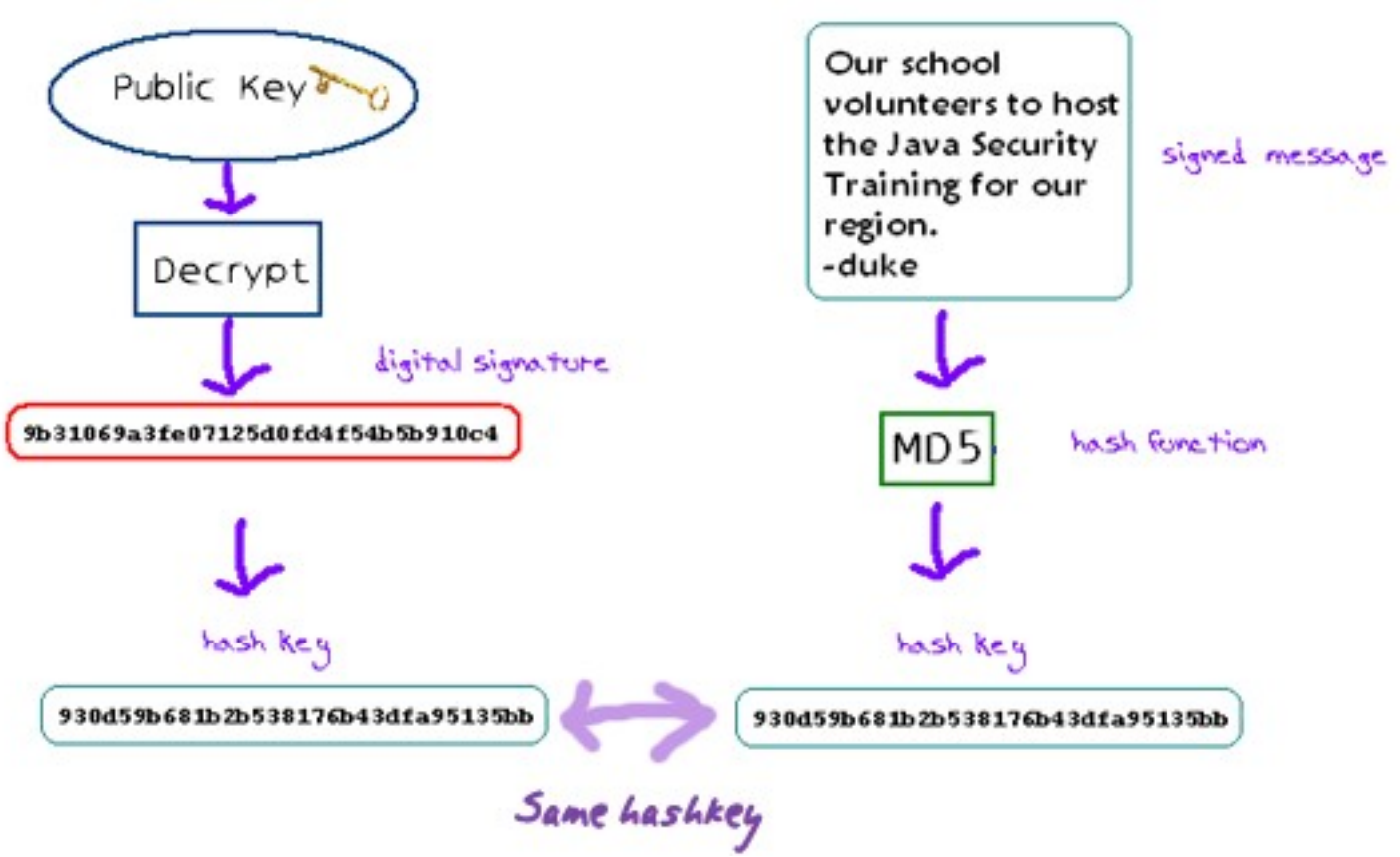
Nome	***Algoritmo***
SHA-1	Produz uma mensagem com 20 bytes (40 dígitos Hex); aplicável a documentos com menos de 2^{64} bits.
SHA-256	Produz uma mensagem com 32 bytes (64 dígitos Hex); aplicável a documentos com menos de 2^{64} bits.
SHA-384	Produz uma mensagem de 48 bytes (96 dígitos Hex); aplicável a documentos com menos de 2^{128} bits.
SHA-512	Produz uma mensagem de 64 bytes (128 dígitos Hex); aplicável a documentos com menos de 2^{128} bits.

Aplicações Comuns

- Aumento de desempenho
- Autenticação
- Assinatura digital de documentos
- Verificação de Dados

Assinatura Digital de Documentos – Criptografar

Assinatura Digital de Documentos – Decriptar

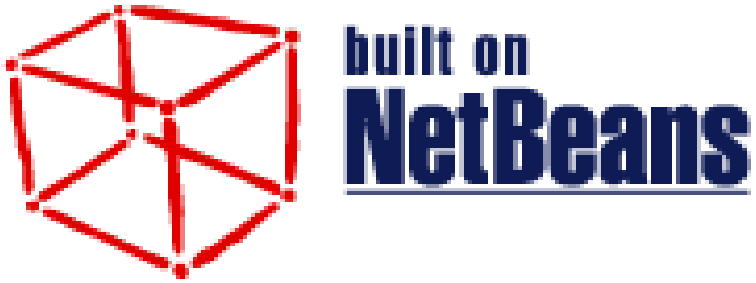


Classe MessageDigest

- getInstance(String algorithm)
- getInstance(String algorithm, Provider provider)
- getInstance(String algorithm, String provider)
- update(byte input)
- update(byte[] input)
- update(byte[] input, int offset, int len)
- reset()
- digest()
- byte[] digest()
- byte[] digest(byte[] input)
- int digest(byte[] buf, int offset, int len)

Implementar uma message digest

- Passaremos agora para o NetBeans



Sumário

- Algoritmos de *message digest*
- Aplicações comuns
- Classe *MessageDigest*
- Implementar uma *message digest*

Parceiros

- **Os seguintes parceiros tornaram JEDI™ possível em Língua Portuguesa:**