

Exercícios sobre Criptografia

1. Considere as seguintes plataformas em ambiente cloud para teste de sistemas criptográficos:

<https://www.functions-online.com/hash.html>

<http://cryptool-online.org>

https://www.tools4noobs.com/online_tools/

- a) Apresente o código ASCII, em binário, correspondente à palavra: "ANA".
- b) Apresente o código de Base64 correspondente à palavra "ANA".
- c) Apresente o código de Huffman da palavra "Mapping".
- d) Apresente o código corresponde à password "passwd" e "67YnB5e9" usando o método de encriptação MD5. Porquê que a 2ª password é mais segura que a 1ª opção?
- e) Apresente o código corresponde à password "passwd" e "67YnB5e9" usando o método de encriptação SHA1. Será mais seguro o MD5 ou SHA1?
- f) Apresente o código corresponde à password "passwd" e "67YnB5e9" usando o método de encriptação CRC32. Qual dos 3 métodos é o mais seguro?
- g) Converta o número "1023" da base 10 para a base 2.
- h) Converta o número "1024" da base 10 para a base 2. Quantos bits são usados nestes dois cenários?
- i) Converta o número "ABA12A" da base 16 para a base 2. Quantos bits são usados?
- j) Converta o número "AHL" da base 30 para a base 2. Quantos bits são usados?
- k) Converta o número "AFEFE" da base 16 para a base 2.
- l) Testa a similaridade das strings abaixo:
 - "Compra de uma casa" vs. "Comprei o carro"
 - "Compra de uma casa" vs. "Sou proprietário"
 - "Compra de uma casa" vs. "compra da Casa"Qual é a situação que apresenta maior similaridade? Porquê?
- m) Procure decifrar a mensagem original correspondente às situações abaixo usando a chave "ABC".

2e5ec6179ce5ed8ff17e514f309a2918

teste do sistema - tripledes CBC Hexa

ecf35dcfbfba82bf6f3d67a89a139ceefc9659dae52256960547a9315b805dff

aulas de segurança informática - tripledes CBC Hexa

8178674daa22e0de28431f542cb0011bf2383bf13105477f

Métodos de criptografia - Xdea CBC Hexa

2. Use o software abaixo, de forma a transmitir uma mensagem codificada entre dois colegas da sua turma.

Link: <https://pgptool.org/>