Segurança em Redes Informáticas

Miguel Magalhães
RSI
Nº: 20211031166
2022/2023

Exercícios sobre Criptografia:

1

a) Através da ferramenta do site "Cryptool-online":

ANA = 01000001 01001110 01000001

b) ANA $\xrightarrow{\text{Base64}}$ QU5B

c) Mapping $\xrightarrow{\text{Huffman}}$ 111100010111000101

d) "passwd" = 96a2173be6393254e72ffa4d6df1030a

"67YnB5e9" = 64a76c3e1f62d4129e5fe3128db01d3d

Como a primeira password apenas tem caracteres minúsculos, esta não tem a mesma segurança do que a segunda. No entanto, a segunda password já contém não só caracteres minúsculos e maiúsculos, mas também contém números e não forma uma palavra, na sua constituição.

e) "passwd" = 3027c47f903bd1bacf633b5f09f43149bb805f

"6?YnB5eq" = ?011fe336b54e5109366616 61fcd495?e35a6a50

A "MD5" é menos segura do que a "SHA1".

f) "passwd" = 456024468

"6?nYB5eq" = 318058102

O "SHA1" é o método mais seguro.

g) $1023_{(10)} = 1111111111_{(2)}$

h) $1024_{(2)} = 10000000000_{(2)}$

São usados 10 bits no primeiro e 1 bit no segundo.

i) $"ABA12A"_{(16)} = 101010111010000100101010_{(2)}$

São usados 11 bits.

j) $"AHL"_{(30)} = 10010100\,111\,011_{(2)} \rightarrow 8$ bits

k) "AFEFE" = 1010111111101111110(2) -> 16 bits

l) A última, pois, relaciona o mesmo tema: "compra" "de casa".

m)

1. Teste do Sistema -> Tripledes CBC Hexa.
2. Aulas de segurança informática -> Tripledes CBC Hexa.
3. Métodos de criptografia -> Xdea CBC Hexa.

(2) Este exercício consta na pasta enviada: "Exercício 2 - Miguel e Rui".