

## Lista 1: Segurança da Informação

### Ex 1

- a) sulydfldghsxeoldwudqsdhqqfidsulydgd
- b) MOFUZBFRZRAMTEIFBZQOZKMZOAKBFZMOFUZRZ
- c) hvvcaumqhdwthilagnarschrwrppahvvcave

### Ex 2

Assumindo  $q = \text{tamanho do alfabeto} = 26$

Para uma sequência gerada aleatoriamente, o tamanho do universo depende do tamanho da mensagem a ser cifrada ( $l$ ). Assumindo um alfabeto de 26 letras, temos:

$$\text{tam}(U) = q^l = 26^l$$

Agora, usando a lógica de repetição de chave, temos para cada tamanho de  $k$ :

1. para  $|k| = 1$ ,

$$\text{tam}(U) = q^1 = q$$

2.  $|k| = 2$ , existem itens na permutação de  $|k|=2$  cobertos pela repetição de  $|k| = 1$  como:

$$k1 := a$$

$$k2 := aa$$

$$\text{rep}(k1, 2) = aa = k2$$

por isso o valor do item (1) é subtraído.

$$\text{tam}(U) = q^2 - \text{tam}(U \text{ para } |k| = 1) = q^2 - q^1$$

3. para  $|k| = 3$ , é preciso o mesmo tratamento que o item (2)

$$\text{tam}(U) = q^3 - \text{tam}(U \text{ para } |k| = 1) = q^3 - q^1$$

4. O  $|k| = 4$  é coberto pelas repetições de (1) e (2)

$$\text{tam}(U) = q^4 - \text{tam}(U \text{ para } |k| = 2) - \text{tam}(U \text{ para } |k| = 1) = q^4 - q^2 - q$$

Escrevendo de forma genérica:

$$\text{tam}(U) = q^{|k|} - \left( \sum (q^i), \forall i \in P \right)$$

Usando apenas palavras contidas em um dicionário, esse

Uma vulnerabilidade da cifra de deslocamento é que, para uma dada chave, cada caractere da entrada é sempre cifrado com o mesmo símbolo, possibilitando ataques de frequência.

### Ex 5

A probabilidade de o adversário derrotar o sistema cairia para 0.500000000000000000054210109%

```
def check_zeros(y: [y0, y1, ..., yn | n >= 16])
  for i in 9..16:
    if y[i] == 1:
      return true
  return false
```