Lista 1: Segurança da Informação

Ex 1

a) sulydflgdghsxeolfdwudqsduhqfldsulydgd
b) MOFUZBFRZRAMTEIFBZQOZKMZOAKBFZMOFUZRZ
c) hvvcaumqhdwthilagnarsrchrwrppahvvcave

Ex 2

Assumindo q = 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:

$$tam(U) = q^l = 26^l$$

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

1. para $|k| = 1$,
$$tam(U) = q^1 = q$$
2. $|k| = 2$, existem itens na permutação de |k|=2 cobertos pela repetição de $|k| = 1$ como:

$$k1 := a$$
$$k2 := aa$$
$$rep(k1, 2) = aa = k2$$

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

$$tam(U) = q^2 - tam(Upara|k| = 1) = q^2 - q^1$$

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

$$tam(U) = q^3 - tam(Upara|k| = 1) = q^3 - q^1$$

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

$$tam(U) = q^4 - tam(Upara|k| = 2) - tam(Upara|k| = 1) = q^4 - q^2 - q$$

Escrevendo de forma genérica:

$$q^{|k|} - (\sum (q^i), \forall i \in P))$$

onde P compreende os divisores inteiros de |k| menores que |k|

Ex 3

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

Ex 4

$$p(n = 128) = 100 * 1/2 + 1/(2^{32})$$
$$p(n = 256) = 100 * 1/2 + 1/(2^{64})$$

A probabilidade de o adversário derrotar o sistema cairia para $0.50000000000000000054210109\%$

Ex 5