Lista 1: Segurança da Informação

Nome: Eder Gabriel da Trindade Félix

NrUsp: 9778515

Ex 1

Cifra de deslocamento

sulydflgdghsxeolfdwudqsduhqfldsulydgd

Cifra de substituição

MOFUZBFRZRAMTEIFBZQOZKMZOAKBFZMOFUZRZ

Cifra de Vigenere

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:

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

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

Usando apenas palavras contidas em um dicionário, esse

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

Nesse algoritmo, o conteúdo da mensagem é crifrado bit-a-bit com a saída de um gerador de números pseudo-aleatório. Geralmente a cifragem é feita pela função booleana XOR. Para garantir a segurança, o gerador deve se aproximar de uma função aleatória. Padrões na saída do gerador tornam a cifra vulnerável à criptoanálise.

Ex 5

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

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

Ex 6

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

Ex 7

No modo CTR, o processamento de um bloco é independente dos outros. Logo, o bloco no qual o bit se encontra ficará corrompido, mas o resto da mensagem estará legível. No CBC, a descriptografação dos blocos ocorre em sequência, com o processamento de um dados bloco dependendo do resultado do anterior (com exceção do primeiro). Logo, a corrupção de um único bit impede a decodificação da mensagem inteira.

Ex 8

Não, pois a cifragem de cada bloco é determinística: se houverem dois blocos idênticos na mensagem, eles gerarão o mesmo bloco de cifra, o que torna o algoritmo vulnerável à criptoanálise.