Segurança da Informação - Lista 1
Prof. Márcio Moretto Ribeiro

Mirela Mei - 11208392

1. **Mensagem: privacidadepublicatranparenciaprivada**

    a) **cifra de deslocamento com k = 3**

    c = SULYDFLGDGHSXEOLFDWUDQUSDUHQFLDDULYDGD

    b) **cifra de substituição com a seguinte permutação de letras: ZEBRASCDFGHIJKLMNOPQTUVWXY**

    c = MOFUZBFRZRAMTEIFBZQOZKPMZOAKBFZMOLUZRZ

    c) **cifra de Vigenère com chave senha**

    c = HVVCAUMQHDWTHILAGNARSRFWAJIAJISTEPVSHN

    m = 5 7 8 21 0 2 8 3 0 3 4 15 20 1 11 8 2 0 19 17 0 13 17 15 0 17 4 13 2 8 0 15 17 8 21 0 3 0

    c = 18 20 11 24 3 5 11 6 3 6 7 18 23 4 14 11 5 3 22 20 3 16 20 18 3 20 7 16 5 11 3 18 20 11 24 3 6 3

2. **Calcule o tamanho do universo das chaves em uma cifra de Vigenère da forma como usada normalmente (escolhendo uma palavra) e na forma como apresentamos formalmente (sequência aleatória com tamanho fixo l)?**

    Considerando a palavra FOME, tem-se:
    O tamanho do universo da chave é 26^4 = 456976
    Já o universo de uma chave aleatória de tamanho fixo ℓ é 26^ℓ

3. **Mostre que a cifra de deslocamento não garante sigilo perfeito**

É possível demonstrar que a cifra de deslocamento não garante sigilo perfeito por meio de um exemplo.
Seja π<gen, E, D> um sistema de criptografia de deslocamento.
Criptografando a mensagem OVO e utilizando a cifra de deslocamento com k = 4 obtemos a mensagem SZS.
Pr(C = c| M = mo) = 1/26.1.1 = 0
Porém, não é possível fazer o processo inverso de descriptografar a cifra SZS e obter a mensagem OVO, o que quebra o sigilo perfeito.

4. **Descreva com suas palavras o sistema de criptografia de cifra de fluxo. O que precisamos assumir para que esse sistema seja seguro? Em que sentido podemos considerá-lo seguro?**

   O sistema de criptografia de cifra de fluxos consiste em definir uma sequência aleatória de bits chamada semente e, a partir dessa semente, gerar uma sequência maior de bits que será usada para encriptar a mensagem utilizando o XOR. Para gerar essa sequência maior de bits utilizamos um gerador de números pseudoaleatórios (PRG). Para assumir que esse sistema é seguro, é necessário assumir que não é possível distinguir as sequências de bits produzidas por um PRG de uma sequência realmente aleatória e para isso é possível utilizar testes distinguidores.
   O sistema é seguro para ataques ciphertext only.

5. **Considere um sistema Π seguro contra ataques ciphertext only cujo parâmetro de segurança tem 128 bits (n = 128) e um adversário polinomial que derrota o sistema com probabilidade 1/2 + 1/(2^n/4). Com que probabilidade esse adversário derrotaria o sistema se dobrassemos n?**

   Considerando n=256, tem-se:
   12+12n/4=12+12256/4 = 12+1264 = 0.5
   Portanto, a probabilidade é de 0.5.

6. **Sejam y0, y1, y2 . . . os bits gerados pelo algoritmo RC4. É possível mostrar que para uma distribuição uniforme de sementes e vetores iniciais, a probabilidade dos bits y9, . . . , y16 serem todos iguais a 0 é 2/256 . Mostre como construir um algoritmo eficiente D capaz de distinguir as sequências de bits produzidas pelo RC4 de uma sequência realmente aleatória.**

Seja D um distinguidor que recebe uma sequência m, onde |m|>=16. D retorna 1 se os bits da posição 8 até 16 forem 0 ou retorna 0 caso contrário.
Portanto:

P[D(RC4(s))=1]-P[D(s)=1]
2/256 - 1/256 = 1/256

7. **Suponha que um bit em uma cifra tenha sido alterado por um erro. Qual o efeito disso na mensagem descriptografada caso a cifra tenha sido produzida usando o modo Ctr? E no caso de ter sido produzida usando o modo CBC?**

   Utilizando o modo CTR somente o bloco do bit alterado seria perdido. Já no modo CBC, não seria mais possível recuperar a mensagem, pois os blocos subsequentes também seriam afetados

8. **Suponha que f seja uma função pseudo-aleatória com chave e blocos ambos de 128 bits e considere o seguinte sistema: .....**
   Esse sistema é seguro? Por que?

   O sistema não é seguro, pois é possível escolher 2 mensagens de mesmo tamanho, a primeira com blocos iguais e a segunda com blocos diferentes. Dessa forma, ao ver a cifra gerada, será possível distinguir qual mensagem originou cada uma das cifras.