Vitor Caetano = 9276999

Lista 1 - Segurança da Informação

1.

privacidadepublicatranparenciaprivada

a) deslocamento: k = 3:
   resultado: sukyãekêâêfswdokeãvuãõsãufõekãsukyãêã
b) substituição: ZEBRASCDFGHIJKLMNOPQTUVWXY
   resultado: MOFUZBFRZRAMTEIFBZQOZKMZOAKBFZMOFUZRZ
c) Vigenére: senha
   resultado: hvvcaumqhdwthilagnarsrchrwrppahvvcave

2.

Somatório das permutações de bytes: 256^N X K sendo N o número de chaves e K o tamanho da Chave.

Em uma chave aleatória teríamos o K de tamanho variável e o N aumentaria a cada nova chave, o que aumentaria ainda mais o universo de chaves da cifra de Vigenére.

3. O sigilo perfeito é garantido quando o espaço da mensagem, o espaço da chave e o espaço do texto são iguais. Pois assim não é possível obter mais do que palpites sobre a cifra.

Numa cifra de deslocamento, é possível detectar padrões gerados pelo deslocamento da chave. E isto compromete o sigilo da cifra, pois se tornam pistas sobre o deslocamento entre as posições das letras.

4. Cifras de fluxo geram uma sequência de bits que será usada como chave (keystream) a partir de uma chave inicial. A encriptação ocorre pela combinação do texto plano com a keystream através de operações XOR. Na cifra de fluxo, não é necessário ter um bloco para cifrar. As cifras de fluxo convertem um byte de cada vez. Aplicar uma série de testes estatísticos na sequência gerada para tentar distingui-lo de uma sequência aleatória. O objetivo do teste é distinguir as sequências de bits produzidas por um PRG de uma sequência realmente aleatória.

5. ½ + $1/2^{128/4}$ = ½ + $1/2^{32}$ é a probabilidade de derrota pelo adversário. Dobrando-se o n seria ½ + $1/2^{64}$ o que reduziria considerávelmente a probabilidade de derrota pelo adversário.

6. O RC4 funciona pela cifra em stream, logo para distinguir as sequências de bits produzidas pelo RC4 de uma sequência aleatória deveria ter probabilidade 1/256 para todos os bits, inclusive para zero. Medindo-se a probabilidade da sequência de bits produzida pelo RC4 e verificando-se com a distribuição uniforme de todas as probabilidades, conseguimos saber a distinção entre as distribuições de uma aleatoriedade real e uma pseudo aleatoriedade.

7. No modo CTR haverá apenas um byte com erro e o resto da cifra será descriptografada normalmente. Já no modo CBC, a cifra poderá ter problemas de interpretação em todo o bloco a diante, pois neste algoritmo há a limitação de que o algoritmo precisa processar os blocos em sequência.

8. A segurança da criptografia simétrica é baseada no quão difícil é saber a chave correspondente por simplesmente chute. Por exemplo, uma chave de 128-bits pode levar bilhões de anos até alguém conseguir adivinhar usando um computador comum. Normalmente, quanto maior a chave, maior a segurança envolvida. Como os blocos trabalham em tamanho fixo e as mensagens podem variar de tamanho, são adicionados alguns bytes ao final para que ela fique com tamanho múltiplo desse bloco.
O sistema é seguro pois é baseado no tamanho da chave de 128 bits que é um tamanho razoável para evitar quebras por força bruta.