Lista 1: Segurança da Informação

Prof. Márcio Moretto Ribeiro

28 de setembro de 2022

Exercício 1: Considere a seguinte mensagem:

`privacidadepublicatranparenciaprivada`

- Criptografe essa mensagem utilizando a cifra de deslocamento com $k = 3$.
- Criptografe essa mensagem utilizando a cifra de substituição com a seguinte permutação de letras: `ZEBRASCDFGHIJKLMNOPQTUVWXY`
- Criptografe essa mensagem utilizando a cifra de Vigenère com chave `senha`.

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

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

Exercício 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?

Exercício 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 $\frac{1}{2} + \frac{1}{2^{n/4}}$. Com que probabilidade esse adversário derrotaria o sistema se dobrassemos n?

Exercício 6: Sejam $y_0, y_1, y_2 \ldots$ os bits gerados pelo algoritmo RC4. É possível mostrar que para uma distribuição uniforme de sementes e vetores iniciais, a probabilidade dos bits $y_9, \ldots, y_{16}$ serem todos iguais a 0 é $\frac{2}{256}$. Mostre como construir um algoritmo eficiente D capaz de distinguir as sequências de bits produzidas pelo RC4 de uma sequência realmente aleatória.

Exercício 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?

Exercício 8: Suponha que f seja uma função pseudo-aleatória com chave e blocos ambos de 128 bits e considere o seguinte sistema:

1. Seleciona aleatoriamente duas sequência de 128 bits, a chave k e o vetor inicial IV
2. Divide a mensagem m em blocos de 128 bits: $m_0, m_1, \ldots, m_{n-1}$ (podemos supor que $|m|$ é múltiplo de 128).
3. A cifra $c = c_0||c_1||\ldots||c_{n-1}$ é tal que $c_i = m_i \oplus f_k(IV)$ para $i = 0, ..., n-1$
4. Para descriptografar fazemos $c_i \oplus f_k(IV)$ para $i = 0, \ldots, n-1$.

Esse sistema é seguro? Por que?