Prova Substitutiva

Segurança da Informação

Prof. Márcio Moretto Ribeiro

2019

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

Esse sistema é seguro? Por que?

Exercício 3: Seja f uma função pseudo-aleatória e considere o sistema $\Pi = \langle Gen, E, D \rangle$ uma cifra de bloco que aplica f no modo contador. Suponha que Alice e Bob compartilham uma chave secreta *k*. Considere os seguintes cenários:

1. Alice enviar E(k, m) para Bob que descriptografa usando a chave *k*
2. Açice gera um checksum H(m) da mensagem e envia $H(m) || m$ para Bob que pode verificar o checksum antes de ler a mensagem

Algum desses cenários garante que a mensagem lida por Bob é idêntica a mensagem que foi enviada por Alice? Por que? Caso nenhum dos cenários garanta isso, descreva como poderíamos fazê-lo.

Exercício 4: Descreva esquematicamente o protocolo de Diffie-Hellman. Para que usamos esse protocolo? O que precisamos assumir para garantir que ele seja seguro?