Lista 2: Segurança da Informação

Prof. Márcio Moretto Ribeiro

17 de Junho de 2019

Exercício 1: 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. Alice 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 2: Explique com suas palavras a definição de segurança de hashes. Por que o SHA-1 não é mais considera segura?

Exercício 3: Descreva um ataque força-bruta contra o protocolo de Diffie-Hellman. Em termos assintóticos em relação ao tamanho da entrada, qual é o consumo de tempo deste ataque?

Exercício 4: Mostre que para qualquer $n \in \mathbb{Z}$ a estrutra $\langle \mathbb{Z}_n^\star, \cdot \rangle$ é um grupo.

Exercício 5: Explique com suas palavras o que é uma autoridade certificadora e qual sua importância para garantir a segurança na comunicação.