Prova 1

Segurança da Informação

Professor Márcio Moretto Ribeiro

08 de Maio de 2019

1. Suponha que você tenha recebido um texto com diversas páginas criptografado usando a cifra de substituição. Descreva com suas palavras os passos que você seguiria para decifrar essa cifra, ou seja, para extrair dela o texto original.

2. Descreva, utilizando um diagrama se necessário, o sistema One Time Pad (OTP). É possível utilizar a estratégia descrita na resposta do Exercício 1 para decifrar uma cifra criptografada com OTP? Enumere duas limitações deste sistema de criptografia

3. Descreva uma vantagem prática e uma desvantagem teórica do uso de uma cifra de fluxo em relação ao OTP.

4. Descreva, utilizando um diagrama se necessário, o modo Cipher Block Chaining (CBC) de aplicação de uma cifra de bloco. Supondo que a cifra de bloco seja uma permutação pseudo-aleatória, descreva o modelo de ameaças contra qual esse sistema é seguro.