Exercícios sobre Criptografia Simetrica

Exercício 1

Criptografia. Uma mensagem binária é transmitida usando o esquema OTP.

a) Se o texto cifrado for **10010111** e a chave for **01100111**, qual foi a mensagem transmitida.

b) Um atacante intercepta 2 mensagens criptografadas com o mesmo OTP: **C1** = **1011** e **C2** = **1101**. Se ele sabe que a primeira mensagem transmitida foi **M1** = **0001**, qual foi a segunda?

c) Comente como é possível impedir que o atacante tenha sucesso no cenário anterior.

Exercício 2

Tamanho da chave. Um algoritmo de criptografia de bloco convencional usa chaves de 128 bits.

a) Se a chave for selecionada aleatoriamente, qual é a probabilidade de adivinhar a primeira tentativa?

b) Se um invasor tiver a capacidade de testar 10^6 chaves por segundo, quanto tempo levará, em média, para encontrar a chave usando força bruta.

Exercício 3

Ataque ao modo ECB. O seguinte fragmento de mensagem é criptografado com um algoritmo de cifra de bloco:

N.1 Pagar o Saul 10000000 reais, 10, para White,

O caracteres da mensagem (incluindo espaços) são codificados usando 8 bits. O algoritmo criptógrafa blocos de 128 bits.

a) Quantos blocos devem ser processados pelo algoritmo de criptografia?

b) Se um atacante captura a mensagem criptografada e troca o segundo bloco criptografado com o terceiro antes de enviá-lo ao destinatário, qual será a mensagem descriptografada?

c) O que acontece se, em vez de usar o modo ECB, o CBC for usado.

Exercício 4

Troca de chaves. Em um aplicativo em que N usuários precisam se comunicar com segurança usando criptografia de chave simétrica, quantas chaves devem ser trocadas?

a) por um usuário,

b) no total.

c) Se um KDC for usado, quantas chaves devem ser trocadas usando um canal seguro alternativo?