Exercício para Prova 2

prof. Ricardo Felipe Custódio

18 de outubro de 2016

1. Considere que você deseja cifrar e decifrar mensagens de até 6 bits usando o algoritmo RSA.
   (a) Nesse cenário, gere um par de chaves RSA, onde o expoente público deve ser 3;
   (b) Usando a chave privada, cifre a mensagem $M = 5$.
2. Considere o algoritmo de acordo de chaves de Diffie-Helamnn (DH) e seja $p = 97$ o número primo parâmetro global do algoritmo.
   (a) Sabendo que p tem 32 raízes primitivas e uma delas é $r_1 = 5$, determine outra (diferente de 2) raíz primitiva para uso nesse protocolo. Seja essa outra raiz r_2;
   (b) Usando os parâmetros públicos p e r_2 e sabendo que as chaves secretas de Alice e Beto são $X_A = 5$ e $X_B = 7$, respectivamente, proceda ao acordo de chaves.
3. Prova que a estrutura de Horst Feistel é inversível
4. Sobre o Blowfish
   (a) Descreva a cifra
   (b) Compare-o com o DES
5. Utilizando o DES Simplificado
   (a) Usando chave k = 20, cifre a mensagem M = 12;
   (b) Determine o efeito avalanche do DES-S. Considere cifrar 2 vezes o SDES e diga como proceder para determinar o valor médio.
6. Compare o modo de operação contador com os demais modos de operação que estudamos, em termos de:
   (a) Tipo de cifragem (bloco ou em cadeia)
   (b) Atraso
   (c) Comprometimento de 1 bit do texto cifrado
   (d) Paralelização do processo de ciframento e deciframento
   (e) Aplicações a que se destina