TERCEIRA LISTA DE EXERCíCIOS

Criptografia e Segurança de Redes – 01-2015

Disponibilizada em 20/05/2016 – A ser entregue em 14/06/2016

1. Escreva um programa que implemente o Gerador de Números Pseudo-Aleatórios utilizado no cifrador de fluxo RC4. Em seguida faça o download da suite de testes para geradores de números pseudo-aleatórios do NIST e teste a saída do seu gerador RC4 usando esta suite de testes. O código (já pronto e testado) e o manual do usuário desta suite de testes podem ser encontrados no URL seguinte:

   http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

2. Implemente o algoritmo de Miller-Rabin para determinar se um dado número ímpar n é primo ou não.

   O seu programa tomará como entradas o número n, o qual se deseja determinar se é primo ou não, e o número m de vezes que um inteiro a, $1 < a < n-1$, deverá ser escolhido pelo seu programa (aleatória e automáticamente) para rodar o algoritmo.

   A saída do programa deverá dizer:

   (a) Que o número é composto; ou
   (b) Que o número é primo com probabilidade p.