Instituto Politécnico de Beja
Escola Superior de Tecnologia e Gestão

Curso de Engenharia Informática
Disciplina de Segurança em Redes de Comunicação

Projecto de criptografia aplicada

Ano lectivo de 2007/08, Primeiro semestre

Título: ***Desenvolvimento de um programa de cifra baseado num PRNG***

Objectivo

Pretende-se com este projecto que os alunos desenvolvam um programa que cifre ficheiros de entrada em qualquer formato. O programa deverá funcionar em ambiente linux e em ambiente Windows e fazer uso da biblioteca GMP – *The GNU Multiple Precision Arithmetic Lyibrary*.

Descrição

1. O programa deve receber como parâmetros de entrada o nome do ficheiro a cifrar ou decifrar e o nome do ficheiro de saída correspondentemente decifrado ou cifrado. A sintaxe de invocação do programa deverá ser portanto:

nomedoprograma -<c|d> file_in file_out

2. O processo de cifra deve recorrer a um gerador de números pseudo-aleatórios (PRNG). Este PRNG deve ser validado recorrendo à bateria de testes estatísticos Diehard e aos seguintes testes a realizar por programas que os alunos deverão desenvolver: Relação entre zeros e uns; Função de distribução; Auto-correlação; Correlação-cruzada; Complexidade.

3. O programa de cifra deverá poder processar o ficheiro a cifrar de forma parametrizada, variando entre blocos deste 8, 16, 32, 64, 128, 256 e 512 bits. O ficheiro a cifrar deverá ser múltiplo de 8 bits, podendo opcionalmente os alunos contornar este problema.

Avaliação

Os alunos deverão entregar um pequeno relatório técnico impresso em papel, para apreciação juntamente com a defesa do projecto. Nesse relatório deverão incluir os testes efectuados ao PRNG, e a avaliação do programa de cifra relativamente ao seu tempo de execução e memória ocupada (complexidade computacional) para os vários modos de parametrização possíveis e para diversas dimensões dos ficheiros a processar.
Os gráficos podem ser obtidos recorrendo ao simulador gnuplot disponível na distribuição cygwin entregue aos alunos.

Além do referido relatório técnico os alunos deverão entregar ainda um cd com a seguinte estrutura de directórios, onde o carácter 'X' deverá ser substituído pelo número do respectivo grupo:

```
\projcry2007081s\grupoX\
\projcry2007081s\grupoX\source\
\projcry2007081s\grupoX\release\
\projcry2007081s\grupoX\report\
```

Na directoria `grupoX` deverá estar um pequeno ficheiro denominado `grupoX.txt`, contendo o nome completo e número de todos os alunos do grupo X. Note novamente que deverá sempre substituir o carácter 'X' pelo número do respectivo grupo.
Na directoria source deverão estar todos os ficheiros fonte do projecto.
Na directoria release deverá estar o ficheiro executável do projecto.
Na directoria report deverá estar uma cópia em formato editável e outra em formato pdf do relatório técnico do projecto, e ainda os testes realizados.

Prazos e Datas

Prazo de entrega do enunciado relatório: 6 de Dezembro

Prazo de entrega do relatório e do CD: 17 de Janeiro

Boa Sorte !