Universidade Federal do Rio Grande do Norte - UFRN
Centro de Ensino Superior do Seridó - CERES
Departamento de Ciências Exatas e Aplicadas - DCEA

Curso: Bacharelado em Sistemas de Informação
Disciplina: BSI2402 – Auditoria e Segurança de Sistemas de Informação
Professor: João Borges
Data: 01 de setembro de 2011

Atividade em Dupla

Laboratório de Criptografia Simétrica

ATENÇÃO 1: Só serão aceitos trabalhos em **Dupla** ou **Individual**, mais do que 2 participantes invalidará o trabalho;

ATENÇÃO 2: Não serão permitidos plágios entre os grupos, sendo punidos, ambos os grupos que tiverem seus trabalhos iguais, com nota 0 (zero).

1. Esta atividade consiste na implementação do algoritmo de criptografia simétrica DES (*Data Encryption Standard*):
   (a) Processo de cifragem
   (b) Processo de decifragem
2. A implementação deverá seguir o algoritmo DES, descrito nas seguintes fontes:
   - Site NumaBoa
     - *http://www.numaboa.com/criptografia/bloco/313-des2?showall=1*
   - Artigo *The DES Algorithm Illustrated*
     - *http://www.box.net/shared/static/vhgipu600g.pdf*
3. Os resultados da criptografia podem ser testados no seguinte endereço:
   - Testing DES
     - *http://www.tero.co.uk/des/test.php*
4. A implementação deverá, no mínimo, ser capaz de receber e en/decriptar um bloco de 64 bits, juntamente com uma chave de 64 bits.
5. Exemplo de Mensagem:

```
Texto:    c        a        r       a        m        e        l       o
Hexa:    63       61       72      61       6d       65       6c      6f
Bin:  01100011 01100001 01110010 01100001 01101101 01100101 01101100 01101111
```

6. Exemplo de chave:

```
Chave:    a        b        c        d        e        f        g        h
Hexa:    61       62       63       64       65       66       67       68
Bin:  01100001 01100010 01100011 01100100 01100101 01100110 01100111 01101000
```

7. Este texto de entrada gerará o texto cifrado:

```
0xc994d7f34d656df2
```

8. A linguagem de programação da implementação é de livre escolha das duplas.

9. O código-fonte e sua execução serão analisadas e testadas pelo professor, podendo este levantar questionamentos à dupla quanto aos detalhes de sua implementação.

10. Não será permitido utilizar funções prontas da linguagem para en/decriptar as mensagens. As duplas deverão efetuar as operações conforme descritas no algoritmo DES.

11. Os códigos-fonte dos algoritmos deverão ser enviados por um dos integrantes da dupla pelo SIGAA, até a data estabelecida da tarefa cadastrada no sistema.