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: 08 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 e análise do algoritmo de criptografia assimétrica RSA (*Rivest, Shamir, Adleman*):

   (a) Processo de cifragem

   (b) Processo de decifragem

   (c) Criptanálise do algoritmo

2. A implementação deverá ser baseado no algoritmo RSA apresentado em sala de aula, e também descrito nas seguintes fontes:

   - Site NumaBoa
     - *http://www.numaboa.com.br/criptografia/chaves/350-rsa?showall=1*
   - Criptografia RSA (Laboratório de Matemática)
     - *http://www.uam.es/personal_pdi/ciencias/pangulo/doc/laboratorio/b6RSA.html*

3. A primeira parte da implementação consistirá em um gerador de chaves pública e privada, a serem utilizadas para en/decriptar uma determinada *string*.

   Como um teste inicial, utilizar os seguintes valores, conforme apresentados na aula teórica:

   - $p = 17$
   - $q = 11$
   - $e = 7$

4. A implementação deverá receber como entrada uma *string* e en/decriptá-la utilizando o par de chaves pública e privada geradas com o gerador.

5. A *string* passada deverá ser dividida em blocos para serem criptografados. O tamanho de cada bloco poderá corresponder ao tamanho (em inteiro decimal) de cada caracetere do bloco. Lembrando que $0 < m < n$.

6. Exemplo de cifragem:

Texto:	c	a	r	a	m	e	l	o
Dec:	99	97	114	97	109	101	108	111
Cifra:	176	92	126	92	131	84	48	155

7. Após a implementação, modificá-la de forma a considerar meios para melhorar a segurança do texto cifrado, dificultando o processo de criptanálise:

   - Quanto às chaves geradas, encontrar meios de geração de chaves mais seguras, principalmente quanto à escolha dos valores utilizados em sua geração (p, q, e);
   - Quanto à divisão dos blocos de cifragem, definir novos meios de divisão de forma a dificultar ataques qaunto à redundância das informações, por meio da análise da frequência da repetição de caracteres.

8. Após a melhoria da implementação, descrever em formato de relatório quais as escolhas tomadas e demonstrar que essas medidas aumentaram a segurança.

   - A demonstração da vulnerabilidade das chaves simples, que foram tomadas como exemplo inicial, pode ser realizada por meio da quebra destas chaves, através da fatoração do valor de n, encontrando os valores p e q, e, consequentemente, encontrando o valor de d.
   - A demonstração do aumento da segurança do processo de encriptação do algoritmo melhorado poderá ser realizada por meio da demonstração do tempo que será necessário para fatorar o valor de n, para obter os valores de p e q.

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

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

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

12. 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.