Trabalho de Segurança e Auditoria de Sistemas

- Data de entrega: 19/11
- Trabalho em grupo de no mínimo 3 e máximo 4 alunos
- Entregar: documentação e código fonte

1 Objetivo

Comparar o desempenho de duas formas de criptografias: simétrica e assimétrica. O trabalho deve demonstrar a diferença, se existir, de desempenho em termos de tempo computacional, da criptografia simétrica versus assimétrica, em um caso específico.

2 Projeto

A ideia é medir o tempo para encriptar e decriptar usando criptografia simétrica e assimétrica variando o tamanho das mensagens e o tamanho das chaves. Posteriormente, fazer uma análise estatística dos tempos medidos. A implementação deve ser em uma linguagem de programação escolhida pelo grupo.

2.1 Pesquisa

Pesquisar as bibliotecas disponíveis que implementam o algorítimo AES de criptografia simétrica e outra que implementa o algorítimo RSA de criptografia assimétrica.

2.2 Avaliação de desempenho

- **Definir as mensagens**: escolher uma mensagem de texto claro de tamanho m. Criar mensagens de tamanho: 2m, 4m e 8m, com base na mensagem m.
- **Comprimento das chaves**: para o AES utilizar 128 bits e 256 bits e o RSA 512 bits e 1024 bits.
- **Obter os tempos em microsegundos**: tempo, T^E_{AES}, para cifrar com a chave simétrica; tempo, T^D_{AES}, para decifrar com a chave simétrica; tempo, T^E_{RSA}, para cifrar com a chave pública; e tempo, T^D_{RSA}, para decriptar com a chave privada.
- **Monitor**: implementar o monitor para obter os tempos de cada operação. Inserir cuidadosamente os monitores de tempo no código de maneira que o tempo medido seja somente do procedimento de encriptação e decriptação, não medir os tempos de leitura do arquivo, criação das chaves, etc.
- **Controle do ambiente**: controlar o ambiente de teste. As medidas de tempo devem sofrer a mínima interferência possível. Portanto, deve-se evitar executar aplicações em paralelo durante as medições dos tempos. O ideal é manter o mesmo ambiente (softwares e hardware) para obter uma comparação justa entre AES e RSA.
- **Repetições:** repetir a medida 15 vezes para cada combinação, calcular a média e preencher a tabela 1 para os valores calculados:

Tabela 1: Tempo médio das operações de encriptação e decriptação para o AES e RSA

Algoritmo:	AES				RSA			
Chave:	128		256		512		1024	
Mensagem (MB)	Cifrar	Decifrar	Cifrar	Decifrar	Cifrar	Decifrar	Cifrar	Decifrar
m =								
2m =								
4m =								
8m =								

3 Entrega do projeto

O trabalho deve ser entregue via moodle. Somente um membro do grupo deve fazer *upload* dos arquivos. A entrega do projeto deve conter:

- Código fonte e descrição de compilação e execução (zip ou tar.gz);
- Planilha com os valores medidos
- Documentação do projeto (pdf), deve conter, pelo menos:
  - Descrição do ambiente de teste: configuração do hardware (cpu, memória, hd, etc). Espaço de livre de memória, uso do processador, velocidade de leitura do disco, sistema operacional, etc. (as configurações que podem influenciar no resultado);
  - Tabela e gráficos dos resultados;
  - Detalhamento dos procedimentos de implementação e avaliação de desempenho.

É importante o grupo dar atenção especial a documentação do projeto. O formato da documentação é livre, contudo deve ser objetivo, bem escrito e estruturado. A documentação pode conter diagramas, figuras, trechos de código, tabelas, printscreen etc.

A avaliação do trabalho será, principalmente, com base na documentação, portanto, a descrição da implementação, do ambiente de teste, da avaliação de desempenho e dos resultados das medidas devem ser claros.