DEPARTAMENTO DE MATEMÁTICA

Licenciatura: Informática - Redes e Multimédia

Segurança e Gestão em Redes
Ano Lectivo 2012/2013

Trabalho Individual 1

Objectivos:

Este trabalho de projecto individual tem por objectivo a aplicação e praticabilidade dos conteúdos ministrados nas aulas teóricas e práticas da cadeira de Segurança e Gestão de Redes.

É pretendido que os alunos apliquem os conhecimentos científicos adquiridos e possam construir pequenos shell scripts, em bash.

Proposta de Trabalho:

No âmbito de segurança – criptografia simétrica e assimétrica -, por enumeras vezes necessitamos de gerir chaves assimétricas, distribuir chaves simétricas, assinar/verificar assinatura de chaves simétricas.

Neste sentido, pretende-se que o aluno construa uma pequena aplicação em shell script que permita ao utilizador gerir as suas chaves e realizar operações de segurança sobre documentos a enviar e/ou verificar a chave simétrica recebida de outro interlocutor da comunicação.

Descrição do Trabalho:

Pretende-se que o aluno concretize uma aplicação de shell script (em bash), de nome **criptoSGR** de funcionalidades descritas de seguida.

O aluno terá de utilizar os comandos necessários do openssl para realizar as funcionalidades pretendidas, onde os mesmos serão embebidos em shell script. Para um melhor grafismo da aplicação a realizar, o aluno utilizará o comando dialog e/ou Xdialog.

criptoSGR

FUNÇÂO

Executa a aplicação de gestão de chaves e implementação de segurança de documentos.

SINTAXE

./criptoSGR

DESCRIÇÃO

A aplicação **criptoSGR** ao ser executada apresentará o seguinte **Menu Principal**:

- Criar Par de Chaves Assimétricas
- Encriptação de Mensagens por Cifra Simétrica
- Distribuição da Chave Simétrica
- Desencriptação de Mensagens por Cifra Simétrica

Após a execução de qualquer opção do Menu Principal a aplicação terá de retornar ao mesmo.

Seguidamente é apresentado a(s) funcionalidade(s) a implementar por cada opção:

- Criar Par de Chaves Assimétricas

Ao seleccionar esta opção será criado para o utilizador o par de chaves RSA. Será solicitado ao utilizador o nome para as suas chaves (ex:. JoaquimMotaBicicleta) e a localização de armazenamento para as mesmas (ex.: /home/JoaquimMotaBicicleta).

Após a introdução dos dois parâmetros, a aplicação gerará dois ficheiros que serão armazenados na localização indicada. Os ficheiros serão o par de chaves gerados pelo algoritmo RSA, onde o seu nome terá o seguinte formato: Nome_PrKey_RSA.pem e Nome_PubKey_RSA.pem, para a chave privada e chave pública, respectivamente

(ex.: JoaquimMotaBicicleta_PrKey_RSA.pem
JoaquimMotaBicicleta_PubKey_RSA.pem).

- Encriptação de Mensagens por Cifra Simétrica

Esta opção servirá para encriptar por cifra simétrica a mensagem a enviar. Assim, será preparado um criptograma que possa navegar numa rede de computadores, o qual será o resultado de um dos seguintes algoritmos de cifra simétrica: DES, DES3, AES256 e Blowfish.

É necessário que o utilizador forneça os dados necessários para a criação correcta do criptograma. O criptograma será armazenado numa localização especificada pelo utilizador.

- Distribuição da Chave Simétrica

Esta opção servirá para preparar um criptograma que possa navegar numa rede de computadores, o qual conterá a chave simétrica utilizada na opção "Encriptação de Mensagens por Cifra Simétrica", e que serviu para encriptar a mensagem pelo algoritmo de cifra simétrica seleccionado.

É necessário que o utilizador forneça os dados necessários para a criação correcta do criptograma. O criptograma final será armazenado numa localização especificada pelo utilizador.

- Desencriptação de Mensagens por Cifra Simétrica

Esta opção permite desencriptar uma mensagem previamente encriptada pela opção "Encriptação de Mensagens por Cifra Simétrica". Para tal, o utilizador terá de possuir dois criptogramas: um com a mensagem cifrada e outro com a chave simétrica. Após a abertura correcta dos criptogramas a mensagem, em *plaintext*, deverá ser apresentada ao utilizador.

Notas:

O *frontend* da aplicação (janelas de shell script) será utilizando o comando dialog e/ou Xdialog.

– Instalação do dialog e Xdialog (em root):

fedora: yum install dialog Xdialog

ubuntu: apt-get install dialog Xdialog

- Referências Bibliográficas:

http://linuxgazette.net/101/sunil.html

http://www.linuxjournal.com/article/2807?page=0,0

http://www.linuxjournal.com/article/2460

http://linux.die.net/man/1/dialog

Entrega e Avaliação:

- A data limite de entrega do trabalho é dia 15 de outubro de 2012, às 23:55 H.
- O aluno, até à data limite de entrega do trabalho, terá de entregar, na plataforma Moodle, na actividade "Envio do Trabalho Individual Nº 1", um ficheiro comprimido (de formato à escolha), contendo o(s) ficheiro(s) de shell script e um ficheiro de texto com a sua auto-avaliação.
- Não serão aceites trabalhos entregues por mail nem por qualquer outro meio não definido nesta secção.
- Alguns dos parâmetros de avaliação são: funcionalidade, estrutura, desempenho, algoritmia, comentários e clareza do código.
- O plágio implica exclusão do trabalho.