UNIVERSIDADE DOS AÇORES
DEPARTAMENTO DE MATEMÁTICA

Informática – Redes e Multimédia
Disciplina: Segurança e Gestão de Redes

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 digital de documentos e criar/verificar resumos criptográficos seguros.

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 ou verificar a autenticidade e integridade de documentos recebidos de terceiros.

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 poderá utilizar o comando dialog e/ou Xdialog, onde beneficiará de uma majoração.

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
- Distribuição de Chave Simétrica
- Encriptação de Mensagens
- Criar Resumo Criptográfico Seguro
- Assinar Digitalmente/Criar Envelope Digital do Ficheiro
- Verificar Assinatura/Envelope/ResumoCriptográfico Seguro

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, o utilizador terá de seleccionar o algoritmo (RSA ou DSA) para criação do seu par de chaves. Também terá de introduzir o nome para as suas chaves (ex:. JoaquimMotaBicicleta) e a localização de armazenamento para as mesmas (ex.: /home/JoaquimMotaBicicleta).

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

(ex.: JoaquimMotaBicicleta_PrKey_Alg.pem

JoaquimMotaBicicleta_PubKey_Alg.pem).

- Distribuição de Chave Simétrica

Esta opção servirá para preparar um criptograma que possa navegar numa rede de computadores, o qual conterá a chave simétrica utilizada num 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.

- Encriptação de Mensagens

Esta opção servirá para preparar 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.

- Criar Resumo Criptográfico Seguro

Ao seleccionar esta opção, o utilizador terá de seleccionar MAC ou HMAC. Caso opte por MAC, terá de utilizar um dos algoritmos indicados na opção anterior.

O resumo criptográfico seguro será armazenado numa localização especificada pelo utilizador e a chave utilizada na sua criação terá de ser preparada para distribuição.

- Assinar Digitalmente/Criar Envelope Digital do Ficheiro

Esta opção permite criar a assinatura digital ou o envelope digital de um dado ficheiro, especificado pelo utilizador. O resultado da operação será armazenado na localização onde se encontra o ficheiro a assinar.

- Verificar Assinatura/Envelope/ResumoCriptográfico Seguro

Ao seleccionar esta opção o utilizador terá de escolher a acção pretendida e fornecer os dados necessários à acção.

<u>Bónus</u>:

O aluno pode optar por realizar todo ou parte do *frontend* da aplicação com recurso a janelas de shell script, utilizando o comando dialog e/ou Xdialog. A implementação deste bónus terá um valor máximo de 4 valores, o qual dependerá da sua implementação e funcionalidade.

– 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 13 de Novembro de 2011, 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 de formato zip ou rar, 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.
- O plágio implica exclusão do trabalho.
- Alguns dos parâmetros de avaliação são: funcionalidade, estrutura, desempenho, algoritmia, comentários, clareza do código.