DEPARTAMENTO DE MATEMÁTICA

Licenciatura: Informática - Redes e Multimédia

Segurança e Gestão em Redes
Ano Lectivo 2012/2013

Trabalho Individual/Grupo 2

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 – assinatura digital e sínteses seguras -, por enumeras vezes necessitamos de comunicar de forma segura, garantido confidencialidade, autenticidade e integridade.

Neste sentido, pretende-se que o aluno/grupo de trabalho desenvolva mais opções de segurança na aplicação ***criptoSGR*** permitam ao utilizador garantir as propriedades de segurança acima referidas.

Descrição do Trabalho:

Pretende-se que o aluno/grupo de trabalho continue a desenvolver a aplicação de shell script (em bash) ***criptoSGR*** com as funcionalidades descritas de seguida.

Para o grupo de trabalho a aplicação base (aplicação desenvolvida no Trabalho Individual 1) seleccionada para implementar as novas operações será a melhor das duas.

O aluno/grupo de trabalho 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.

As novas funcionalidades apresentam-se no menu principal: sublinhadas para implementação de mais uma operação para além da(s) já existente(s); e a negrito para as novas opções.

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
- **Criar Resumo Criptográfico Seguro**
- **Assinar Digitalmente**
- **Verificar Assinatura/Resumo Criptográfico 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:

- 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.

Para garantir a autenticidade do emissor da chave simétrica, é necessário criar o checksum (resumo criptográfico seguro) da chave simétrica e enviar juntamente com o criptograma.

É necessário que o utilizador forneça os dados necessários para a criação correcta do criptograma e do resumo criptográfico seguro. Ambos serão armazenados 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; e o resumo criptográfico seguro da chave simétrica.

Após a verificação do checksum e a abertura correcta dos criptogramas a mensagem, em *plaintext*, deverá ser apresentada ao utilizador.

- Criar Resumo Criptográfico Seguro

Esta opção permitirá obter o checksum de uma mensagem. 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 "Encriptação de Mensagens por Cifra Simétrica".

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

Esta opção permite criar a assinatura 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/Resumo Criptográfico Seguro

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

Entrega e Avaliação:

- A data limite de entrega do trabalho é dia 12 de novembro de 2012, às 23:55 H.
- O aluno/grupo de trabalho, até à data limite de entrega do trabalho, terá de entregar, na plataforma Moodle, na actividade "Envio do Trabalho Individual/Grupo Nº 2", um ficheiro comprimido (de formato à escolha), contendo o(s) ficheiro(s) de shell script e um ficheiro de texto com a 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.