Atividades - Criptografia Chave Simétrica

1. Introdução

OpenSSL é um poderoso conjunto de ferramentas de criptografia Este documento irá lhe fornecer algumas simples de seguir dicas sobre como criptografar as mensagens e arquivos usando OpenSSL.

2. Criptografar mensagens

Podemos começar por criptografar mensagens simples.

Abra o Cygwin e execute os comandos abaixo.

Os seguinte comando irá criptografar uma mensagem "Bem-vindo ao Campus Palmares" usando Base64 Encoding:

```
cd GitHub\Aula04\DES

echo "Bem-vindo ao Campus Palmares" |  openssl enc -base64
```

A saída do comando acima é uma string encriptada contendo a mensagem codificado. Para descriptografar string codificada de volta à sua mensagem original que precisamos para inverter a ordem e anexar opção -d para descriptografia:

```
echo "HASH A SER DESENCRIPTADO" |  openssl enc -base64 -d
```

A encriptação acima é simples de usar, no entanto, carece de uma característica importante, de uma palavra-passe, o que deve ser utilizada para a encriptação. Para criar uma mensagem criptografada com uma senha utilizando AES, você pode usar o seguinte comando:

```
echo "OpenSSL" |  openssl enc -aes-256-cbc -a
```

Se você desejar armazenar a saída do OpenSSL para um arquivo, em vez de simplesmente usar STDOUT, use o ">":

```
echo "OpenSSL" |  openssl enc -aes-256-cbc -a > openssl.dat

file openssl.dat

cat openssl.dat
```

Para descriptografar o arquivo openssl.dat de volta para a mensagem original:

```
openssl enc -aes-256-CBC -d -a -in openssl.dat
```

3. Criptografar Arquivos

Para criptografar arquivos com o OpenSSL é tão simples como criptografar mensagens.

A única diferença é que em vez de o comando echo usamos a opção ***-in*** com o arquivo real que gostaria de criptografar e opção de ***-out***, que irá instruir OpenSSL para armazenar o arquivo criptografado sob um determinado nome:

```
Openssl enc -aes-256-cbc -in /etc/services -out services.dat
```

Para descriptografar volta nosso arquivo de serviços:

```
openssl enc -aes-256-cbc –d -in services.dat –out services
```

4. Listando Algoritmos disponiveis

Para verificar quais outros algoritmos estão disponíveis:

```
openssl enc --help
```

5. Criptografando Arquivo

Criptografe o arquivo **texto2.txt** utilizando o algoritmo ***blowfish*** e senha “ifpe123”, salvando o arquivo contendo o conteúdo encriptado com o nome “texto2.txt.dat”.