OpenSSL — Cifrado e Firma Dixital

Criptografía simétrica

Cifrado

Temos un ficheiro mensaxe.txt e o queremos cifrar co algoritmo DES3. Co seguinte comando procedemos a facer un cifrado simétrico, para o cal se nos preguntará a chave de cifrado. Os datos cifrados gárdanse no ficheiro mensaxes.des3.

```
openssl enc -e -des3 -in mensaxe.txt -out mensaxe.des3
```

Descifrado

Para descrifrar os datos previamente cifrados (no ficheiro mensaxe.des3) procederemos coa seguinte orde. Teremos que indicar a chave de cifrado anterior. Os datos descifrados gardaranse no ficheiro mensaxe2.txt.

```
openssl enc -d -des3 -in mensaxe.des3 -out mensaxe2.txt
```

Criptografía asimétrica

Xeración de certificado

Imos xerar un certificado autofirmado. O certificado contén información acerca do seu titular, a data de validez e o par de chaves privada e pública. Procédese cos seguintes comandos:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

```
openssl rsa -in key.pem -pubout -out pub-key.pem
```

Despois de completar este paso, teremos os ficheiros seguintes:

- key.pem: chave privada
- cert.pem: certificado dixital
- pub-key.pem: chave pública (obtida a partir da privada)

Cifrado

Para cifrar un ficheiro (mensaxe.txt) empregaremos a chave pública. Procederase co seguinte comando, o cal deixará os datos cifrados no ficheiro mensaxe.enc.

```
openssl pkeyutl -encrypt -inkey pub-key.pem -pubin -in mensaxe.txt -out\
mensaxe.enc
```

Descifrado

Para descifrar os datos precisaremos a chave privada. Co comando seguinte descífranse os datos de mensaxe.enc, gardándose no ficheiro mensaxe2.txt.

```
openssl pkeyutl -decrypt -inkey key.pem -in mensaxe.enc -out mensaxe2.txt
```

Firma

Para firmar dixitalmente un conxunto de datos precisamos a chave privada. O comando para facer a firma co algoritmo SHA256 é o seguinte, obtendo coma resultado a firma no ficheiro mensaxe.txt.sha256.

```
openssl dgst -sha256 -sign key.pem -out mensaxe.txt.sha256 mensaxe.txt
```

Validación de firma

Para validar a firma duns datos empregamos a chave pública. O comando que verifica a integridade dos datos de mensaxe.txt firmados en mensaxe.txt.sha256 é o seguinte:

```
openssl dgst -sha256 -verify pub-key.pem -signature mensaxe.txt.sha256\
mensaxe.txt
```