Práctica: Cifrado simétrico con OpenSSL

Seguridad de Sistemas Informáticos

Segunda Práctica

Resumen

El objetivo de está práctica es trabajar con diferentes esquemas de cifrado simétrico disponibles en OpenSSL.

1. OpenSSL: una herramienta de código abierto

OpenSSL es una implementación abierta de los protocolos SSL y TLS para comunicaciones seguras, proporcionando una infinidad de funciones utilizadas en la gestión de seguridad. A continuación se citan algunas de ellas:

- Generación de números aleatorios.
- Utilidades numéricas: comprobación de primalidad, cálculo de inversos, etc.
- Cifrado y descifrado.
- Generación y gestión de claves privadas, públicas y parámetros.
- Evaluación de algoritmos criptográficos.
- Cálculo y verificación de resúmenes (funciones hash criptográficas) para la integridad de ficheros.
- Emisión y gestión de certificados X.509 y CRLs.
- Generación y verificación de marcas (sellado) de tiempo.
- Operaciones criptográficas de clave pública: firma electrónica.
- Testeo de clientes y servidores SSL/TLS.
- Gestión de correo S/MIME firmado o cifrado.

Está compuesto por tres partes `https://www.openssl.org/`: la librería SSL(`https://www.openssl.org/docs/man1.1.1/man7/ssl.html`) , la librería Crypto (https://www.openssl.org/docs/man1.1.1/man7/crypto.html) y una línea de comandos muy potente (https://www.openssl.org/docs/man1.1.1/man1/). En la presente práctica haremos uso de la línea de comandos.

Está disponible para diferentes sistemas operativos y permite el uso de funciones incluidas en su API en el desarrollo de aplicaciones seguras.

Desde el indicador del sistema operativo Linux puedes ejecutarlo en modo comando el programa tecleando OpenSSL.

2. Ejercicios de confidencialidad con clave secreta en OpenSSL

1. Comprueba la lista de algoritmos simétricos soportados por OpenSSL, ¿cómo lo has hecho? ¿Cuáles son cifrados en flujo y cuáles cifrados en bloque?

2. Genera un documento de texto. Puedes usar el siguiente texto:

```
Kernel nuestro que estás en /usr/src/linux
santificados sean tus .h
venga a nosotros tu make xconfig
hagase tu compilación así en el Pentium com en el AMD
perdona nuestros Windows
así como nosotros perdonamos a los que lo usan
y libranos de Bill Gates
exit
```

3. Consulta en la documentación facilitada en clase sobre cómo se utiliza el comando `enc` para cifrar y descifrar.

4. Cifra el fichero anterior con triple des EDE y AES 192. Usa para ambos algoritmo de cifrado los modos de cifrado ECB y CBC. Genera los ficheros de salida.

   a) ¿Cómo has especificado la clave?

   b) Descífralo y comprueba el resultado.

   c) Analiza el comportamiento de los cifrados DES y AES usando todas las longitudes de clave posibles y todos los modos de cifrado implementados. Para cada una de las posibles combinaciones (cifrado, longitud de clave, modo de cifrado) obtén el fichero de salida (usando como fichero de texto en claro DancingMen.txt) y mide el tiempo necesario para la generación de dicho fichero. Resume esta información en una tabla.

   d) Haz el mismo análisis para las versiones de RC4 implementadas en OpenSSL.

5. Genera los parámetros necesarios para cifrar con el cifrado AES usando el modo CFB y una longitud de clave de 192.

6. Cifrado en HTTPs (estas conexiones usan TSL):

a) Accede a las página `https://sede.educacion.gob.es` y `https://www1.sedecatastro.gob.es/`

b) ¿qué algoritmo simétrico se utiliza para cada conexión? Separa los elementos que componen la suite de cifrado utilizado

c) Probar distintos navegadores (Firefox, IE, etc), ¿existen diferencias entre las especificaciones de cifrado?

d) Busca otros sitios seguros y comprueba la configuración asociada a los esquemas de cifrado que se utilizan

7. Prueba de correo electrónico

a) Cifra el fichero DancingMen.txt a tu gusto. Para ello selecciona un esquema de cifrado simétrico, una clave y en caso de ser necesario un vector de inicialización. Genera el resultado codificado en base64.

b) Envía el resultado del paso anterior por correo electrónico a un compañero.

c) Comunica la clave por medio de un "canal de comunicación seguro".

d) Descifrar el fichero que has recibido del compañero de clase, ¿basta con conocer la clave de cifrado?