26. Cifrado Simétrico con Clave Compartida

FASE 1 — COMPRENDER LA AMENAZA

- Texto plano: información que se puede leer directamente.
- Texto cifrado: información que se vuelve ilegible tras el cifrado.
- Clave: el secreto utilizado para controlar el cifrado y descifrado.
- Algoritmo: el método matemático utilizado para realizar el cifrado.

El cifrado simétrico utiliza la misma clave tanto para el cifrado como para el descifrado.
Si la clave se ve comprometida, la seguridad queda totalmente comprometida.

FASE 2 — PREPARAR EL SISTEMA

Verificar módulo criptográfico OpenSSL:

- openssl version

```
ub@forense-ai:~$ openssl version
OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
```

FASE 3 — CREAR MENSAJE SENSIBLE

Simular credenciales del sistema de la nave.

- echo "Credenciales núcleo warp: acceso nivel comandante." > mensaje.txt

```
ub@forense-ai:~$ echo "Credenciales núcleo warp: acceso nivel comandante." > mensaje.txt
```

- cat mensaje.txt

```
ub@forense-ai:~$ cat mensaje.txt
Credenciales núcleo warp: acceso nivel comandante.
```

FASE 4 — GENERAR CLAVE SEGURA

Generar clave criptográfica:

- openssl rand -base64 32

```
ub@forense-ai:~$ openssl rand -base64 32
UiBF0QhXpVZcGY0M5rkEuu5MazHuNITpl5SLa7Zn9/A=
```

FASE 5 — CIFRADO AES-256-CBC

Activar cifrado simétrico estándar de la Federación.

- openssl enc -aes-256-cbc -salt -in mensaje.txt -out mensaje.enc

```
ub@forense-ai:~$ openssl enc -aes-256-cbc -salt -in mensaje.txt -out mensaje.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

Verificar resultado:

- cat mensaje.enc

```
ub@forense-ai:~$ cat mensaje.enc
Salted__◆g◆◆◆Nñ◆◆1Q◆~ф▷y~◆B◆◆◆◆ ◆[J◆◆>Jcp$ß◆Ŵ4◆◆p29Θ◆?◆ЂЛ◆◆◆8X◆◆◆(
```

FASE 6 — INTERCEPCIÓN ENEMIGA

Simular intento de descifrar sin clave correcta.

- openssl enc -aes-256-cbc -d -in mensaje.enc

```
ub@forense-ai:~$ openssl enc -aes-256-cbc -d -in mensaje.enc
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
40C727E11C750000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/ciph
ers/ciphercommon_block.c:124:
d◆g◆◆◆IPĠ◆>]tf
          C◆◆X◆◆◆W◆W◆◆xN◆◆◆◆\hRub@forense-ai:~$
```

Sin la clave correcta, el mensaje no puede recuperarse.

FASE 7 — DESCIFRADO AUTORIZADO

Recuperar mensaje con clave correcta.

- openssl enc -aes-256-cbc -d -in mensaje.enc -out mensaje_recuperado.txt

```
ub@forense-ai:~$ openssl enc -aes-256-cbc -d -in mensaje.enc -out mensaje_recuperado.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- diff mensaje.txt mensaje_recuperado.txt

```
ub@forense-ai:~$ diff mensaje.txt mensaje_recuperado.txt
```

Si no hay ningún resultado, significa que los dos archivos son iguales.

FASE 8 — CIFRADO MODERNO (AES-GCM)

- openssl enc -aes-256-gcm -salt -in mensaje.txt -out mensaje_gcm.enc

```
ub@forense-ai:~$ openssl enc -aes-256-gcm -salt -in mensaje.txt -out mensaje_gcm.enc
enc: AEAD ciphers not supported
enc: Use -help for summary.
```

Las versiones modernas de OpenSSL no permiten usar AES-GCM mediante el comando enc, ya que GCM requiere manejo de etiquetas de autenticación (authentication tag).

FASE 9 — ANÁLISIS TÉCNICO

Tipos de cifrado simétrico

Utiliza una única clave compartida para cifrar y descifrar información.

Cifradores de bloque

Trabajan sobre bloques de tamaño fijo, normalmente 128 bits.

- AES (estándar Federación)
- DES (obsoleto)
- 3DES (retirada progresiva)

Cifradores de flujo

Cifran los datos bit a bit o byte a byte.

- ChaCha20 (uso en comunicaciones rápidas)
- RC4 (inseguro, prohibido)

Modos de operación

Un cifrador de bloque necesita un modo de operación para cifrar mensajes largos.

- ECB → inseguro (filtra patrones)
  Cifra cada bloque de forma independiente. Filtra patrones.

- CBC → clásico
  Cada bloque depende del anterior. Usa un IV y no detecta manipulación.

- CTR → moderno
  Un modo rápido y moderno que convierte un cifrador de bloque en un cifrador de flujo.

- GCM → cifrado autenticado (recomendado)
  Modo moderno de cifrado autenticado (AEAD).Proporciona confidencialidad, integridad y autenticidad.

FASE 10 — EL TALÓN DE AQUILES

¿Cómo compartir la clave sin que sea interceptada?

- El problema del cifrado simétrico es el intercambio seguro de la clave, que se resuelve mediante:
  - **criptografía asimétrica**
  - **intercambio Diffie-Hellman**
  - **protocolo TLS**

  Además el cifrado simétrico nunca viaja solo.

FASE 11 — ERRORES CRÍTICOS (INFORME OWASP)

Fallos detectados en sistemas comprometidos:

- Datos sensibles almacenados o transmitidos sin cifrar
- Uso del modo ECB (filtra patrones)
- Claves embebidas en el código fuente
- Claves débiles o predecibles
- Reutilización de claves
- No utilizar cifrado autenticado (como GCM)
- Envío de claves por canales inseguros

La criptografía falla por mala ingeniería, no por matemáticas.

FASE 12 — EXPERIMENTOS OPCIONALES

Ver algoritmos compatibles

- openssl enc -ciphers

```
ub@forense-ai:~$ openssl enc -ciphers
Supported ciphers:
-aes-128-cbc               -aes-128-cfb               -aes-128-cfb1
-aes-128-cfb8              -aes-128-ctr               -aes-128-ecb
-aes-128-ofb               -aes-192-cbc               -aes-192-cfb
-aes-192-cfb1              -aes-192-cfb8              -aes-192-ctr
-aes-192-ecb               -aes-192-ofb               -aes-256-cbc
-aes-256-cfb               -aes-256-cfb1              -aes-256-cfb8
-aes-256-ctr               -aes-256-ecb               -aes-256-ofb
-aes128                    -aes128-wrap               -aes192
-aes192-wrap               -aes256                    -aes256-wrap
-aria-128-cbc              -aria-128-cfb              -aria-128-cfb1
-aria-128-cfb8             -aria-128-ctr              -aria-128-ecb
-aria-128-ofb              -aria-192-cbc              -aria-192-cfb
-aria-192-cfb1             -aria-192-cfb8             -aria-192-ctr
-aria-192-ecb              -aria-192-ofb              -aria-256-cbc
-aria-256-cfb              -aria-256-cfb1             -aria-256-cfb8
-aria-256-ctr              -aria-256-ecb              -aria-256-ofb
```

Ver estructura del texto cifrado

- xxd mensaje.enc | head

```
ub@forense-ai:~$ xxd mensaje.enc | head
00000000: 5361 6c74 6564 5f5f ef67 c3b8 abdf 4ed1  Salted__.g....N.
00000010: 9bf9 1a31 51e9 7ec9 b83e 797e 9c05 42a1  ...1Q.~..>y~..B.
00000020: 8107 afec 9c20 d55b 4adf c13e 4a63 7024  ..... .[J..>Jcp$
00000030: c39f e7c5 b434 bb8c 7032 39c9 b593 3f8f  .....4..p29...?.
00000040: d294 d4a0 98fa 9838 0058 891d cde6 1d28  .......8.X.....(
```