Algoritmos DES y AES

Instale la herramienta Cryptools (www.cryptools.org). Cree un fichero plano con extensión
.txt y escriba en su interior el texto ‘Esto es un simple ejemplo’. Ejecute la opción Cifrar/ Descifrar y se obtendrá un menú de opciones compuesto por los diferentes algoritmos de cifrado que se le puede aplicar al texto anterior: simétrico clásico, simétrico moderno, asimétrico e híbrido. Al elegir un algoritmo y el número de bits de cifrado, se obtendrá una pequeña ventana con la información cifrada (tal como se indica en la Figura 4.11)

cifrado y descifrado simétrico clásico (cifrado “cesar”)

El cifrado César es un método de cifrado simétrico clásico que consiste en desplazar las letras de un mensaje un número fijo de posiciones en el alfabeto. Este método es uno de los más antiguos y sencillos de la criptografía. A continuación, te explico cómo funciona tanto el cifrado como el descifrado:

Cifrado

Entrada: Un texto plano (mensaje original) y una clave (un número que indica el desplazamiento en el alfabeto).

Proceso: Cada letra del texto se reemplaza por otra que se encuentra un número fijo de posiciones más adelante en el alfabeto.

Por ejemplo, si la clave es 3, la letra A se convierte en D, B en E, y así sucesivamente.

Reglas:

Si el desplazamiento supera la última letra del alfabeto, el conteo se reinicia desde la A (cifrado circular).

Normalmente, solo se cifra el alfabeto y se ignoran los números, espacios o caracteres especiales.

Resultado: El texto cifrado.

Ejemplo:

Texto plano: HOLA
Clave: 3
Texto cifrado: KROD

Descifrado

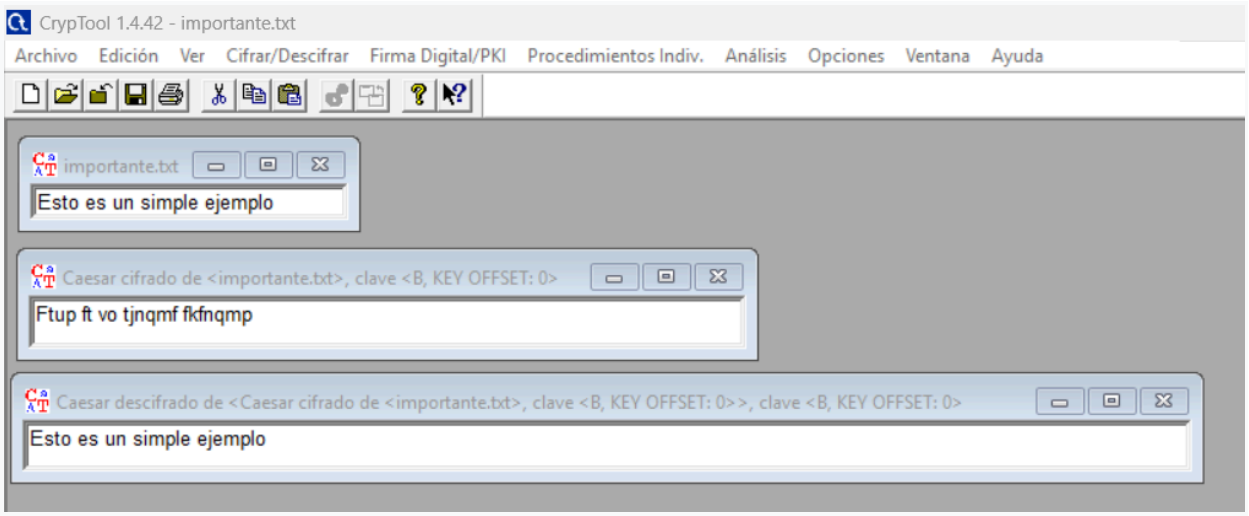
Entrada: Un texto cifrado y la clave.

Proceso: Se realiza el desplazamiento inverso al usado para cifrar.

Si la clave es 3, la letra D vuelve a ser A, E se convierte en B, y así sucesivamente.
Resultado: El texto plano original.

Ejemplo:

Texto cifrado: KROD
Clave: 3
Texto descifrado: HOLA



---

cifrado y descifrado simétrico moderno (cifrado “IDEA”)
El cifrado IDEA (International Data Encryption Algorithm) es un método de cifrado simétrico moderno desarrollado en 1991 por Xuejia Lai y James Massey. Es mucho más complejo y seguro que los cifrados clásicos como el César, y fue diseñado para proporcionar alta seguridad en aplicaciones prácticas, como la protección de datos y comunicaciones.
Cifrado
Entrada:

1. Texto plano: Un bloque de 64 bits (8 bytes).

2. Clave: Una clave de 128 bits (16 bytes).

3. Proceso: IDEA divide el texto en bloques de 64 bits y lo cifra en 8 rondas principales, seguidas de una ronda de salida. Cada ronda utiliza subclaves derivadas de la clave principal.

4. División inicial: El bloque de 64 bits se divide en cuatro partes de 16 bits cada una.

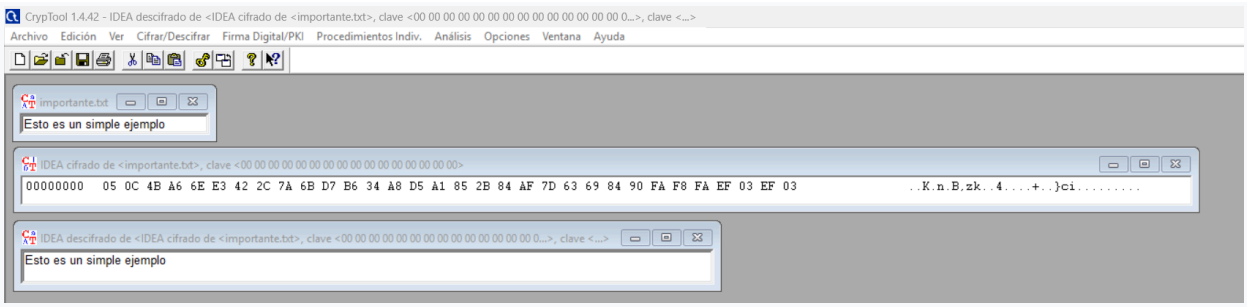
5. Operaciones en cada ronda:
    6. Mezclas no lineales (multiplicación modular y suma modular).
    7. Combinaciones lineales (operaciones XOR).
    8. Permutaciones y reordenamiento de las partes.
    9. Subclaves: En cada ronda, se generan subclaves específicas a partir de la clave original usando un proceso de derivación.

Salida:

Después de completar las rondas y la ronda de salida, se genera un bloque cifrado de 64 bits.

Descifrado

El descifrado invierte el proceso del cifrado, utilizando las subclaves en orden inverso y aplicando las operaciones opuestas (inversas matemáticas de suma y multiplicación modulares).



cifrado y descifrado asimétrico(cifrado “RSA”)

El cifrado RSA es uno de los métodos más conocidos y utilizados en criptografía asimétrica. Fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, de ahí su nombre. A diferencia de los métodos simétricos, RSA utiliza dos claves diferentes: una pública para cifrar y una privada para descifrar.

1. Generación de claves

Para generar un par de claves (pública y privada), se siguen estos pasos:

Seleccionar dos números primos grandes p y q.

Calcular n = p X q. Este n es el módulo y es parte de ambas claves.

Calcular 4(n) = (p — 1) X (q — 1), donde 4(n) es la función de Euler.

Elegir un número e (exponente público) tal que 1 < e < 4(n) y que sea coprimo con 4(n).

(Un valor comúnmente usado es e = 65537.)

Calcular d (exponente privado) como el inverso modular de e respecto a 4(n):

d x e 1 (mod 4(n))

Clave pública: (e, n).

Clave privada: (d, n).

2. Cifrado

Para cifrar un mensaje M:

• El mensaje debe representarse como un número M tal que O < M < n.

• Usar la clave pública (e, n) para cifrar el mensaje:

$$C = M^e \bmod n$$

• El resultado C es el mensaje cifrado.

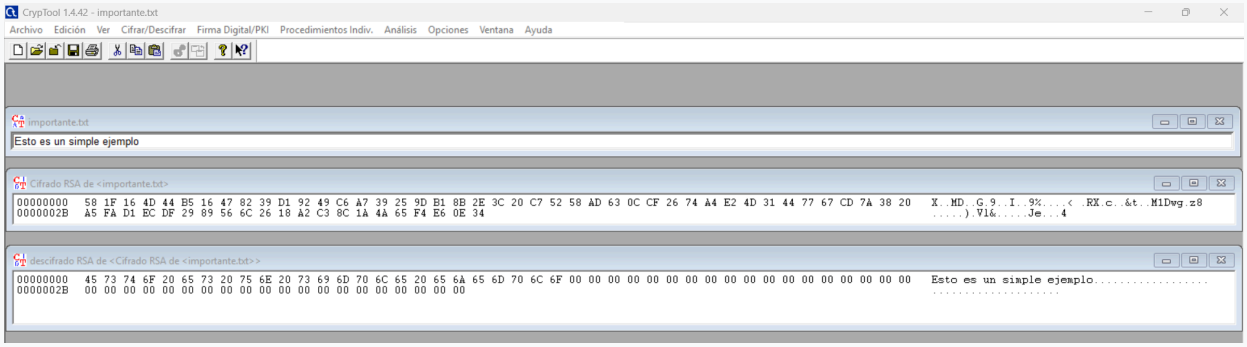
3. Descifrado

Para descifrar el mensaje cifrado C:

• Usar la clave privada (d, n) para recuperar el mensaje original:

$$M = C^d \bmod n$$

• El resultado M es el mensaje original.



---

cifrado y descifrado híbrido (cifrado “RSA-AES”)
El cifrado híbrido combina lo mejor de los cifrados asimétricos (como RSA) y los simétricos (como AES) para lograr una comunicación segura y eficiente. Este enfoque es ampliamente utilizado en protocolos modernos como HTTPS y PGP, ya que aprovecha las fortalezas de ambos tipos de cifrado. A continuación, te explico cómo funciona este sistema híbrido.

1. Cifrado

1. **Generación de la clave AES**:
    - Se genera una clave aleatoria para el cifrado simétrico (**clave de sesión**), que será utilizada por AES.
    - Por ejemplo, una clave AES típica puede ser de 128 o 256 bits.
2. **Cifrado de los datos con AES**:
    - Los datos reales (texto o archivo) se cifran utilizando el algoritmo AES con la clave generada.
3. **Cifrado de la clave AES con RSA**:
    - La clave AES generada se cifra utilizando la **clave pública** del receptor con el algoritmo RSA.
4. **Envío**:
    - Se envían dos cosas al receptor:
        - El **texto cifrado** (por AES).
        - La **clave AES cifrada** (por RSA).

2. Descifrado

1. **Descifrado de la clave AES con RSA**:
    - El receptor utiliza su **clave privada** de RSA para descifrar la clave AES.
2. **Descifrado de los datos con AES**:

- Usando la clave AES descifrada, el receptor puede descifrar el texto o archivo cifrado con AES y recuperar los datos originales.