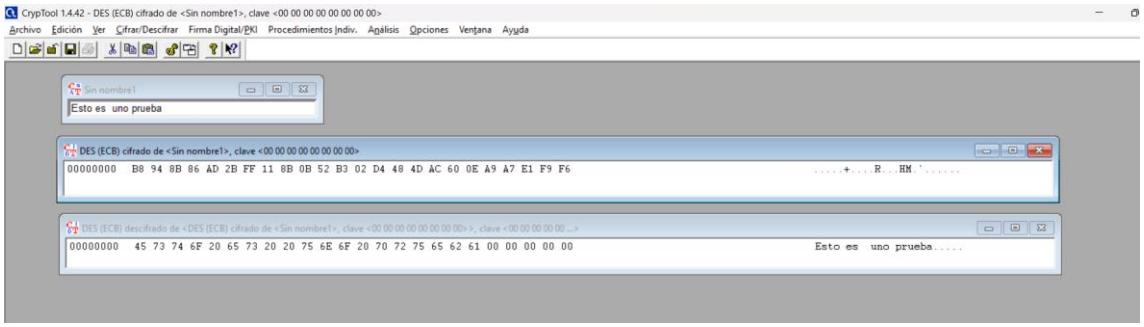
Algoritmos ECB y WPA

Crea un fichero plano con extensión .txt y escriba en su interior el texto 'Esto es uno prueba . Usando la aplicación Cryptools, ejecuta las opciones que se encuentran en Cifrar/Descifrar.

Se obtendrán dos ficheros cifrados, uno a través del algoritmo ECB y, otro, usando el algoritmo WPA. Analiza las diferencias más importantes que se puedan dar entre ambos algoritmos.

Algoritmo ECB



El algoritmo **ECB (Electronic Codebook)** es uno de los modos más simples de operación para los algoritmos de cifrado de bloque, como el **AES** (Advanced Encryption Standard) o el **DES** (Data Encryption Standard). Su funcionamiento es relativamente sencillo, pero tiene algunas desventajas en términos de seguridad, que lo hacen menos recomendable para la mayoría de las aplicaciones modernas.

Funcionamiento básico de ECB:

1. **División en bloques**: El texto plano (el mensaje original) se divide en bloques de tamaño fijo. El tamaño del bloque depende del algoritmo de cifrado utilizado (por ejemplo, AES usa bloques de 128 bits).
2. **Cifrado de cada bloque**: Cada bloque de texto plano se cifra de forma independiente utilizando la misma clave de cifrado. Es decir, el primer bloque se cifra con la clave, el segundo bloque se cifra con la misma clave, y así sucesivamente. La operación de cifrado es exactamente la misma para cada bloque.
3. **Texto cifrado**: El resultado es una serie de bloques cifrados que, al ser concatenados, forman el texto cifrado final.

Ejemplo de funcionamiento de ECB:

Supongamos que tenemos el siguiente texto plano y una clave de cifrado:

- Texto plano: "HOLA MUNDO"
- Clave de cifrado: "1234567890ABCDEF"

El texto plano se divide en bloques de 128 bits (en el caso de AES, por ejemplo), y cada bloque se cifra de forma independiente con la clave proporcionada. Si un bloque se repite en el texto plano, el mismo bloque cifrado se repetirá en el texto cifrado. Esto es una de las características que hacen que ECB sea vulnerable a ciertos ataques.

Algoritmo WPA

El algoritmo WPA (Wi-Fi Protected Access) es un protocolo de seguridad para redes inalámbricas que protege la comunicación cifrando los datos y controlando el acceso. Funciona de la siguiente manera:

1. **Autenticación**: Utiliza un sistema basado en contraseñas (PSK, Pre-Shared Key) o autenticación avanzada con un servidor (802.1X).
2. **Cifrado**: Emplea el protocolo TKIP (Temporal Key Integrity Protocol) en WPA o AES (Advanced Encryption Standard) en WPA2 para cifrar los datos transmitidos.
3. **Integridad**: Garantiza que los datos no sean alterados durante la transmisión mediante un código de verificación de mensajes (MIC).

Esto asegura que solo dispositivos autorizados puedan conectarse y que la información intercambiada esté protegida.