Herramienta para la comprobación de criptografía: CyberChef

1. Introducción

CyberChef es una herramienta web gratuita desarrollada por GCHQ (Cuartel General de Comunicaciones del Gobierno del Reino Unido), diseñada para realizar una amplia gama de operaciones sobre datos, como cifrado, descifrado, codificación, hashing y análisis de formatos. Es conocida como “la navaja suiza de los datos” por su versatilidad, permitiendo que cualquier usuario, sin necesidad de conocimientos avanzados de programación, pueda probar y visualizar algoritmos de criptografía y manipulación de datos de forma sencilla.

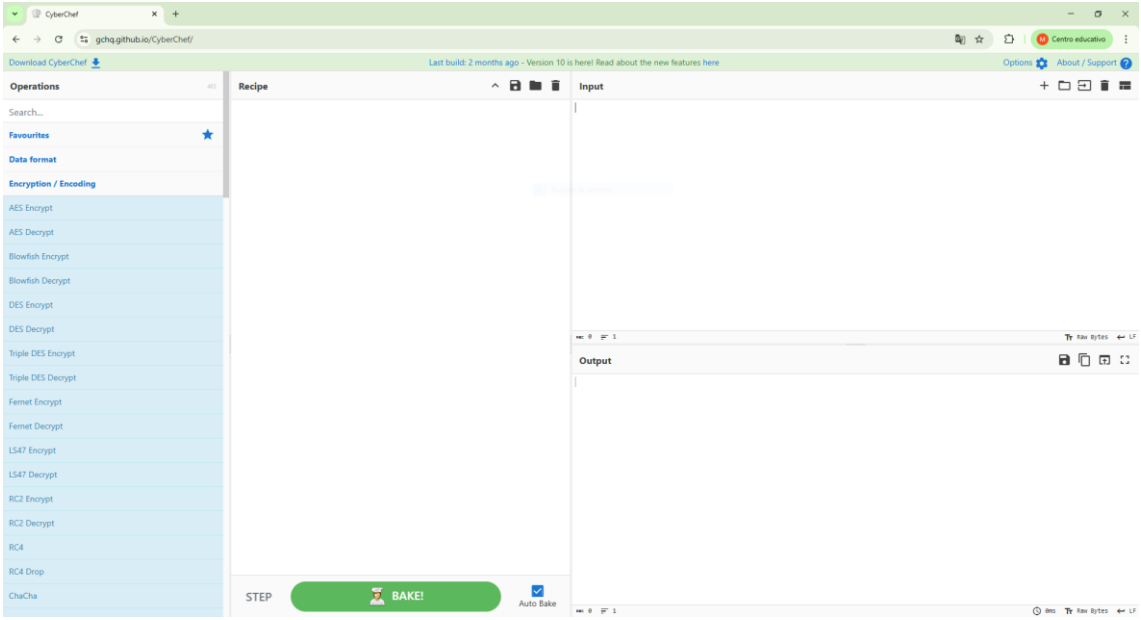
---

2. Funcionamiento Básico de CyberChef

Interfaz principal

La interfaz se divide en cuatro paneles principales:

- **Input (Entrada):** Es el área superior derecha donde introduces el texto o los datos que quieres procesar.
- **Recipe (Receta):** Es la columna central donde arrastras y configuras las operaciones que deseas aplicar. Puedes encadenar varias operaciones en el orden que necesites.
- **Output (Salida):** Es el área inferior derecha que muestra el resultado de aplicar la "receta" a los datos de entrada.
- **Operations (Operaciones):** Es la columna de la izquierda, que contiene una lista completa de todas las funciones disponibles, organizadas por categorías (Cifrado, Codificación, Redes, etc.).

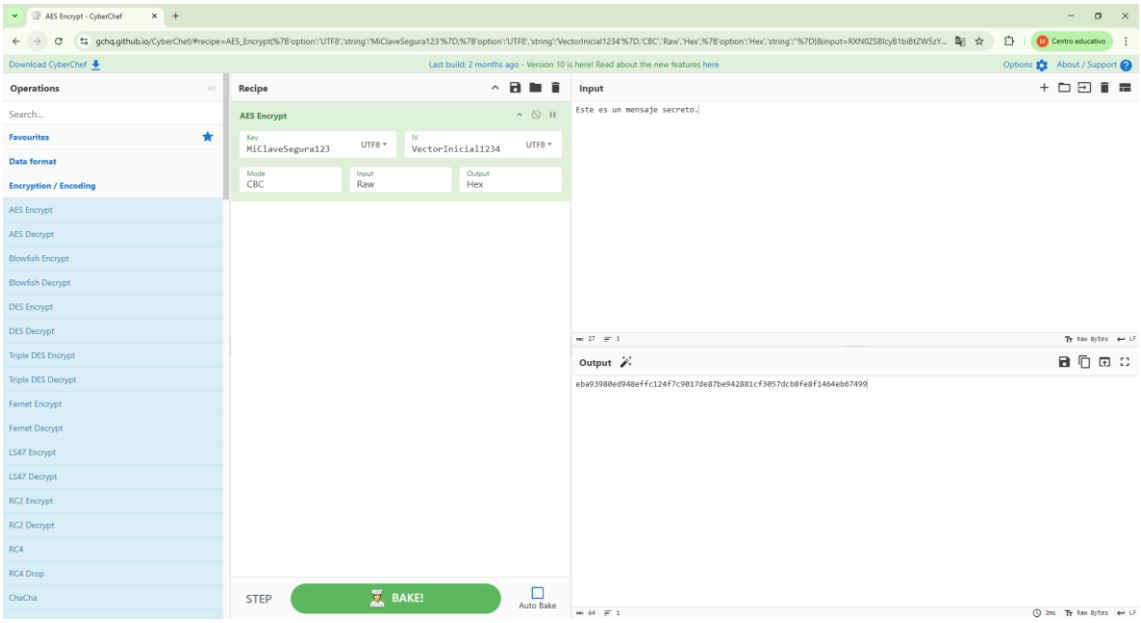


3. Criptografía Simétrica en CyberChef

La criptografía simétrica utiliza la **misma clave** tanto para cifrar como para descifrar la información. Es muy rápida y eficiente, siendo AES (Advanced Encryption Standard) uno de los algoritmos más comunes y seguros.

Ejemplo: Cifrado y Descifrado con AES

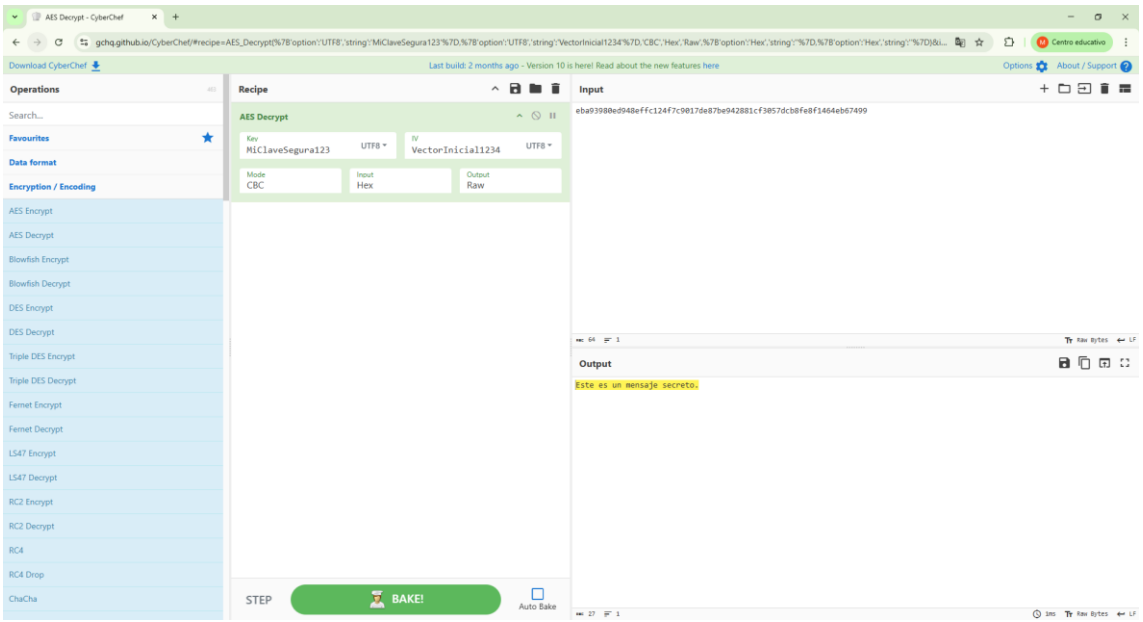
1. **Introduce el texto a cifrar** en el panel de **Input**. Por ejemplo: Este es un mensaje secreto.
2. En la lista de **Operations**, busca y arrastra **"AES Encrypt"** al panel de **Recipe**.
3. Configura los parámetros en la operación:
    - **Key (Clave):** Introduce una clave secreta. Por ejemplo: MiClaveSegura123.
    - **IV (Vector de Inicialización):** Introduce un valor. Por ejemplo: VectorInicial1234.
    - **Mode:** Selecciona un modo de operación, como CBC.
4. El resultado cifrado aparecerá automáticamente en el panel de **Output**.



El texto plano del panel de "Input" se ha transformado en un texto cifrado ilegible en el "Output" al aplicarle la receta de cifrado AES con la clave y el IV especificados.

Para descifrar el mensaje:

1. Copia el texto cifrado del "Output" al "Input".
2. Sustituye la operación "AES Encrypt" por **"AES Decrypt"**.
3. Introduce **exactamente la misma clave y IV** que usaste para cifrar.
4. El texto original volverá a aparecer en el panel de "Output".



El proceso se invierte. Utilizando la misma clave, el texto cifrado es devuelto a su forma original, demostrando el funcionamiento de la criptografía simétrica.

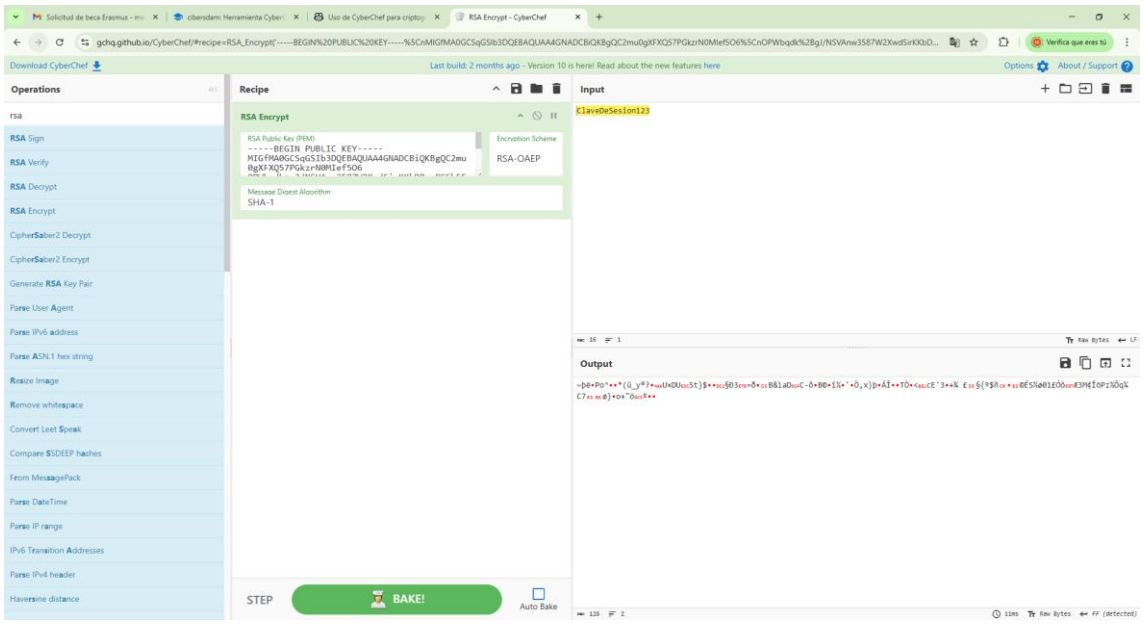
---

4. Criptografía Asimétrica en CyberChef

La criptografía asimétrica utiliza un par de claves matemáticamente relacionadas: una **clave pública** (que se puede compartir) y una **clave privada** (que debe mantenerse en secreto). Lo que se cifra con la clave pública solo se puede descifrar con la clave privada correspondiente. El algoritmo más conocido es **RSA**.

Ejemplo: Cifrado y Descifrado con RSA

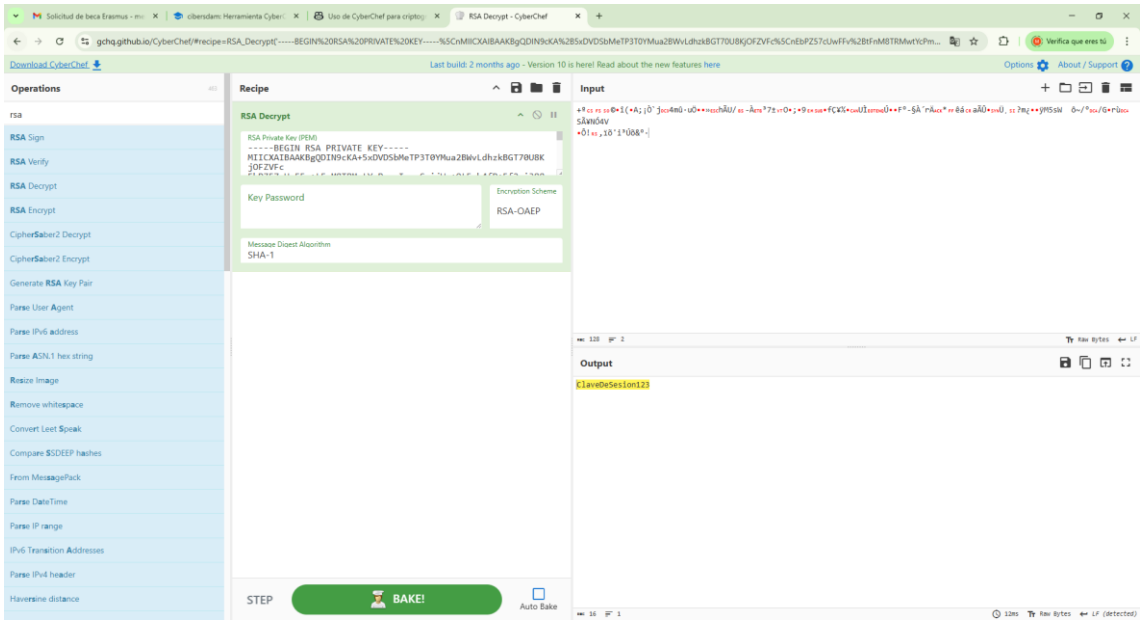
1. Primero, necesitamos un par de claves. En CyberChef, busca la operación **"Generate RSA Keypair"** y ejecútala para obtener una clave pública y una privada. Guarda ambas.
2. Introduce un mensaje en el panel de **Input**.
3. Arrastra la operación **"Public Key Encrypt"** a la receta.
4. En la configuración de la operación:
    - **Encryption:** Selecciona RSA.
    - **Public Key:** Pega la clave pública que generaste en el paso 1.
5. El mensaje cifrado aparecerá en el "Output".



El mensaje se ha cifrado utilizando la clave pública. Este texto cifrado solo podrá ser leído por quien posea la clave privada correspondiente.

Para descifrarlo:

1. Copia el texto cifrado al "Input".
2. Usa la operación **"Private Key Decrypt"**.
3. En la configuración, pega la **clave privada** que generaste.
4. El mensaje original se mostrará en el "Output".



Usando la clave privada, se ha revertido el cifrado y se ha recuperado el mensaje original, demostrando el principio de la criptografía asimétrica.

5. Conclusiones

CyberChef se consolida como una herramienta educativa y práctica de incalculable valor. Permite a estudiantes, desarrolladores y profesionales de la ciberseguridad experimentar de manera visual e interactiva con algoritmos criptográficos complejos sin necesidad de escribir una sola línea de código. Su enfoque modular mediante "recetas" facilita la comprensión de cómo funcionan los sistemas de cifrado simétrico, asimétrico e híbrido, desmitificando conceptos que a menudo son puramente teóricos.