**Universidad Nacional Autónoma de Nicaragua**

**UNAN-León**

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**V año**



**Componente: Laboratorio Seguridad en Redes**

**Tema: Ciffrado AES con Criptool**

**Elaborado por:**

* **Br. Jhonatan Uziel Espinoza Ortega 15-00737-0**

**Dirigido a:**

**M. Sc Aldo Martínez**

**León, Nicaragua lunes 8 de julio del 2019**

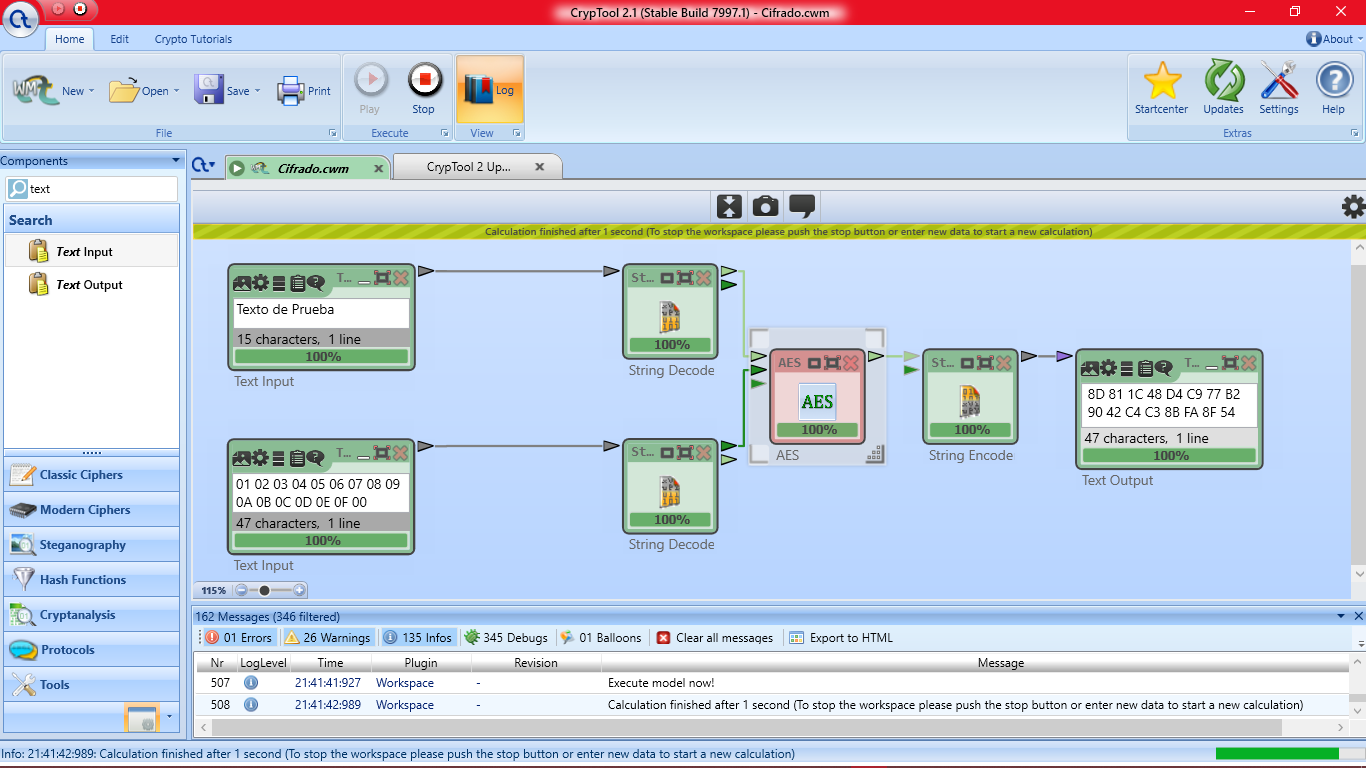
**Algoritmos de Cifrado Simétrico**

**Introducción**

El objetivo de este trabajo es entender las bases de funcionamiento y uso de los algoritmos de cifrado simétrico utilizando la plataforma Cryptool 2.0.

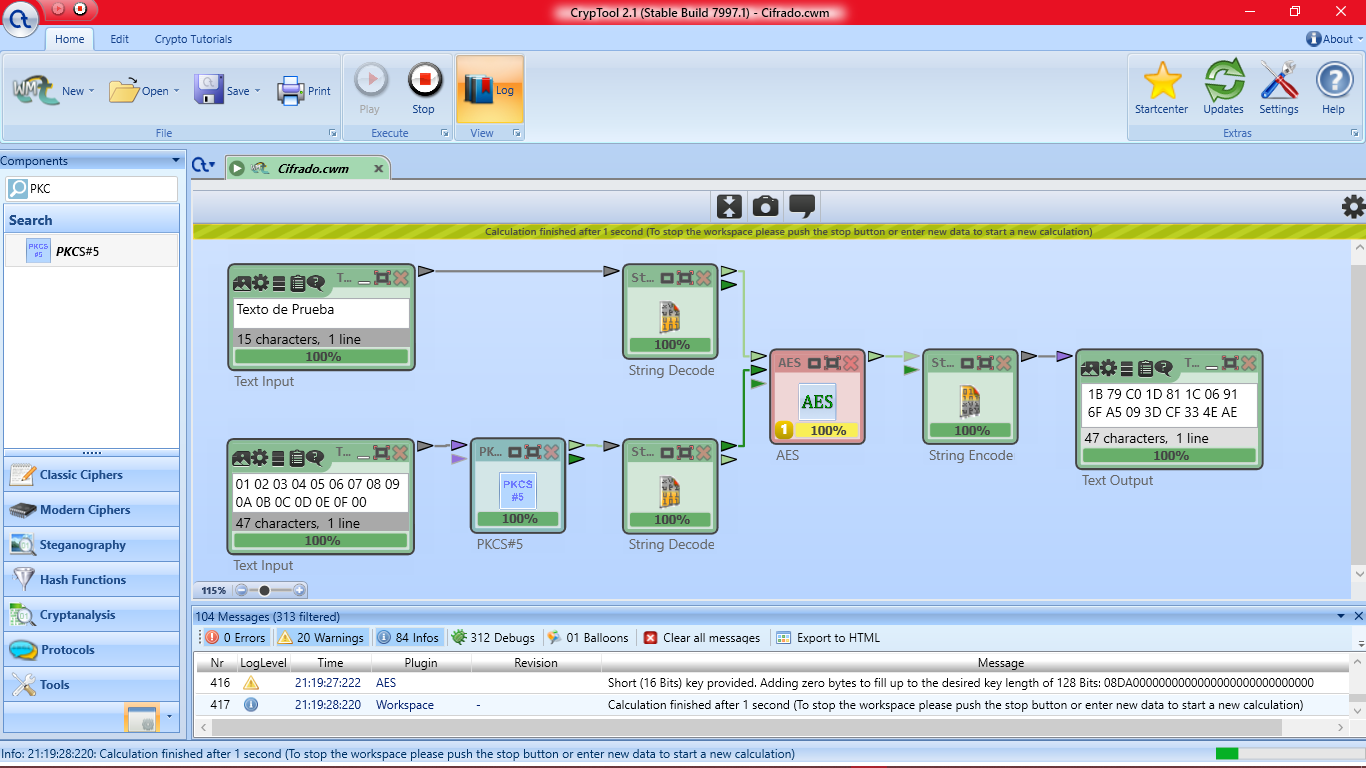
**Cifrado con AES**

Utilizando CrypTool 2.0, diseñar un sistema de cifrado y descifrado con AES. Se puede usar un módulo TextInput o bien un módulo RandomInputGenerator para alimentar la clave y el IV. Utilizar módulos TextInput y TextOutput para introducir el texto en claro y visualizas los resultados. También su puede usar un stream comparator para verificar si son iguales el texto inicial a la entrada del cifrador y el final a la salida del descifrador.

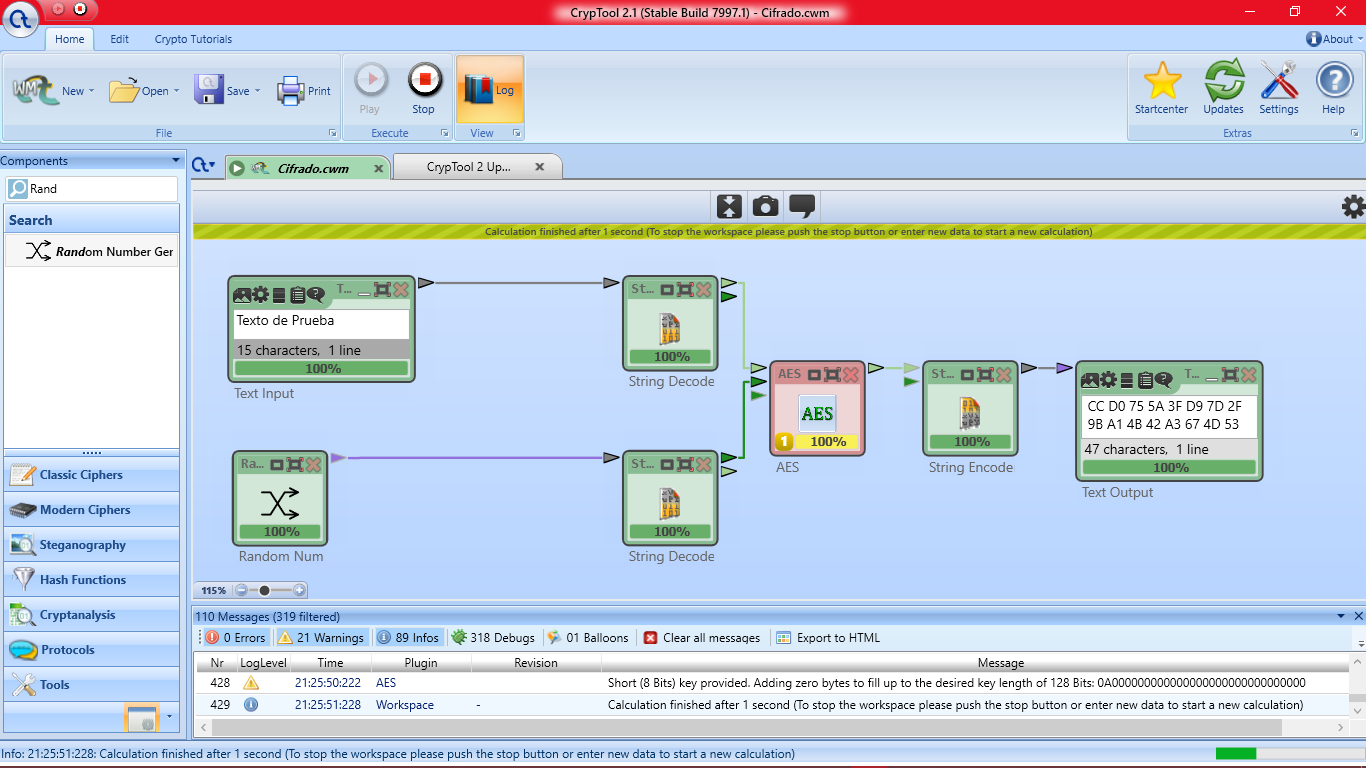


**Se pide:**

* Generar claves AES derivadas de una password, utilizando PKCS#5.

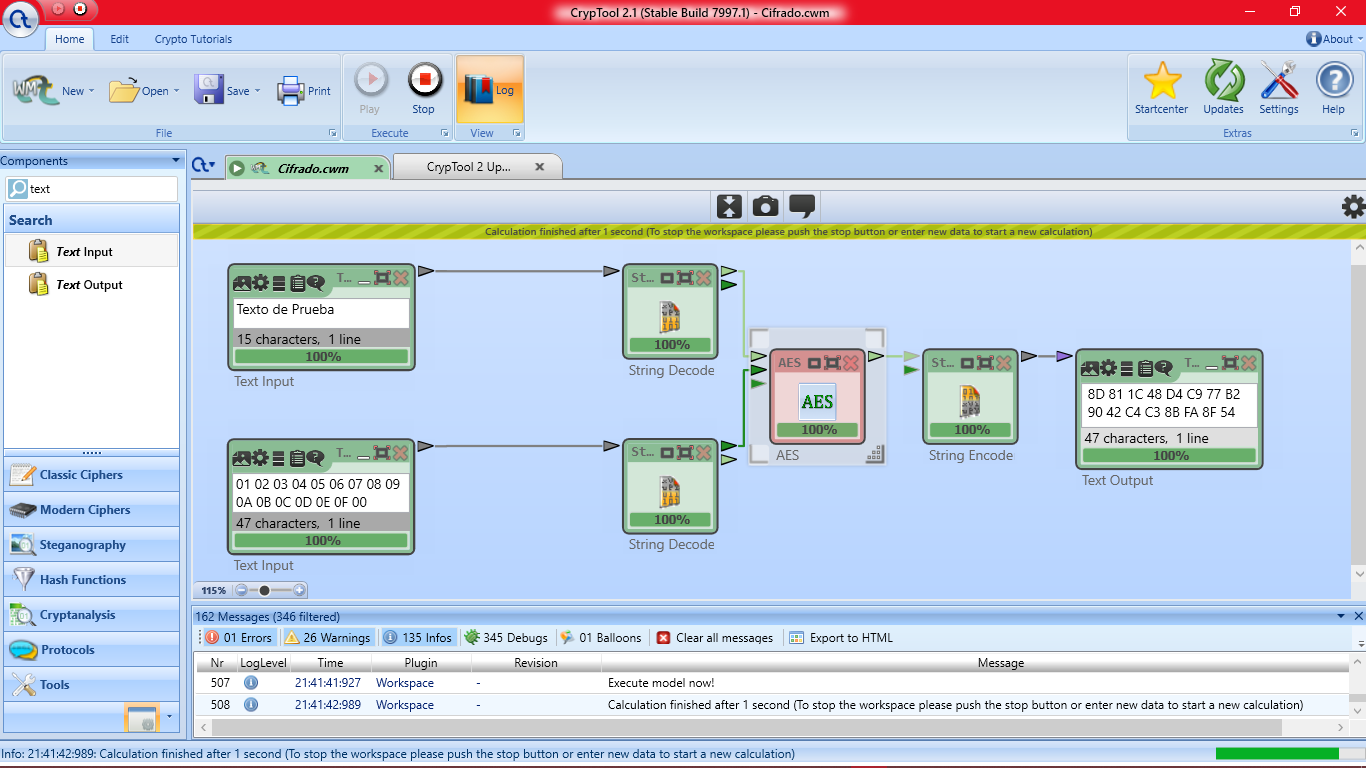


* Generar claves AES con el generador de valores aleatorios (RND).

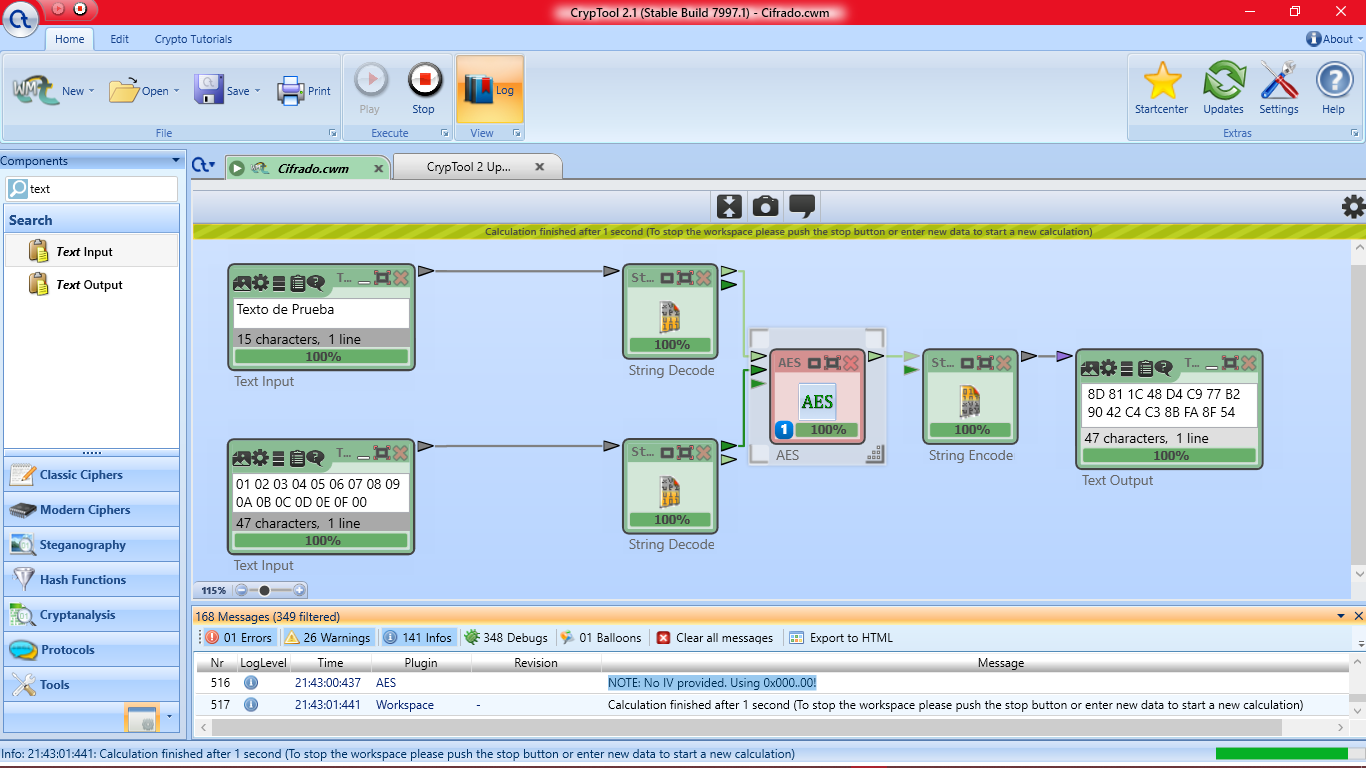


* Verificar con qué métodos de cifrado (ECB, CBC y CFB) es necesario utilizar IV. Probar los diferentes métodos.

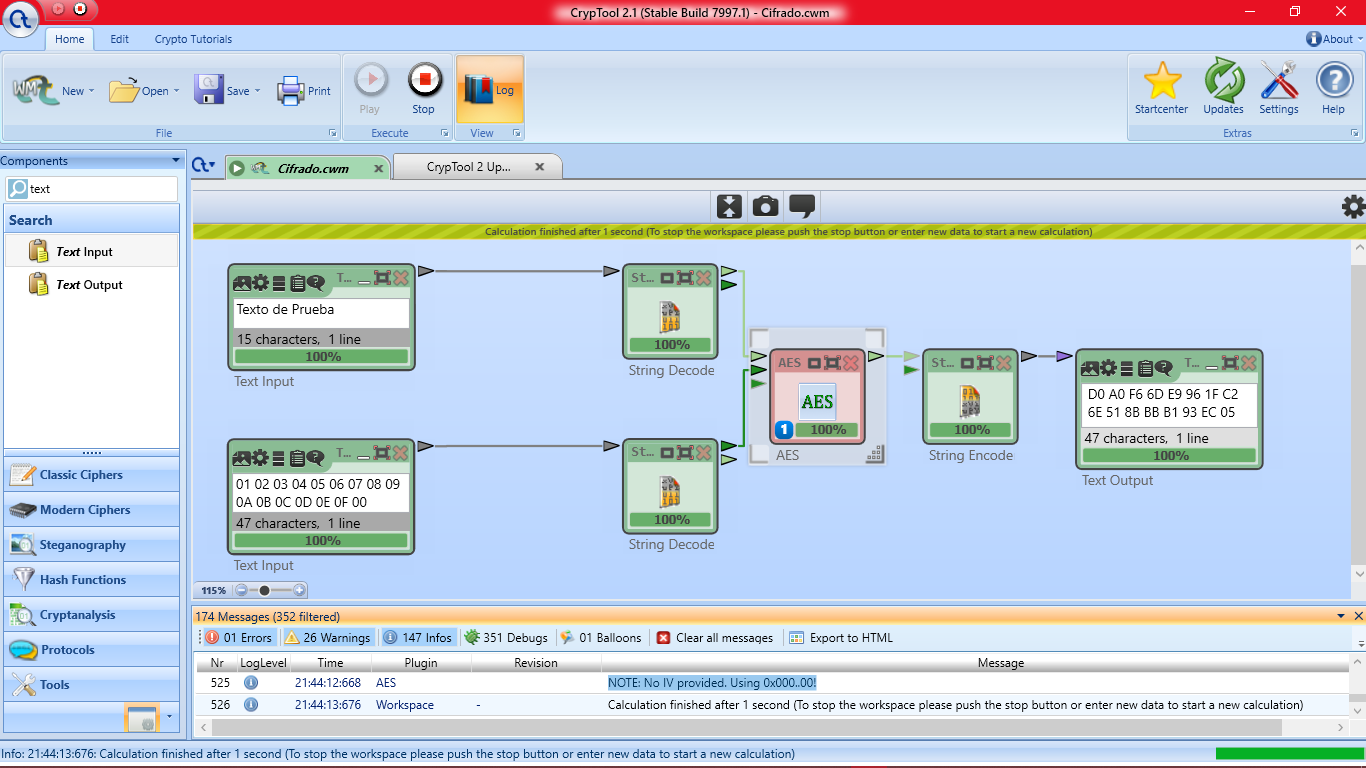
**ECB**



**CBC**

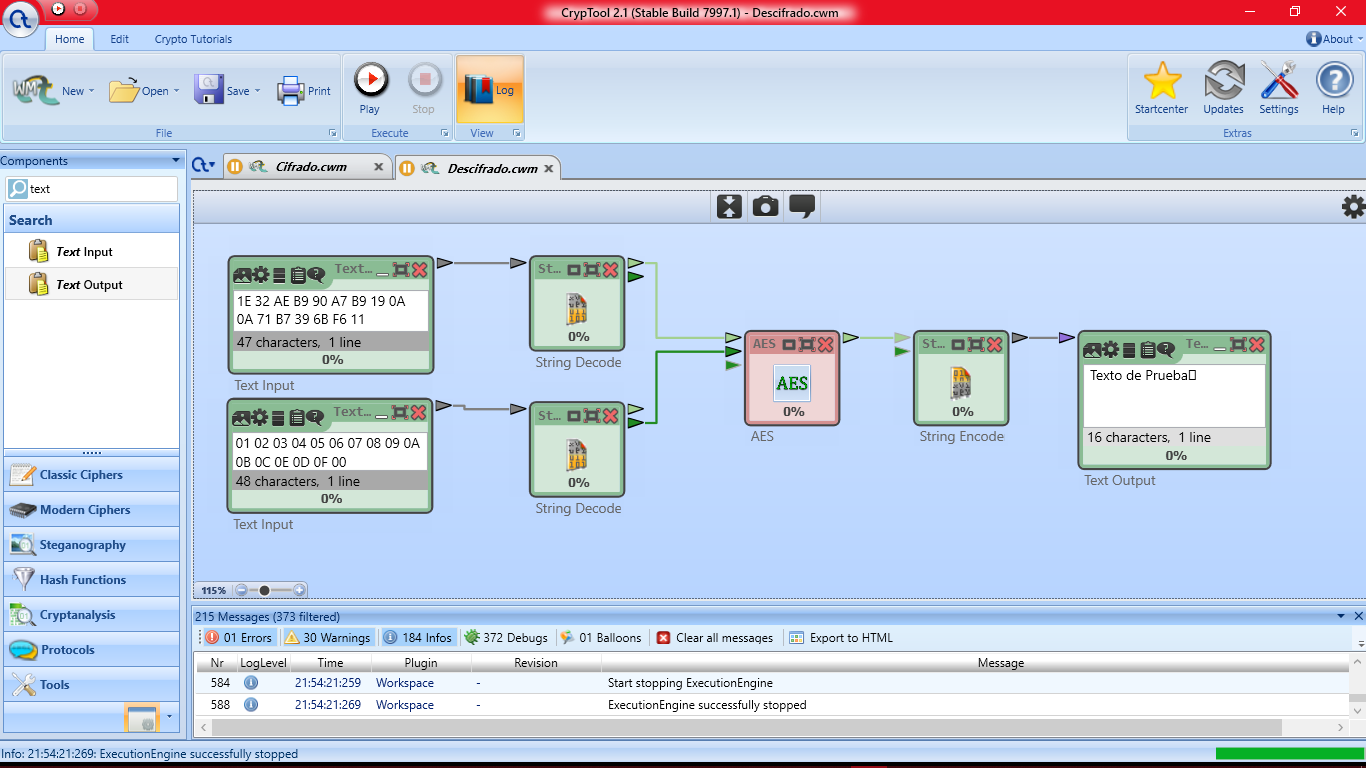


**CFB**



* Verificar el comportamiento al utilizar un texto en claro con longitud no múltiplo del tamaño del bloque (128 bits), con las diferentes opciones de relleno (padding mode) y diferentes métodos de cifrado (Chaining mode).

**Zeros**



**Padding**

