**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**

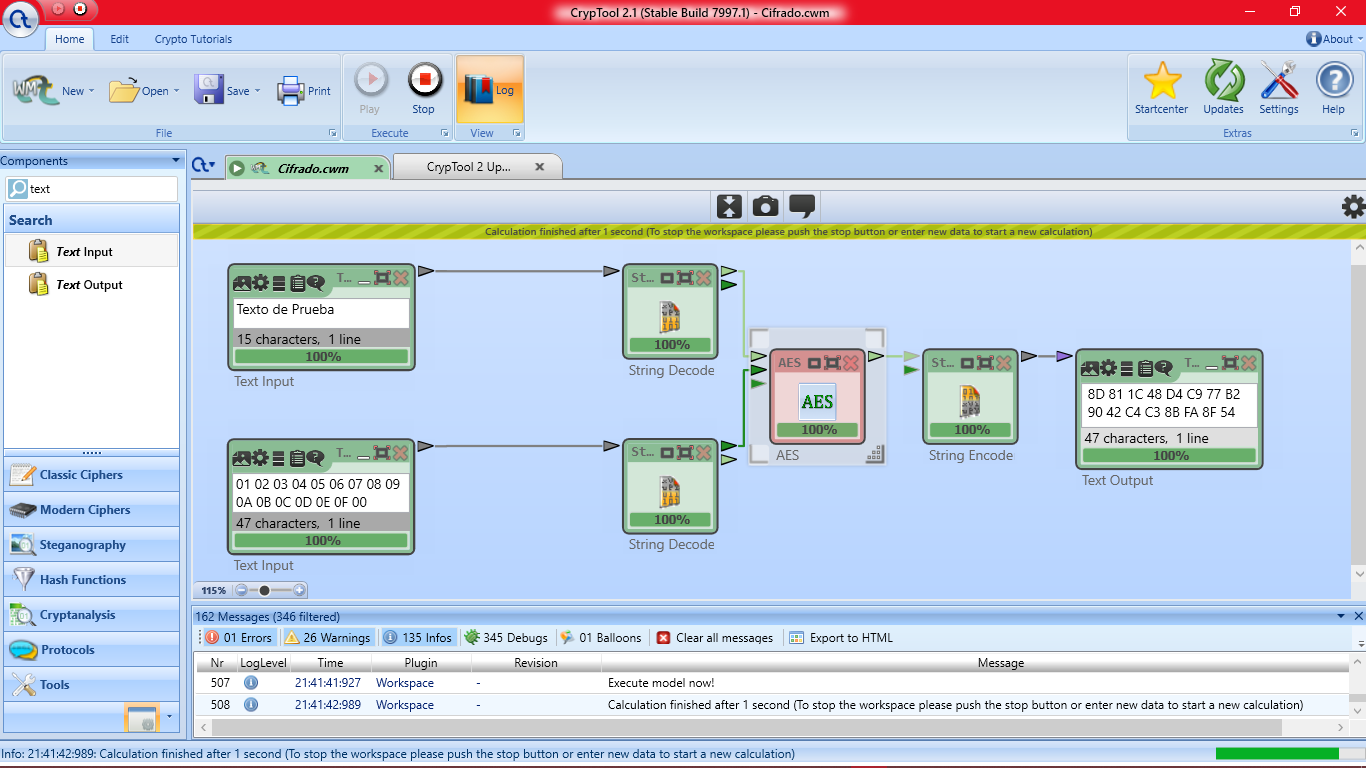
**Algoritmos de Cifrado Simétrico**

**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.

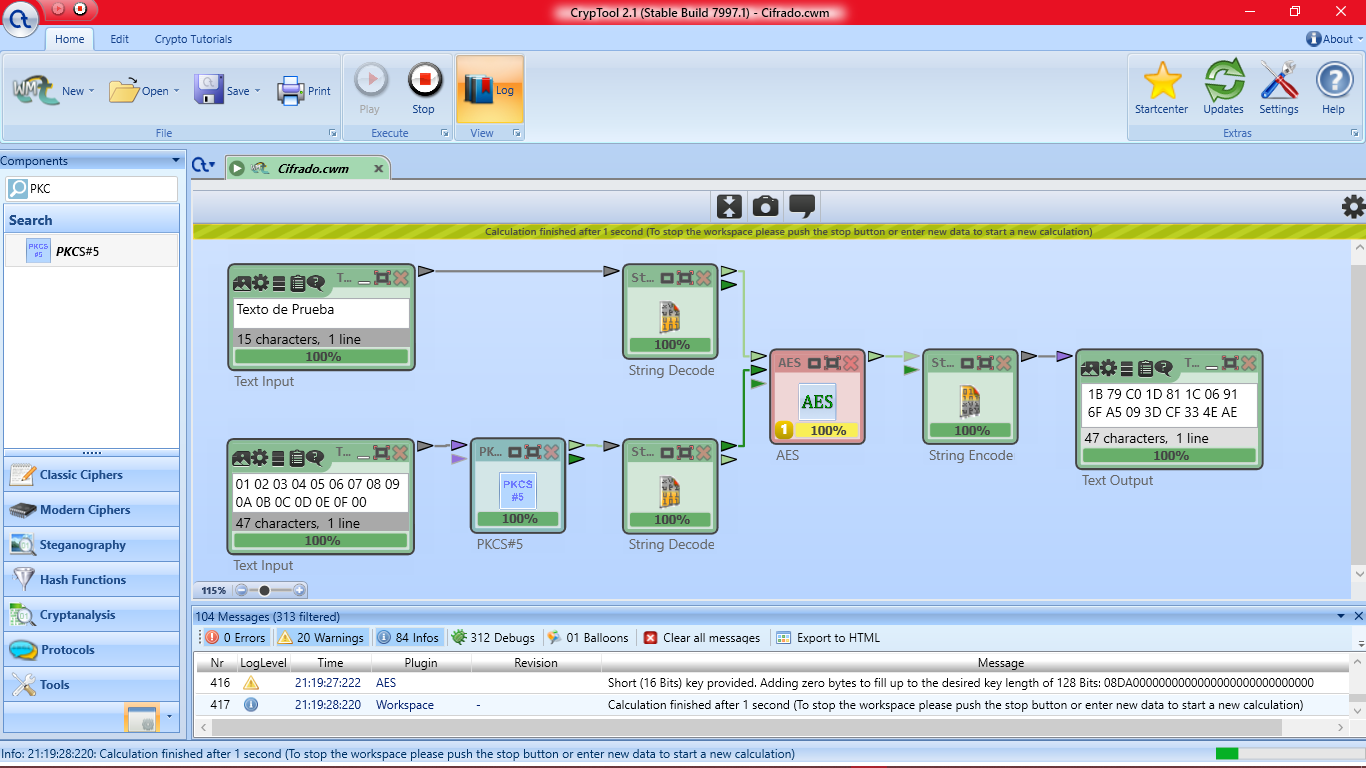
**Cifrado con AES**

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.

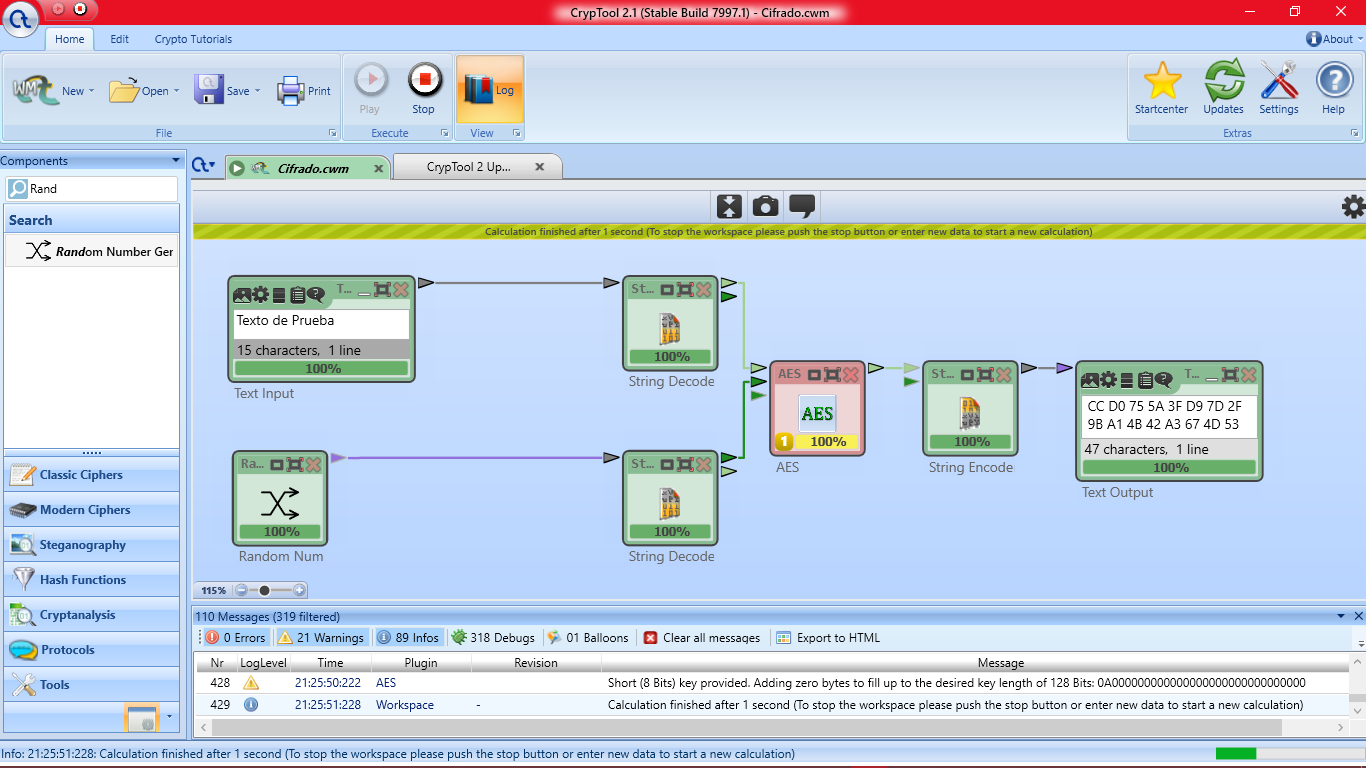


**Se pide:**

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



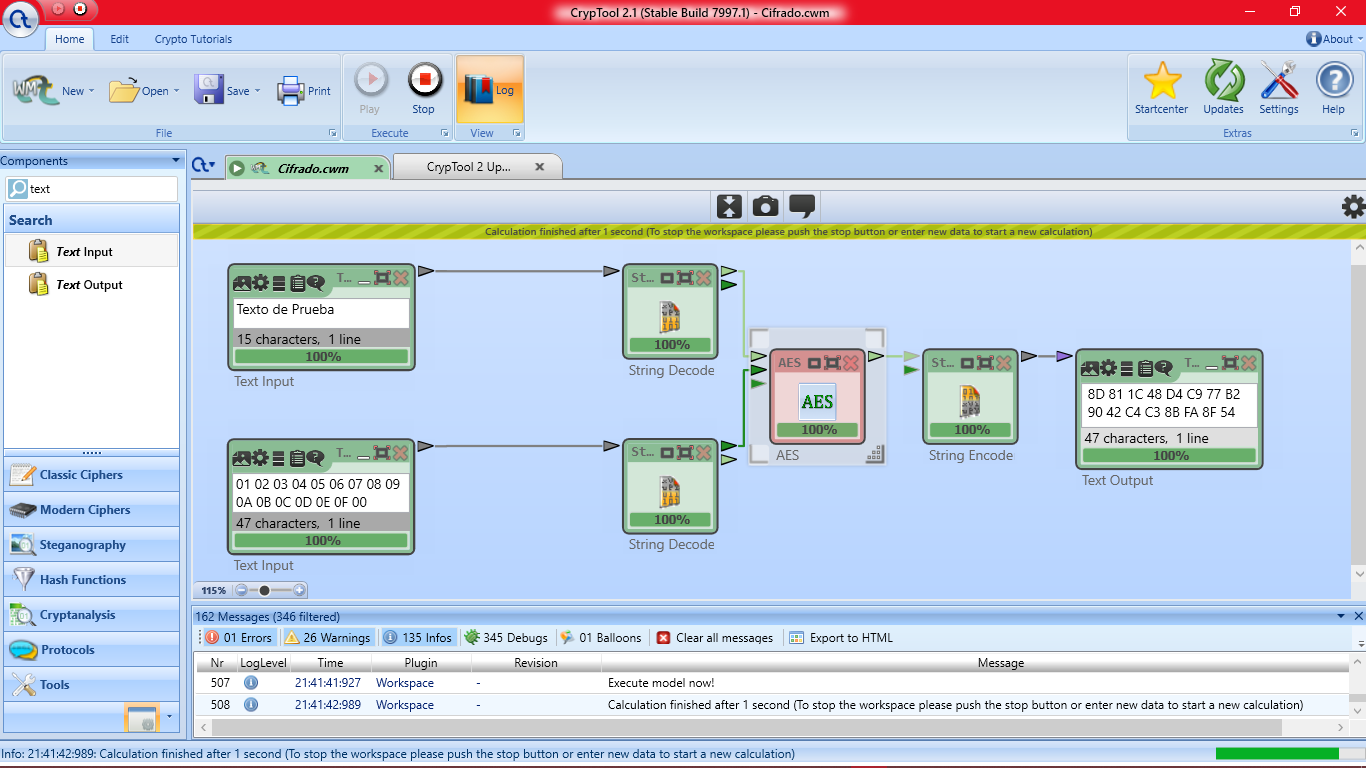
* Generar claves AES con el generador de valores aleatorios (RND).



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

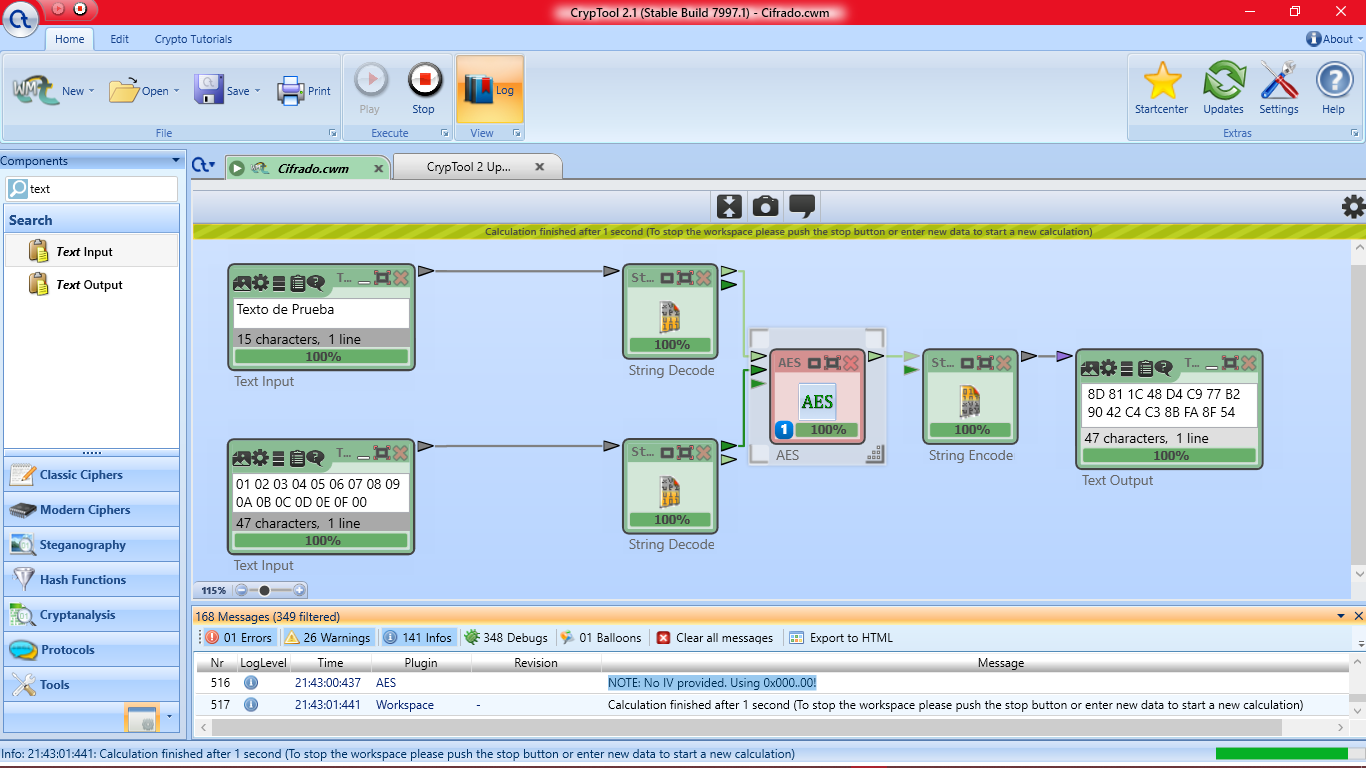
**ECB**

El más sencillo es el modo *electronic codebook* (ECB), en el cual los mensajes se dividen en bloques y cada uno de ellos es cifrado por separado utilizando la misma clave K. La desventaja de este método es que a bloques de texto plano o claro idénticos les corresponden bloques idénticos de texto cifrado, de manera que se pueden reconocer estos patrones como guía para descubrir el texto en claro a partir del texto cifrado. De ahí que no sea recomendable para protocolos cifrados.



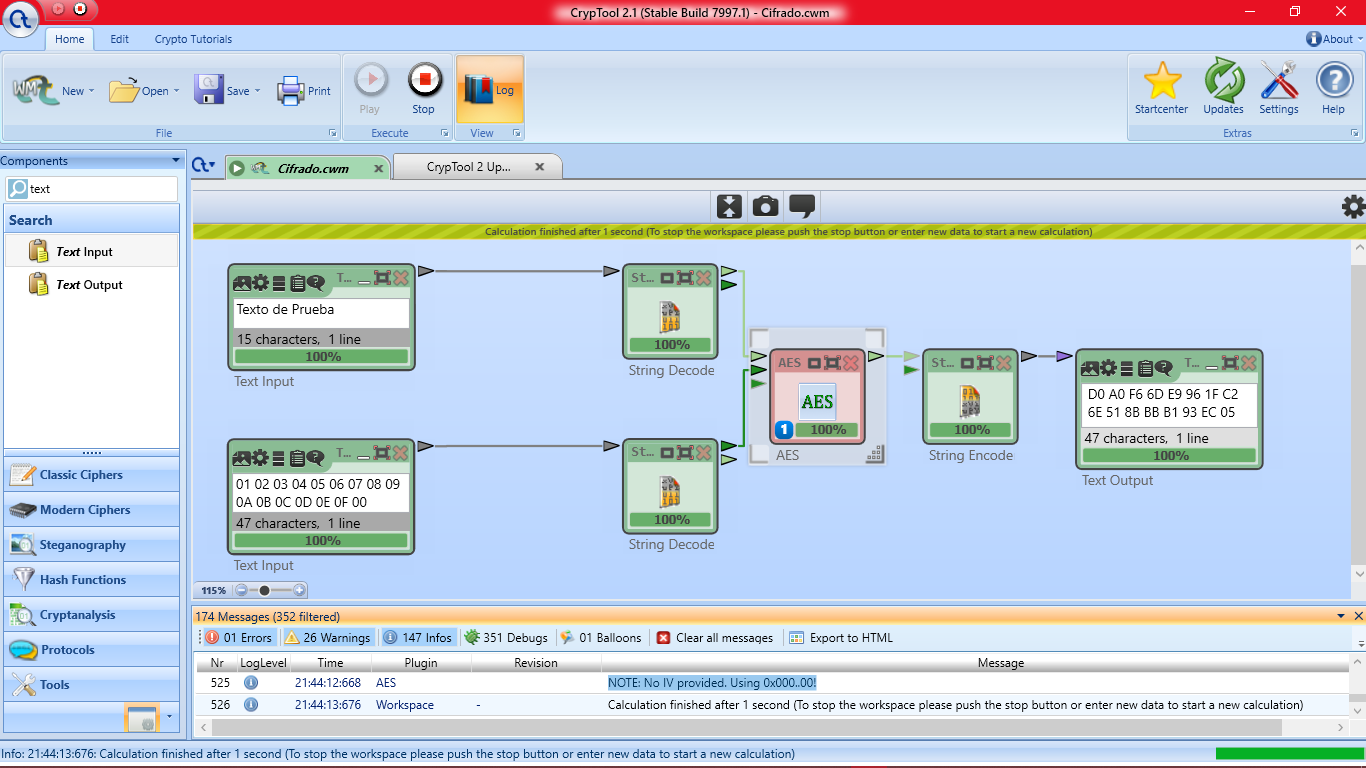
**CBC**

En el modo *cipher-block chaining*(CBC), a cada bloque de texto plano se le aplica la operación [XOR](https://es.wikipedia.org/wiki/Puerta_lógica" \l "Puerta_O-exclusiva_(XOR))con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. Para hacer cada mensaje único se utiliza asimismo un vector de inicialización.



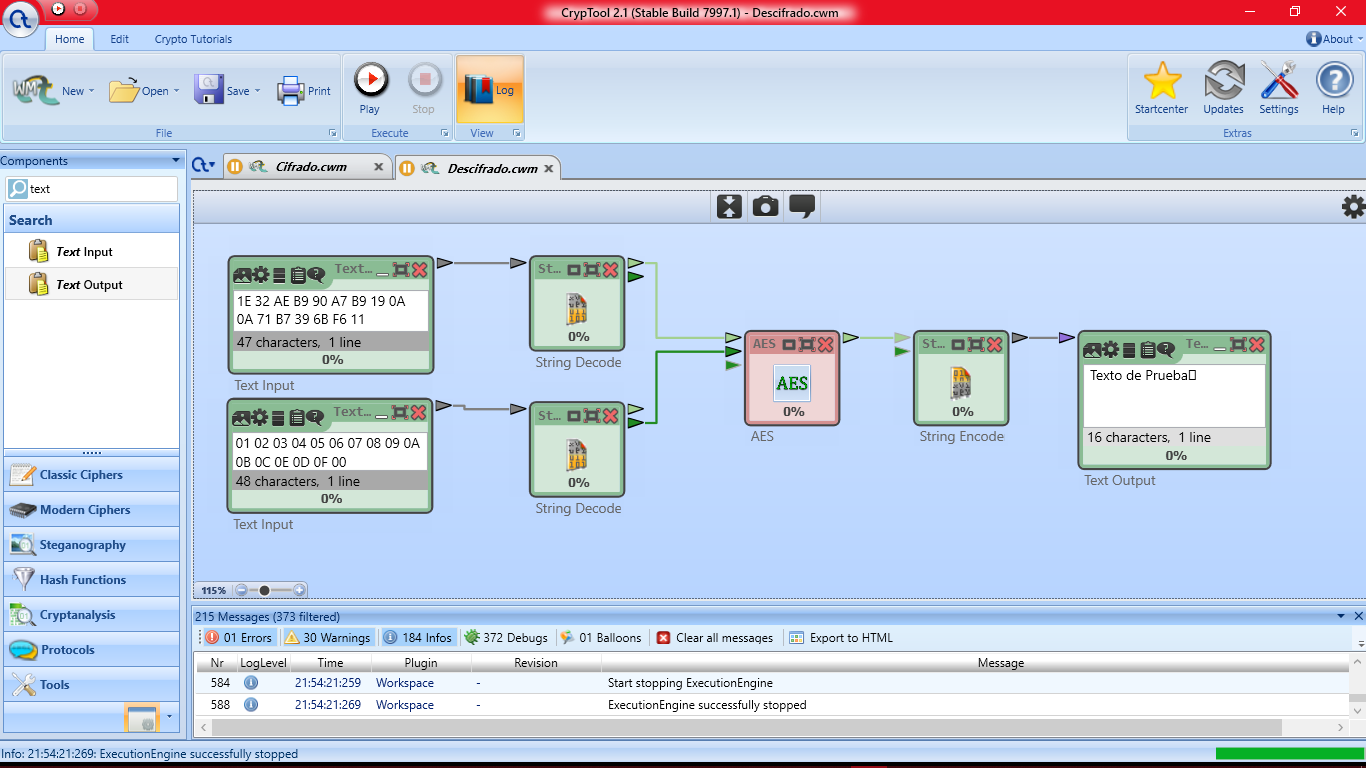
**CFB**

El modo *cipher feedback*(CFB) hace que el cifrado en bloque opere como una unidad de [flujo de cifrado](https://es.wikipedia.org/wiki/Flujo_de_cifrado): se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado.



* 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**

