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.

Analizar cómo funciona AES viendo la animación flash proporcionada en Cryptools 1.4.

Utilizando CrypTool 2.0, diseñar un sistema de cifrado y descifrado con AES.

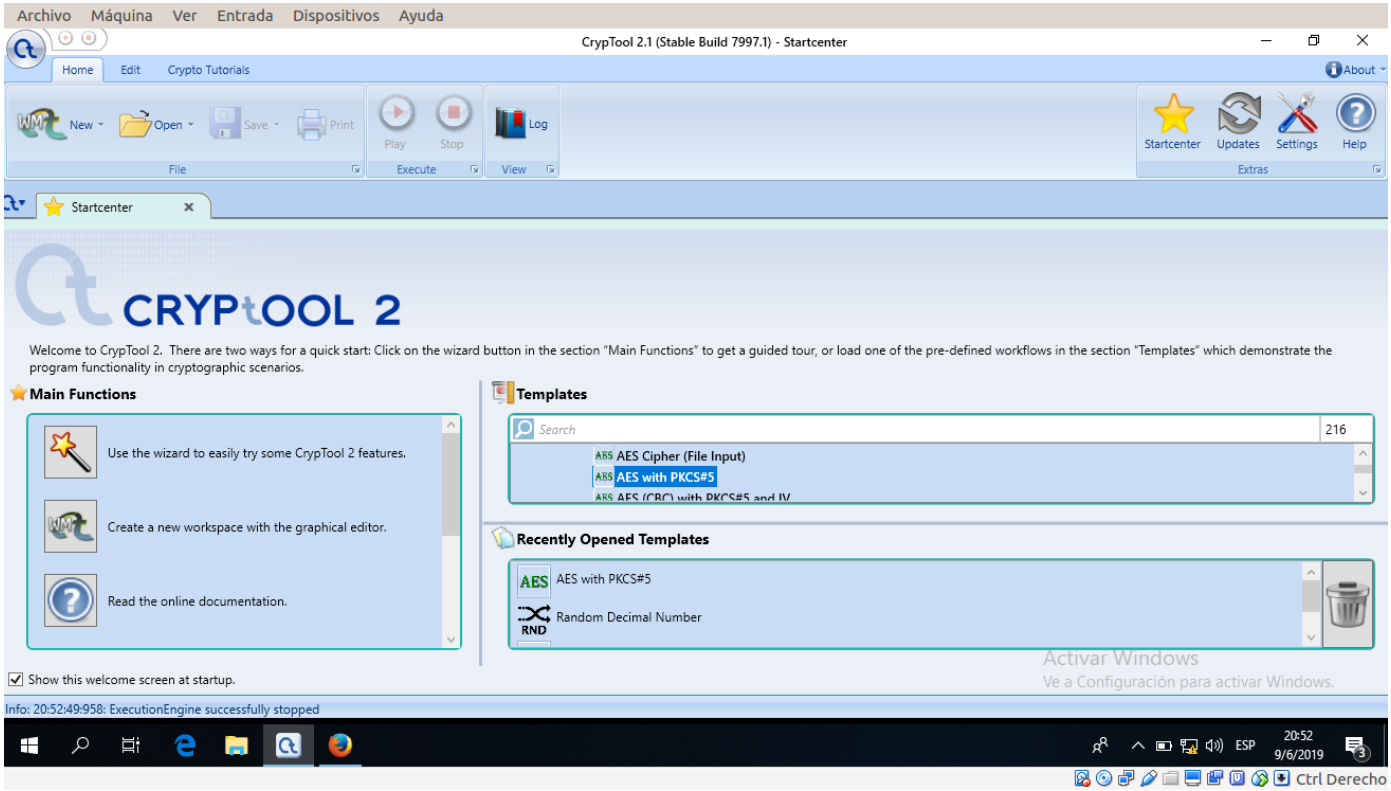
Se puede usar un módulo TextInput o bien un módulo RandomInputGenerator para alimentar la clave y el IV. Utilizar módulos TextInput y TextOutput para introducir el texto en claro y visualizas los resultados.

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.

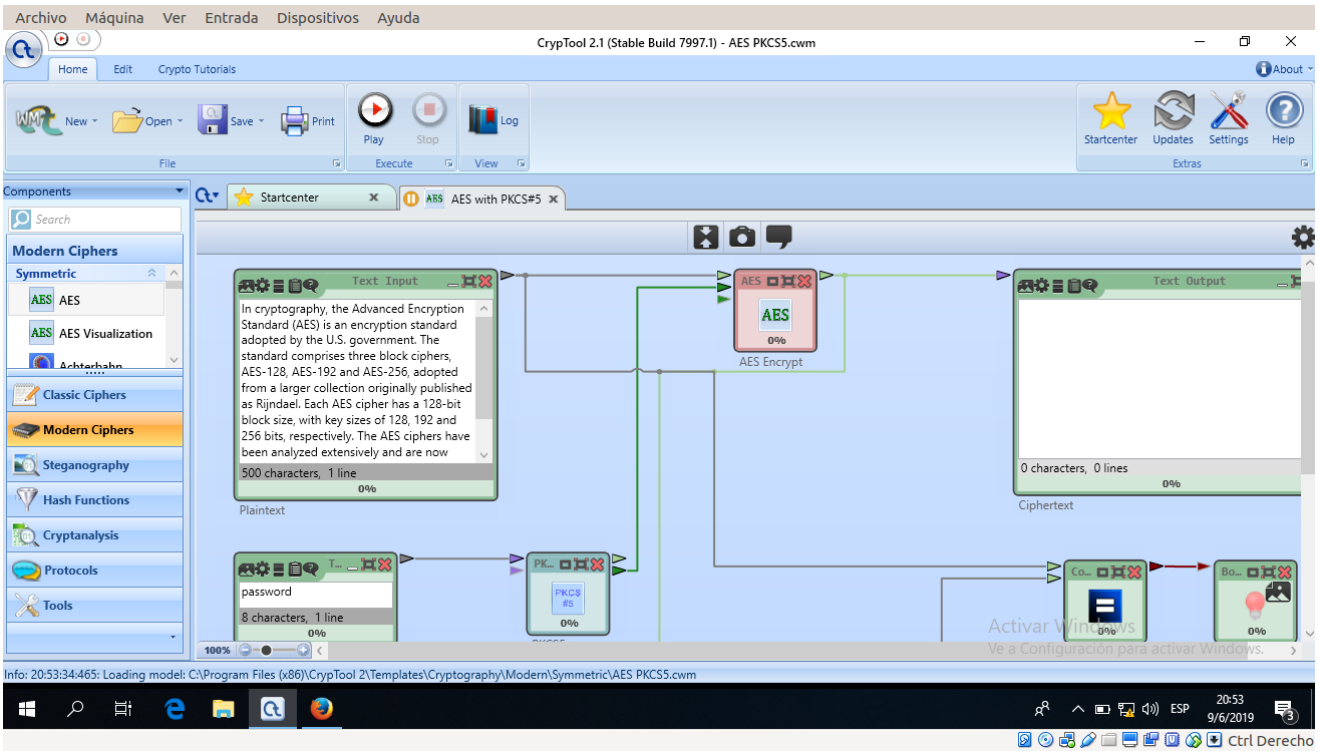
Se pide

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

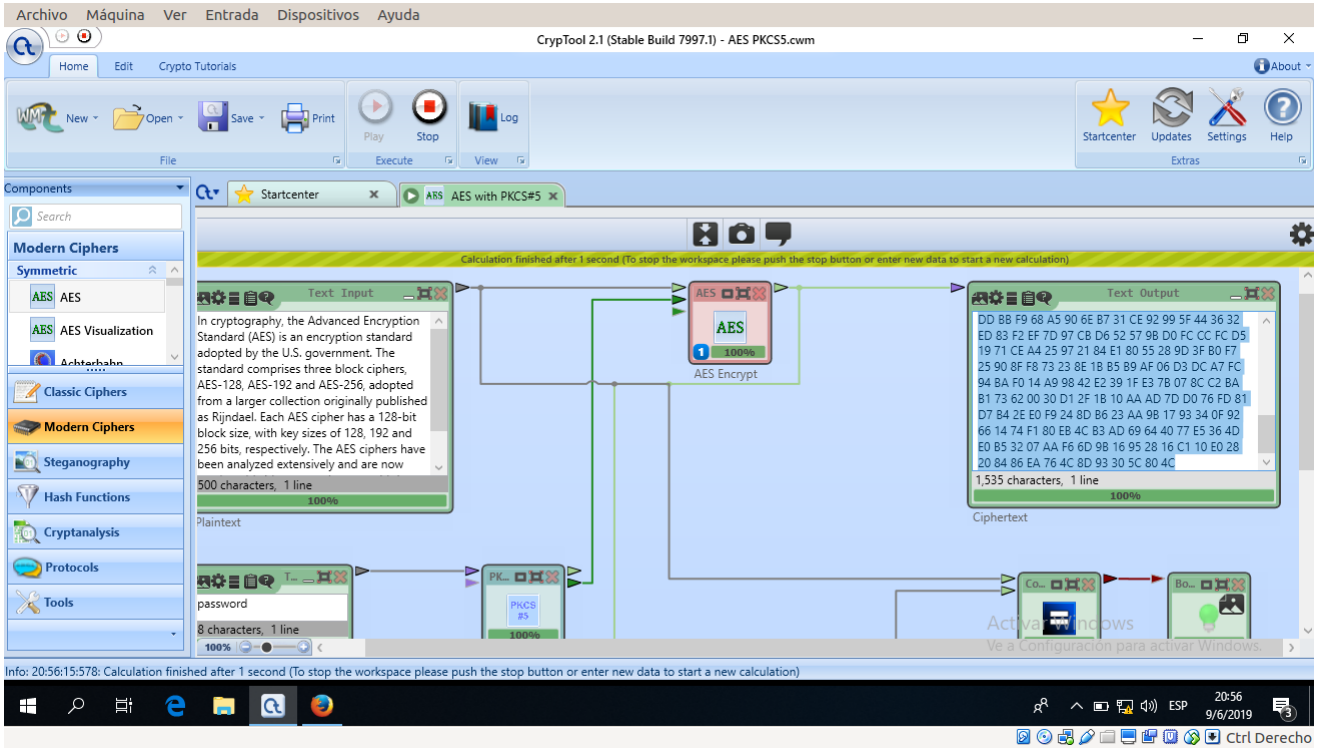
Primeramente, seleccionaremos la template AES (CBC) with PKCS#5



Como segundo paso tenemos la siguiente interfaz que nos demuestra los procedimientos que son empleados para cifrar un mensaje que aparece en la parte superior utilizando una contraseña especificada en la parte inferior.

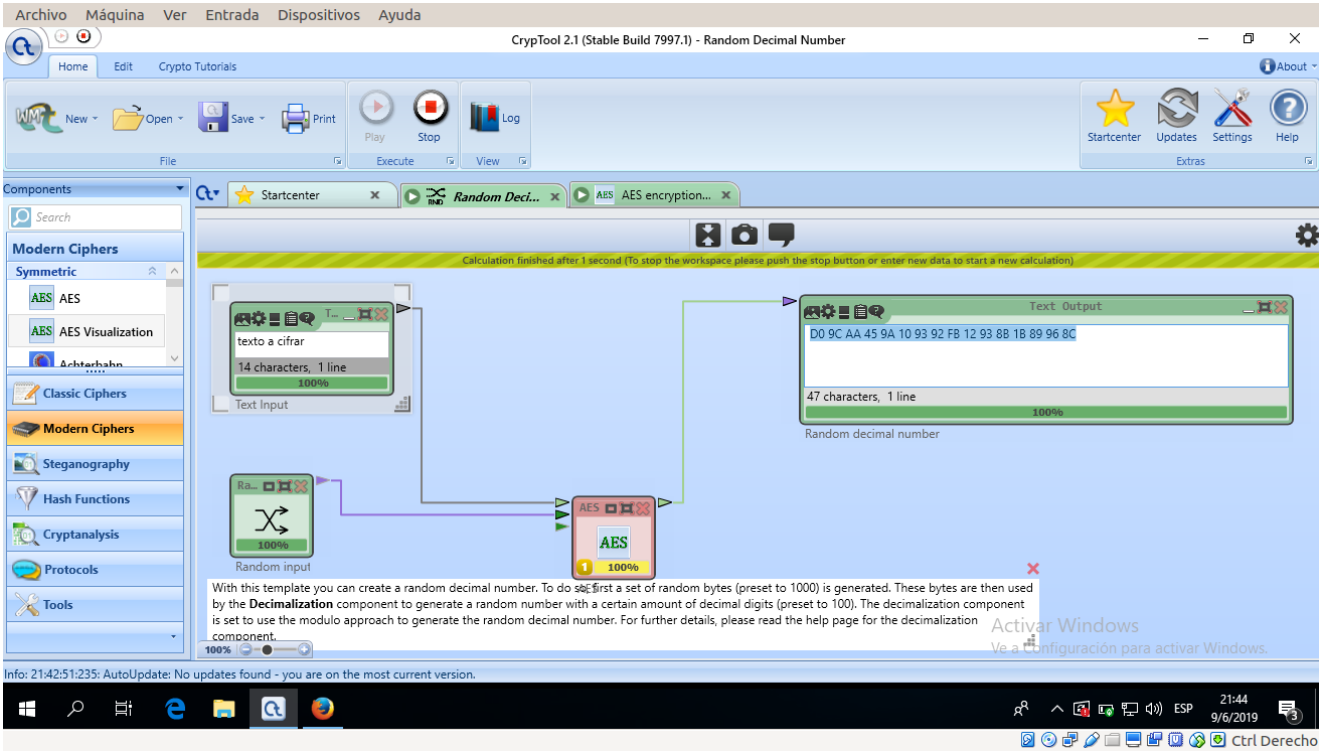


El tercer paso sería darle clic al botón superior que dice play para que empiece la generación de la clave. Dando como resultado la siguiente secuencia de caracteres que sería el texto anteriormente visto solo que ahora está cifrado.



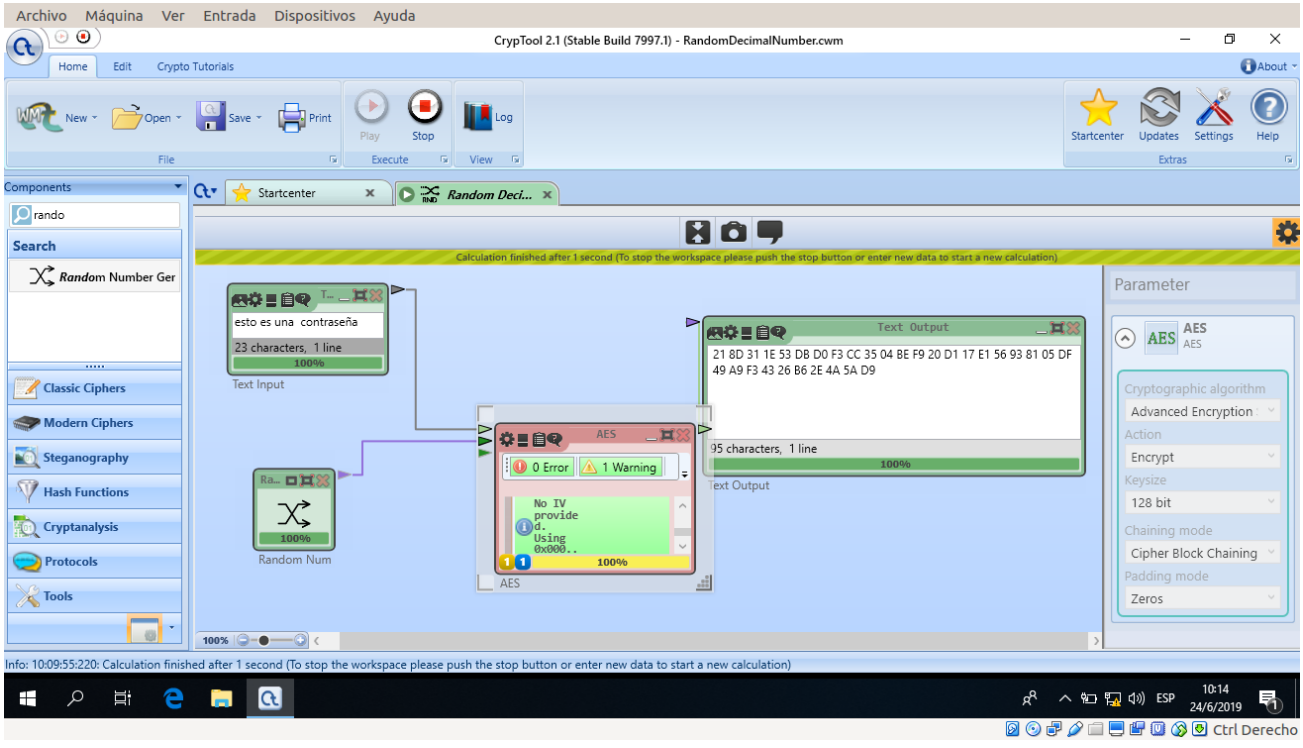
2. **Generar claves AES con el generador de valores aleatorios (RND).**

El primer paso sería colocar un random input esto nos generará valores aleatorios para que después se lo pasemos a AES y este nos genere con un text input una cadena que será el texto cifrado teniendo como password el valor aleatorio generado.



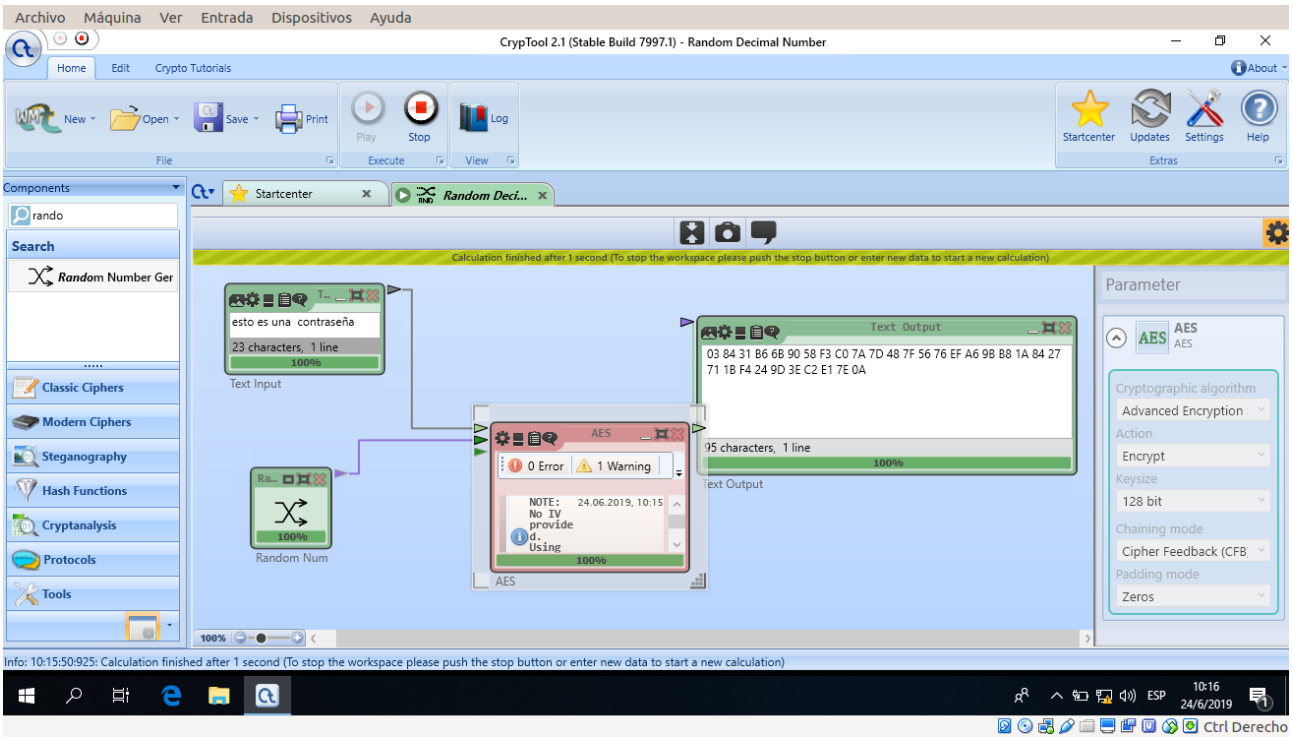
3. **Verificar con qué métodos de cifrado (ECB, CBC y CFB) es necesario utilizar IV. Probarlos diferentes métodos.**

CBC



Este necesita un vector de inicialización para hacer cada mensaje único

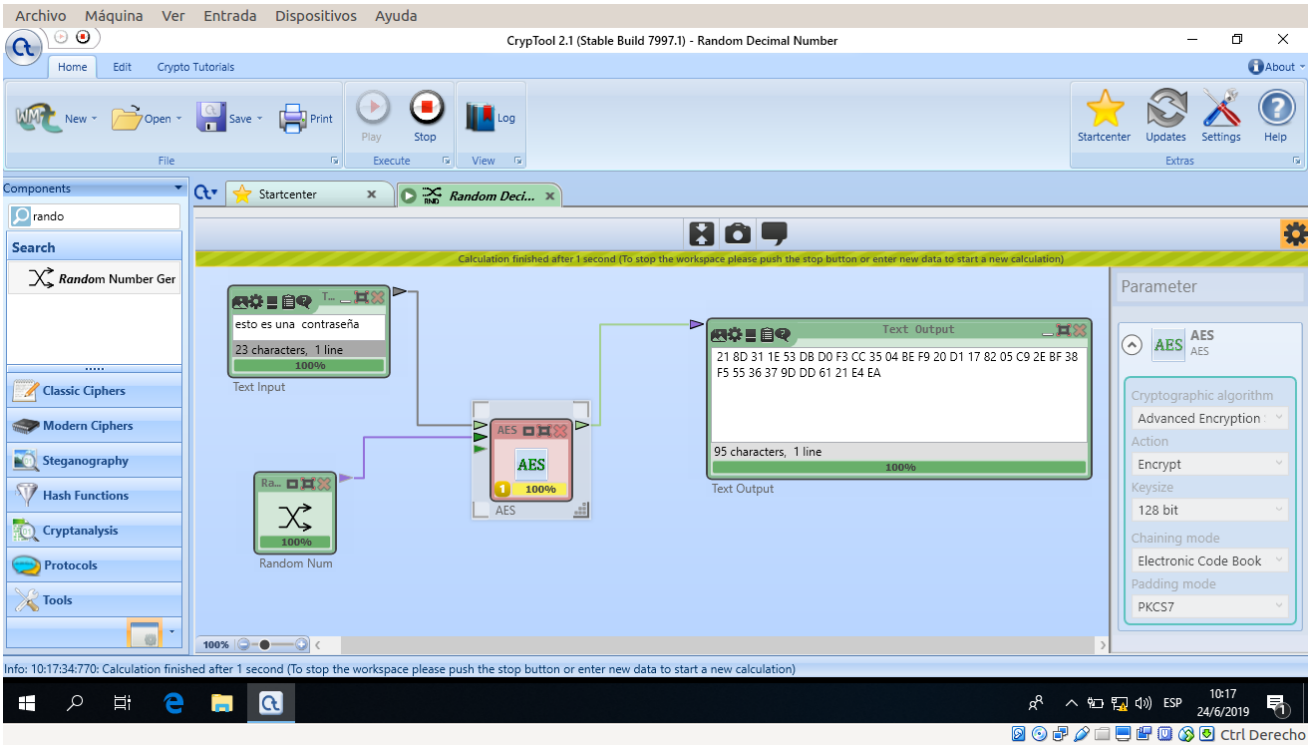
CFB



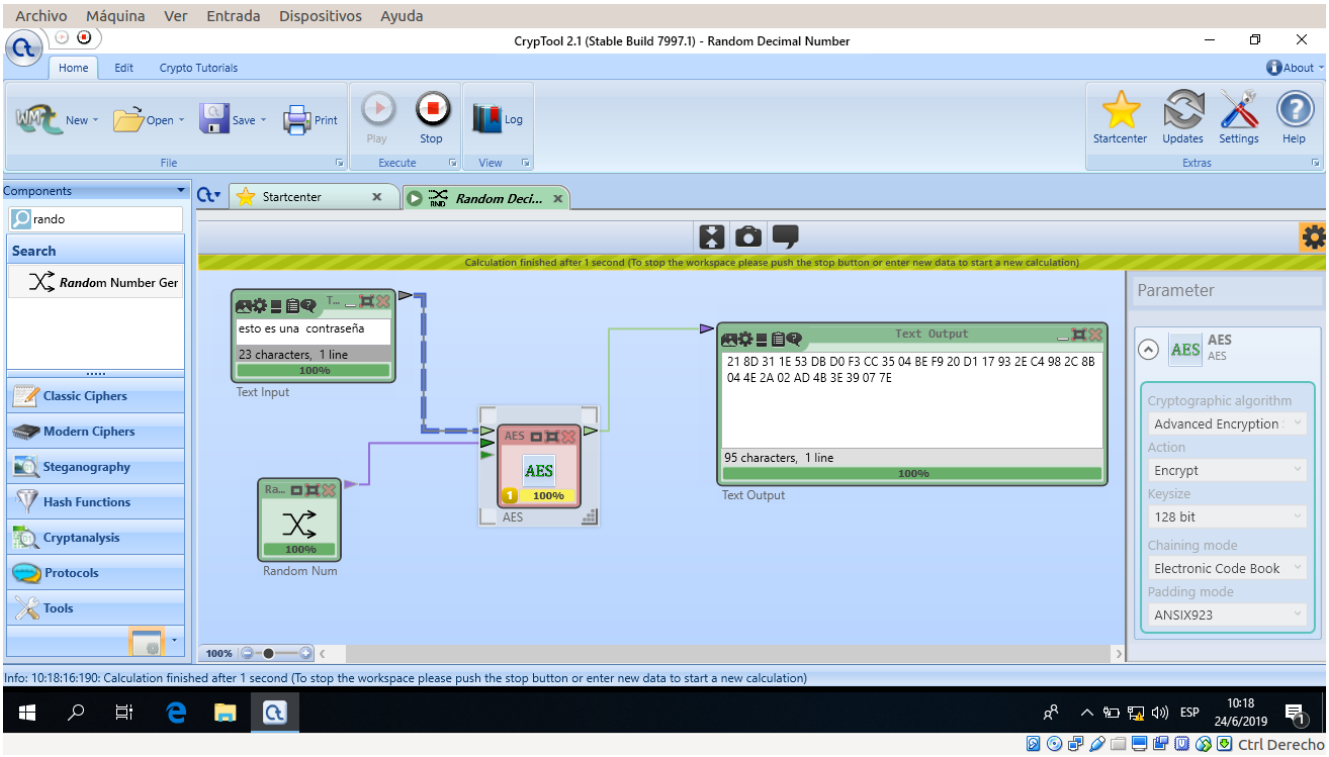
CFB necesita un vector de inicialización de igual manera

4. **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).**

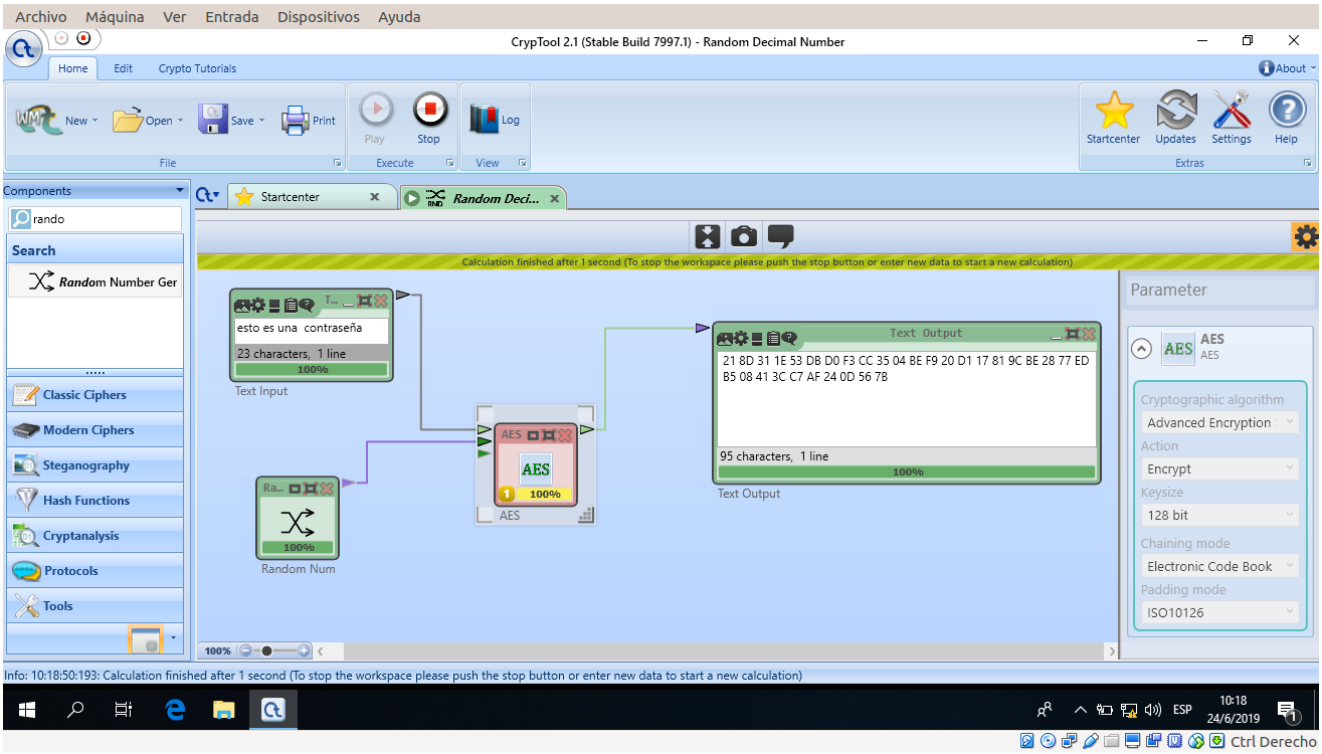
ECB – PKCS7



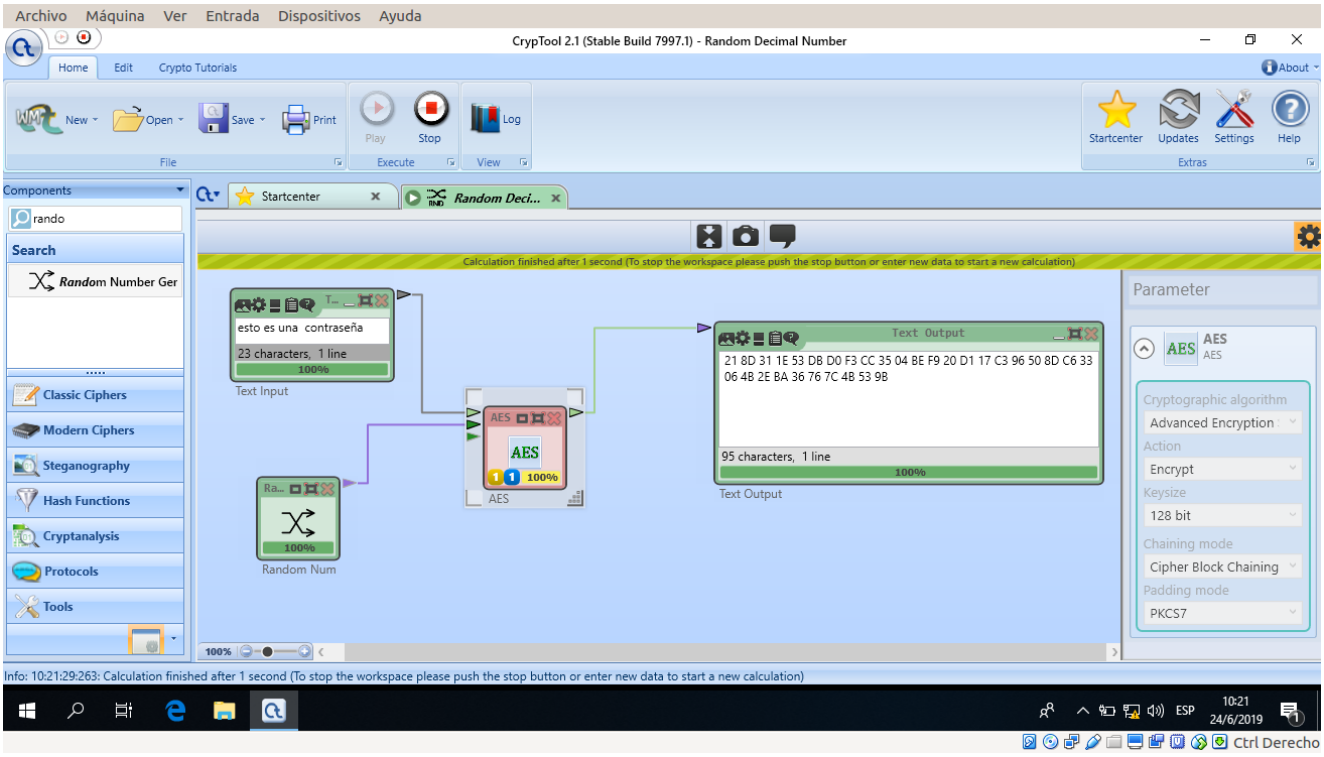
ECB – ANSIX923



ECB – ISO10126

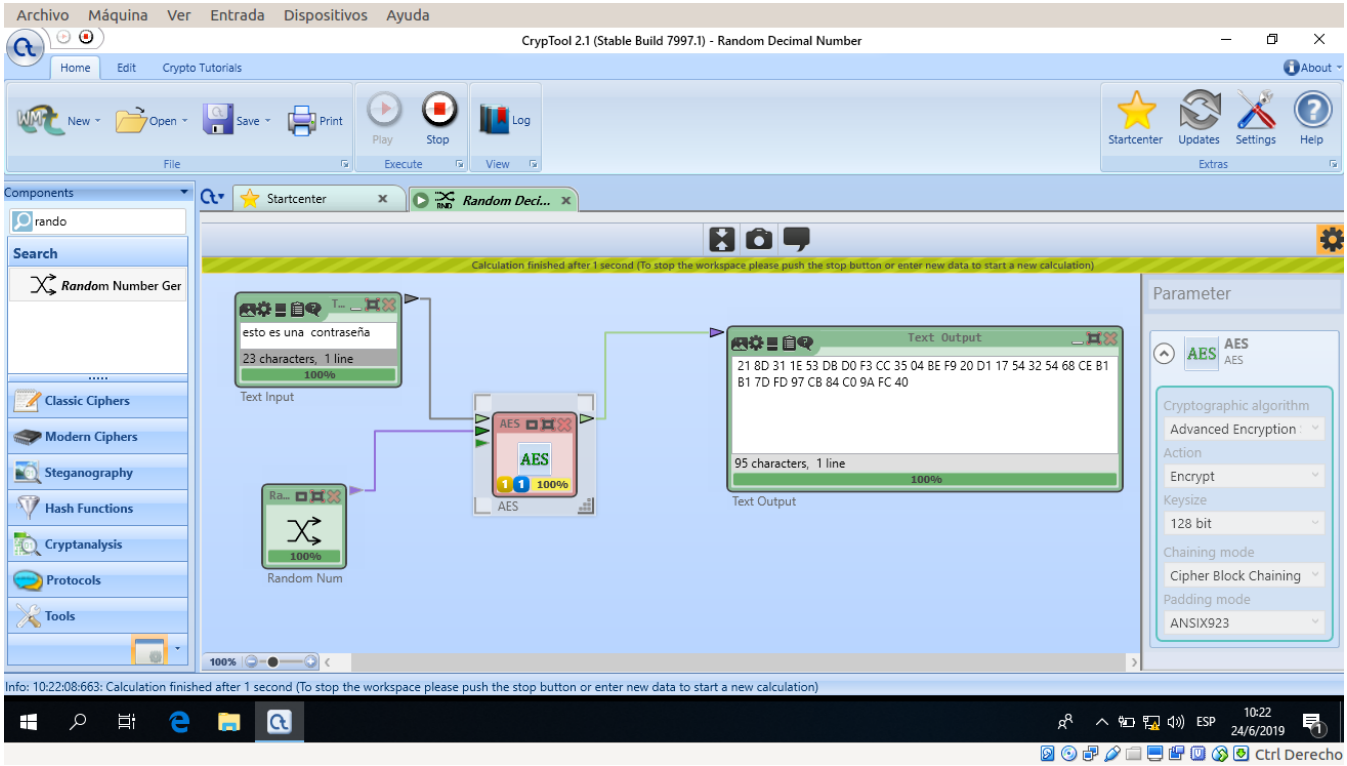


CBC – PKCS7

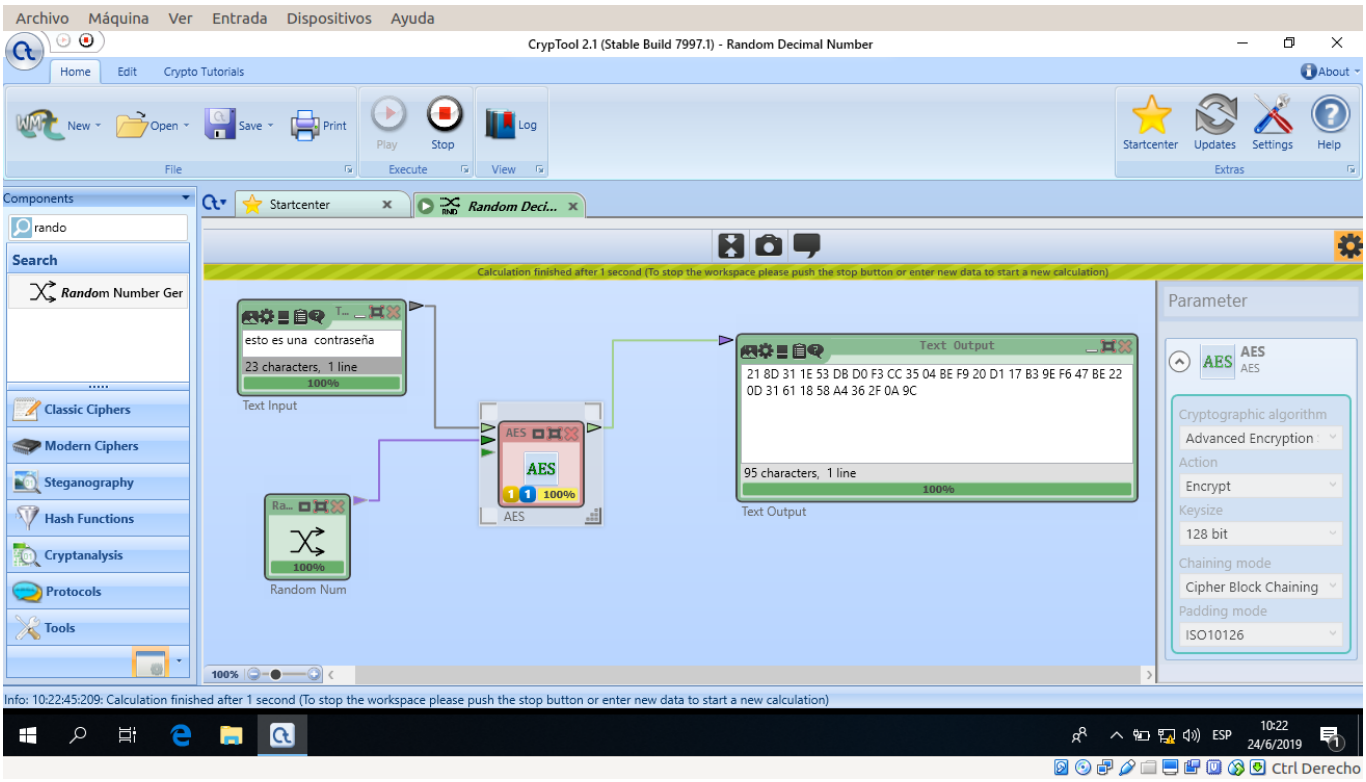


CBC– ANSIX923

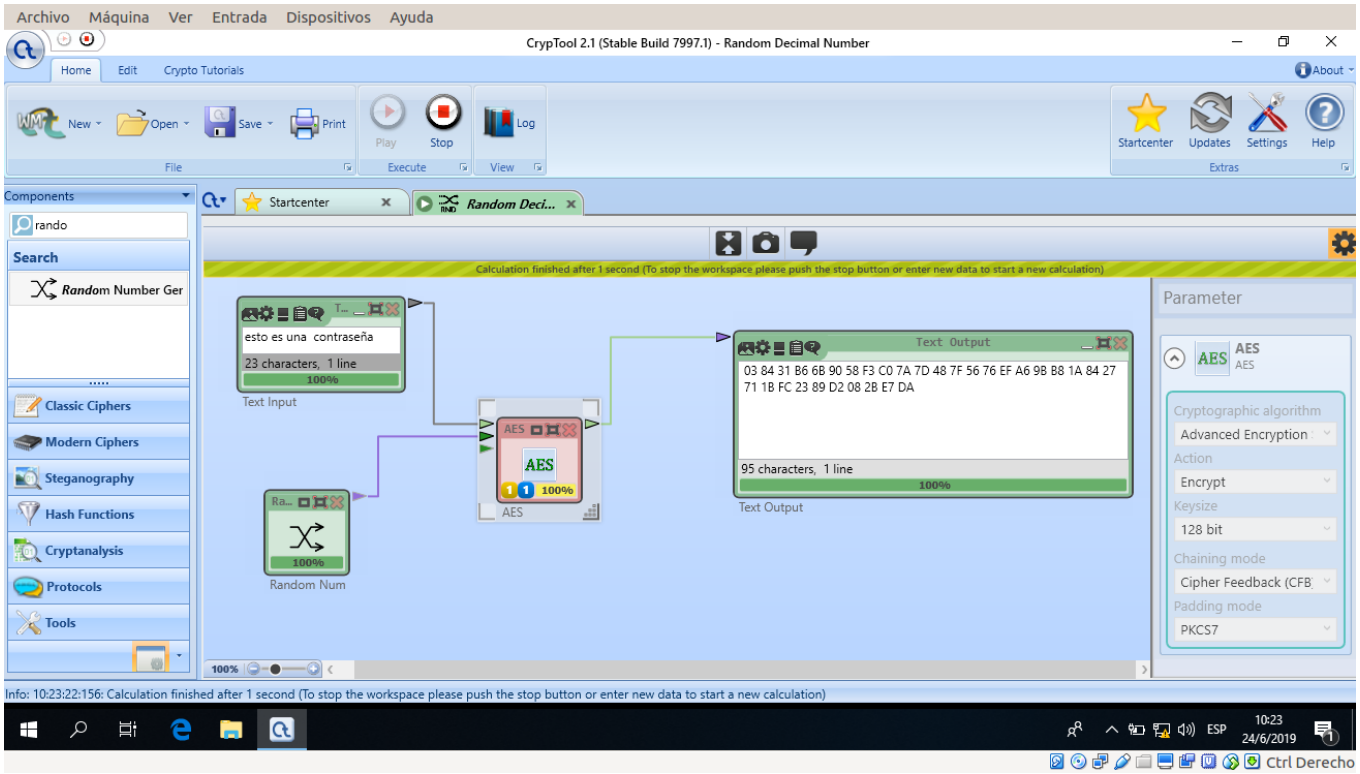
\



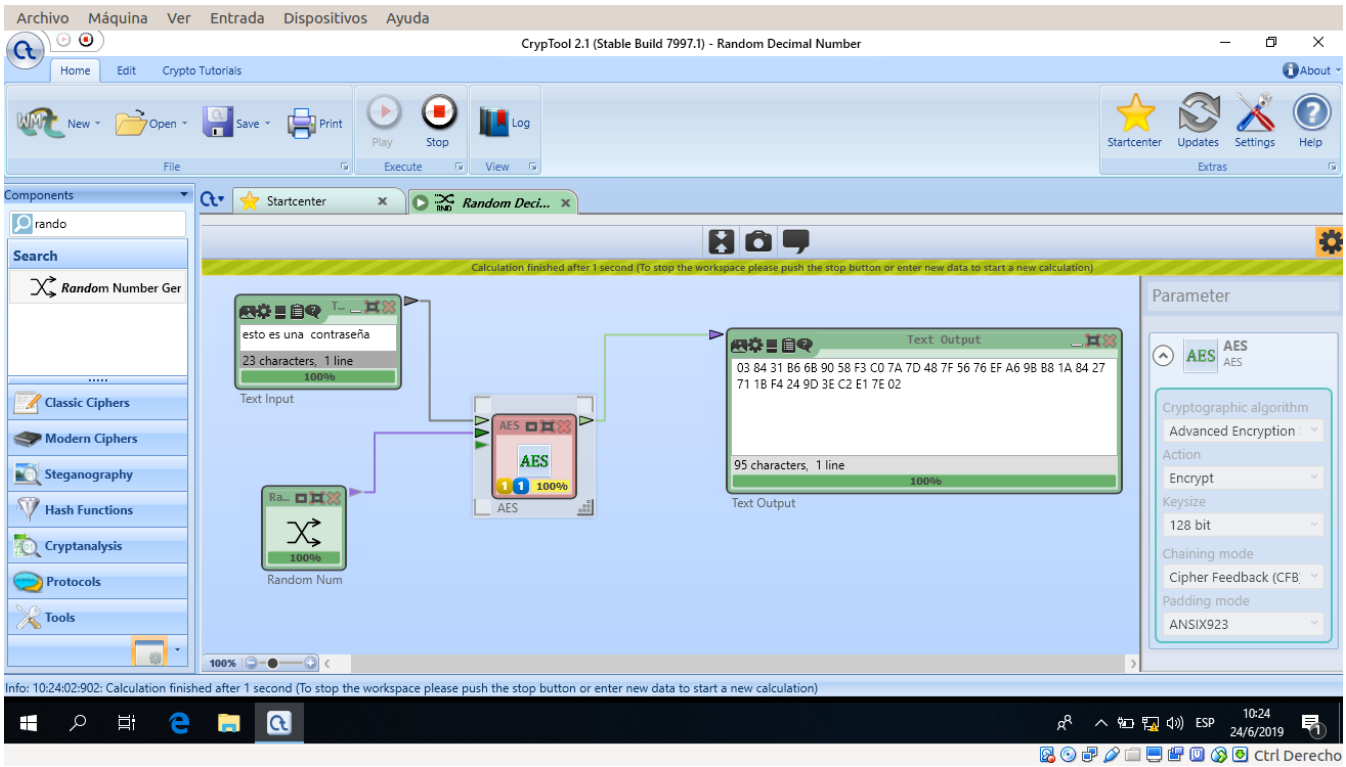
CBC – ISO10126



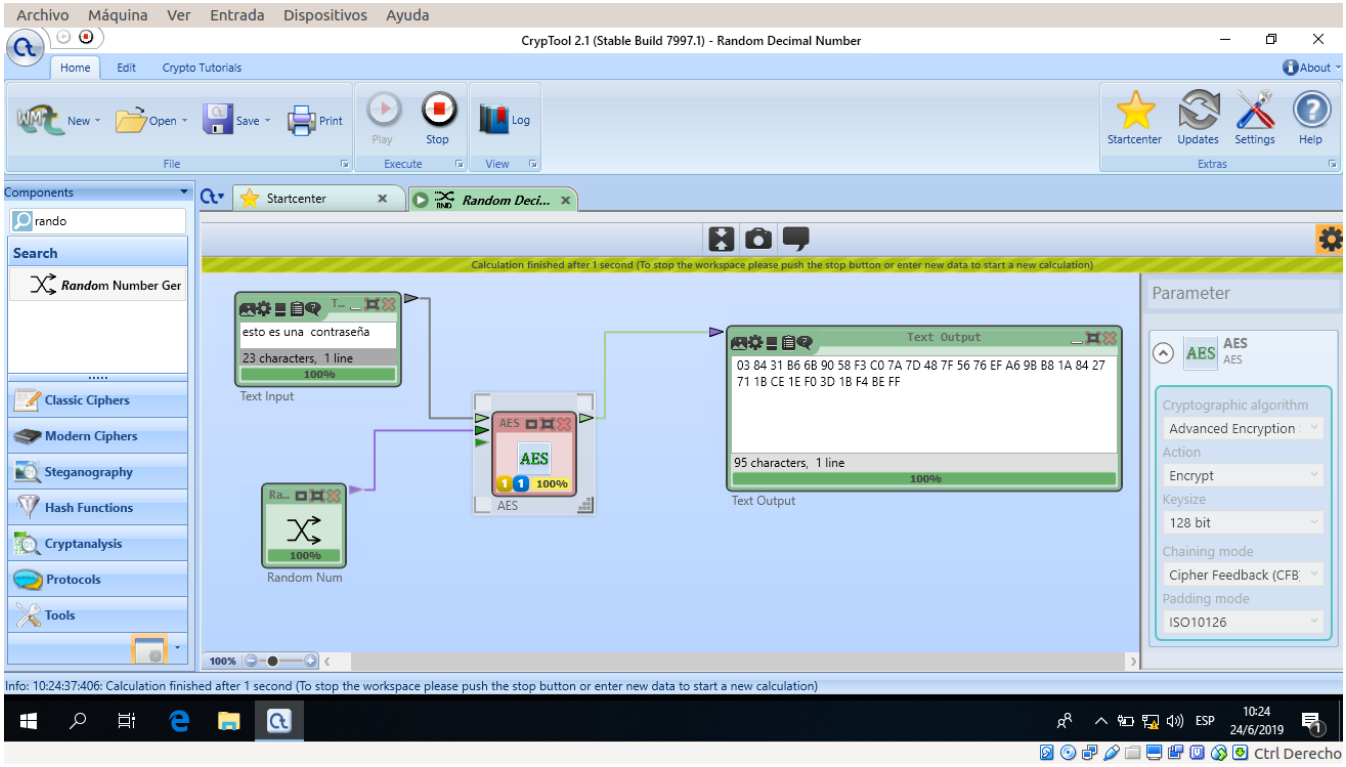
CFB – PKCS7



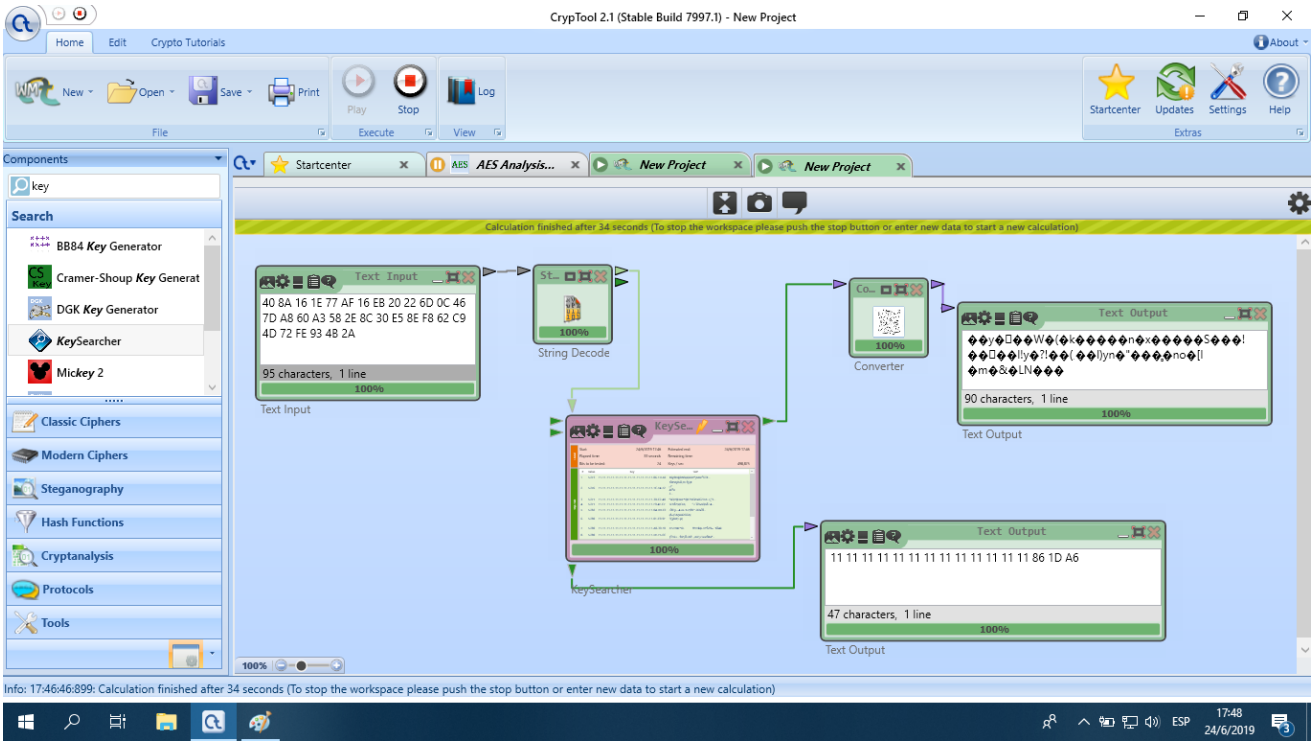
CFB – ANSIX923



CFB – ISO10126

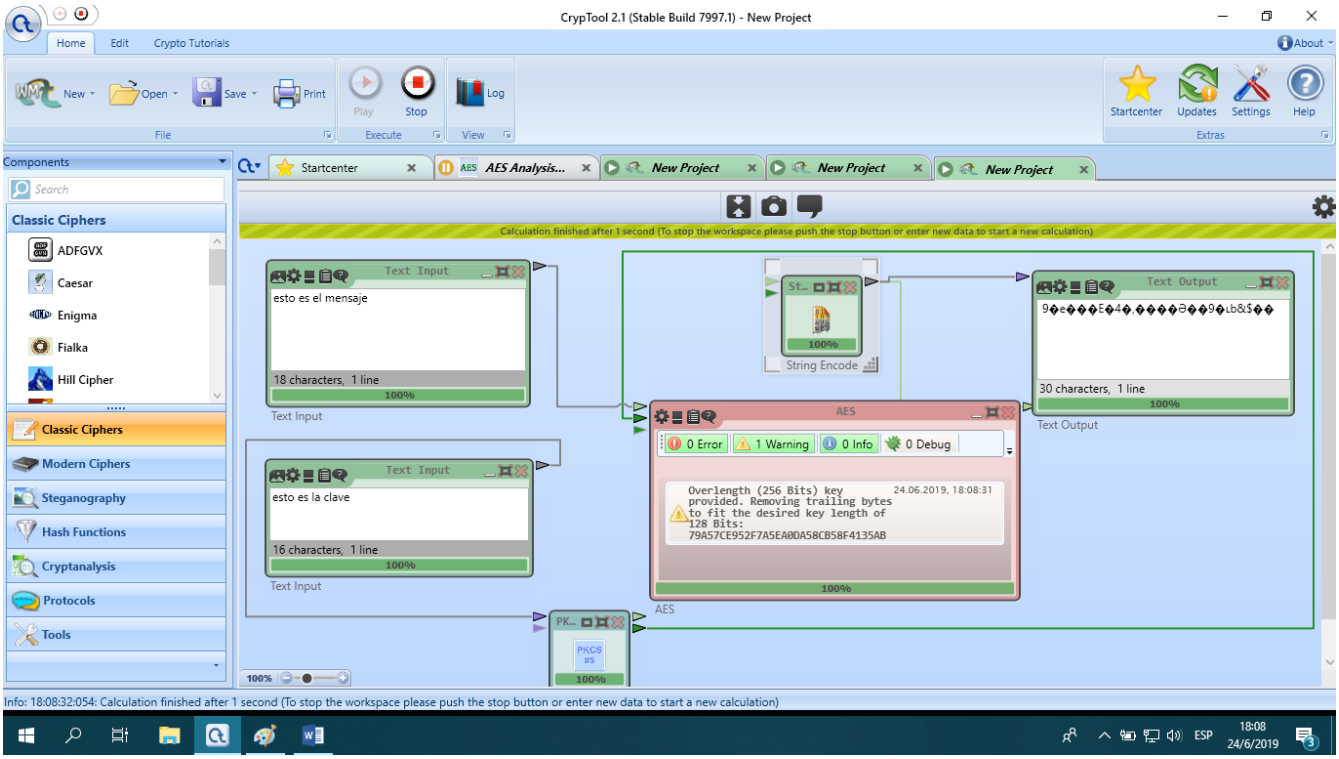


5. **Verificar cómo un cifrado moderno (AES) rompe los parámetros estadísticos del texto en claro.**



Los rompe ya que no es computacionalmente calculable

6. **Verificar cómo se propaga un error en los métodos de cifrado con realimentación.**



R: Dependiendo del método se pude dar de diferentes maneras entre algunas están:

CFB: la propagación de un error se limita a un bloque ya que un bit erróneo en el texto cifrado genera 1+64/m bloques de texto claro incorrectos (siendo m la longitud del flujo en el que se divide el bloque).

OFB: La propagación de un error afecta sólo a un byte, el que se realimenta en el registro de desplazamiento.

CBC: Cada cifrado depende del cifrado del bloque anterior así que un error en un bloque se propaga al siguiente bloque.

Nota sobre padding:
Cuando los bloques a cifrar no tienen una longitud múltiplo del tamaño del bloque, hay que añadir relleno (padding). Hay varias opciones:

Zeros: se rellena con bytes con el valor cero, sin indicar la longitud del relleno.

PKCS7: se rellena con una secuencia de bytes en la que cada byte contiene un valor igual a la longitud de relleno.

ANSIX923: el relleno consiste en una secuencia de ceros y termina con la longitud.

ISO10126: el relleno consiste en una secuencia de bytes con valores aleatorios, terminada con la longitud de relleno.

Ejemplo:

Bloque de datos (longitud 10 bytes): FF FF FF FF FF FF FF FF FF FF

Longitud de bloque de 8 bytes

Opciones de relleno (completar a 16 bytes):

- Zero: FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 00
- X923: FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 06
- PKCS7: FF FF FF FF FF FF FF FF FF FF 06 06 06 06 06 06
- ISO10126: FF FF FF FF FF FF FF FF FF FF 35 3E 45 23 F8 06