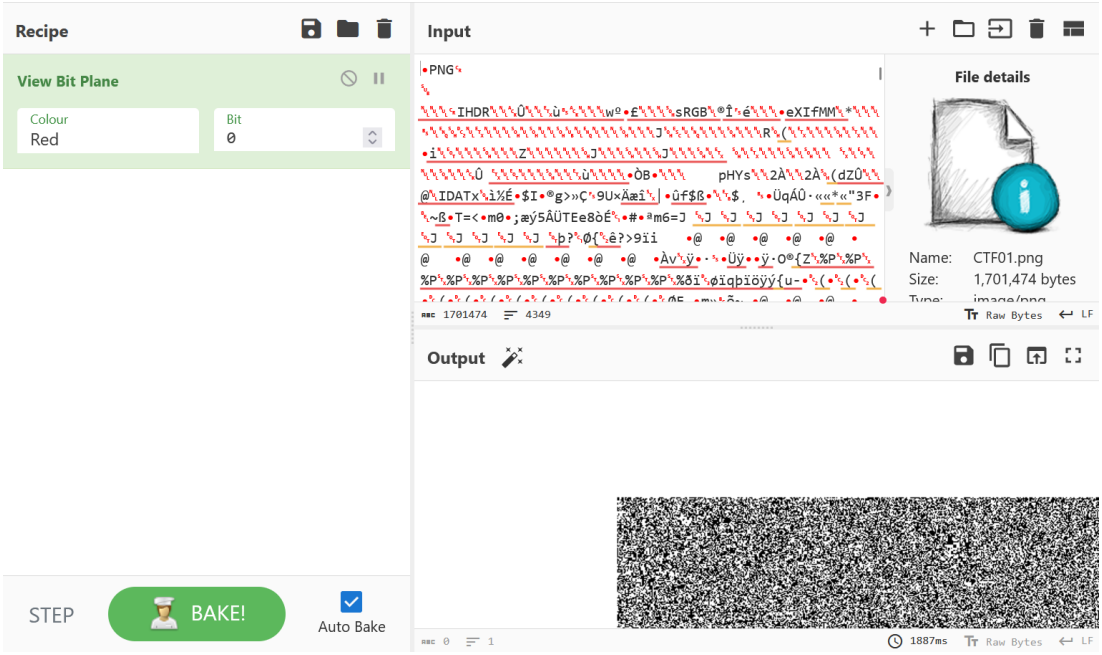
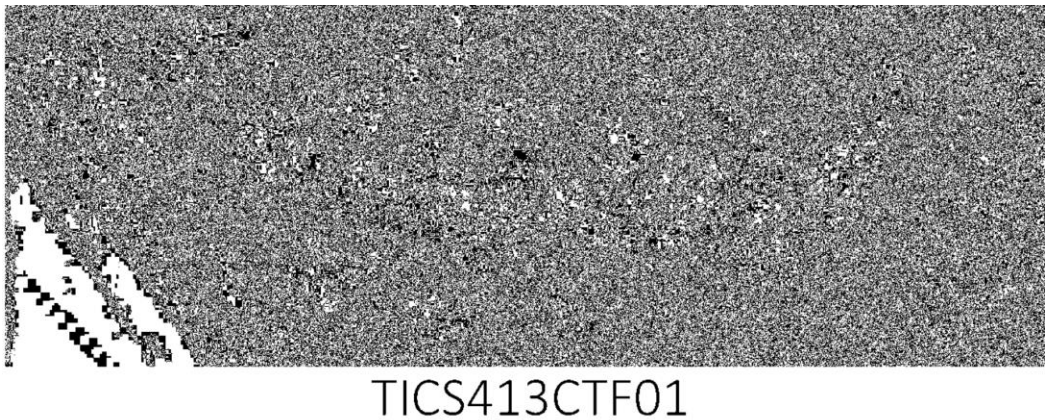
Paso a Paso CTF 01 – Criptografia

Para iniciar se descarga la imagen CTF01.png que se rescató, el archivo CTF01-coordenadas-iniciales.dat con las coordenadas de la entrega de premios y por último el pdf CTF01-keys-locked con las contraseñas, el cual esta protegido por una contraseña.

Ya teniendo todo descargado se procede a acceder a cyberchef desde Google en donde se coloca el archivo de la imagen en la zona que dice input de manera que en cyberchef se muestre el contenido de la imagen, posterior a eso se coloca en el buscador de operaciones image para buscar las operaciones relacionadas con los contenidos de las imágenes, ya con los resultados listos uno los explora hasta encontrar la que se llama View Bit Plane, que extrae y muestra un plano de bits, que solo muestra un solo bit por pixel, de una imagen dada, después se arrastra la función al lugar que dice Recipe y se dejan los parámetros pre-establecidos, esto ocasiona que cyberchef muestre el Bit plane como output, que al ampliarlo y al explorar el resultado se consigue la contraseña del archivo pdf con las llaves que es, TICS413CTF01.



Resultado:



Ya ingresando la contraseña se accede al pdf el cual contiene 2 llaves una llave privada RSA y una llave publica RSA, ya teniendo las llaves se accede nuevamente a cyberchef para tener el programa limpio y en el input colocar el archivo CTF01-coordenadas-iniciales.dat para que muestre el contenido de este, ya con eso en el buscador de operaciones se ingresa RSA y se explora hasta encontrar RSA Decrypt, que permite el cual con la llave privada que se coloca donde dice RSA Private key y los otros valores pre-establecidos nos permite encontrar las coordenadas de la entrega del premio que son -33.489742, -70.513682. Posterior a esto se buscan unas nuevas coordenadas las cuales fueron -2.202712, -80.873138 y se ingresan en el input de cyberchef, después en Recipe se coloca RSA Encrypt con la llave Publica que está en el pdf con una pequeña variación donde dice -----END PUBLIC KEY----- se cambia a -----END RSA PUBLIC KEY----- y con los valores preestablecidos, se logra encriptar las nuevas coordenas que se introdujeron, ya con esto en el apartado de output se selecciona el botón de guardar archivo, al final se le coloca un nombre al archivo y se crea un nuevo archivo .dat.