**Universidad Nacional Autónoma de México**

**Facultad de Ingeniería**

**CRIPTOGRAFÍA**

**Exámen Parcial 2 Parte:** Cifrado AES-128

**Grupo 1**

**Integrantes:**

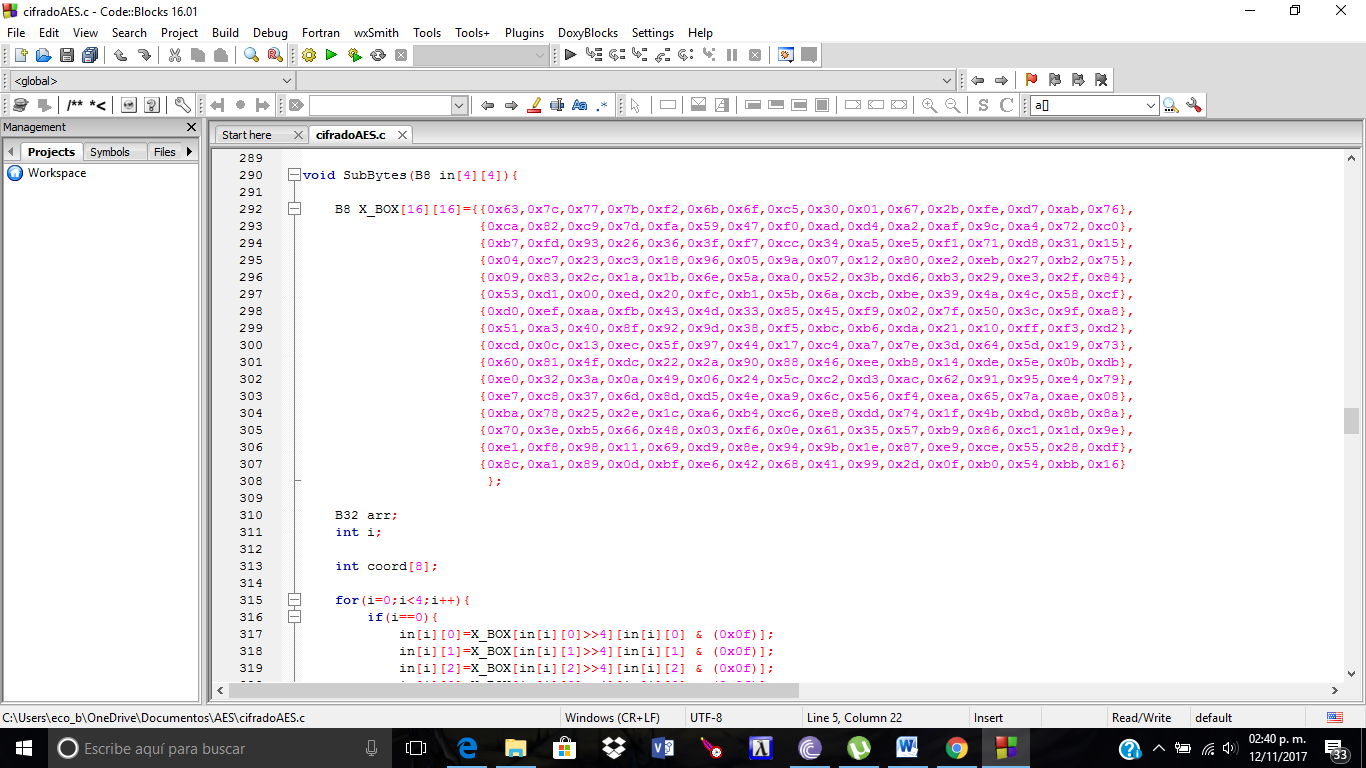
**Banda Martínez César Eduardo**

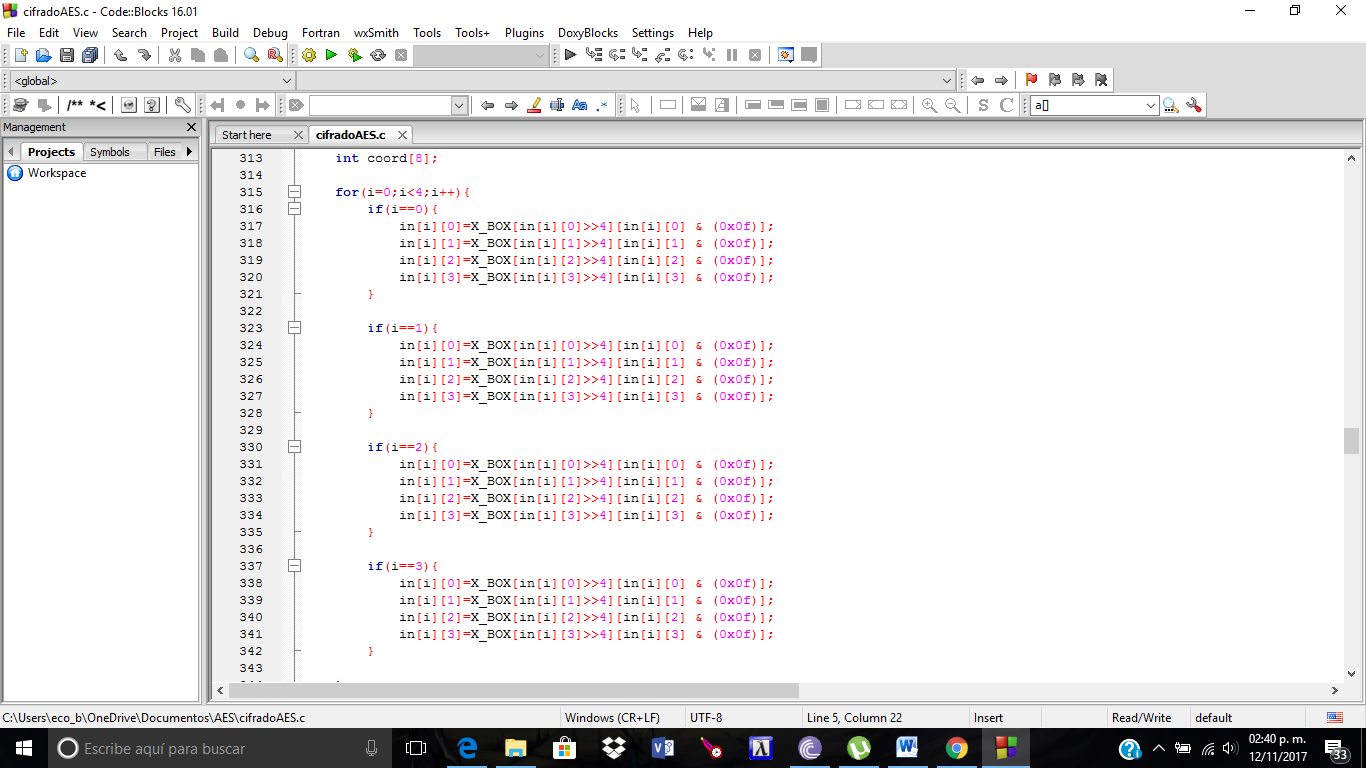
**Limón Hernández Raúl Rogelio**

2018-1

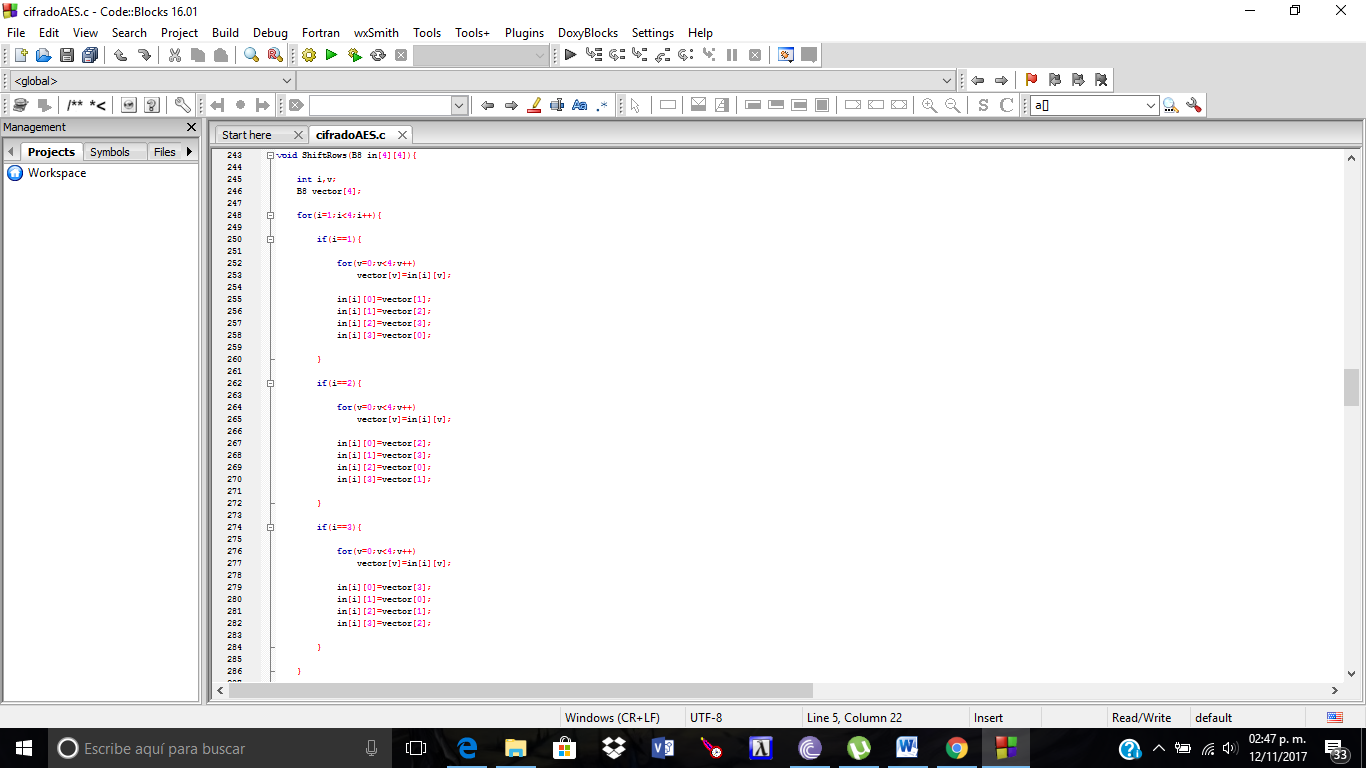
**Funciones requeridas:**

SubBytes: Se utiliza nuevamente la caja S empleada en la expansión de llaves, pero esta vez se desempeñarán corrimientos a la derecha de 4 bits para obtener la primera coordenada y para la otra se filtrará mediante una máscara y una operación AND. Esta operación para todas las celdas de la matriz de estado.

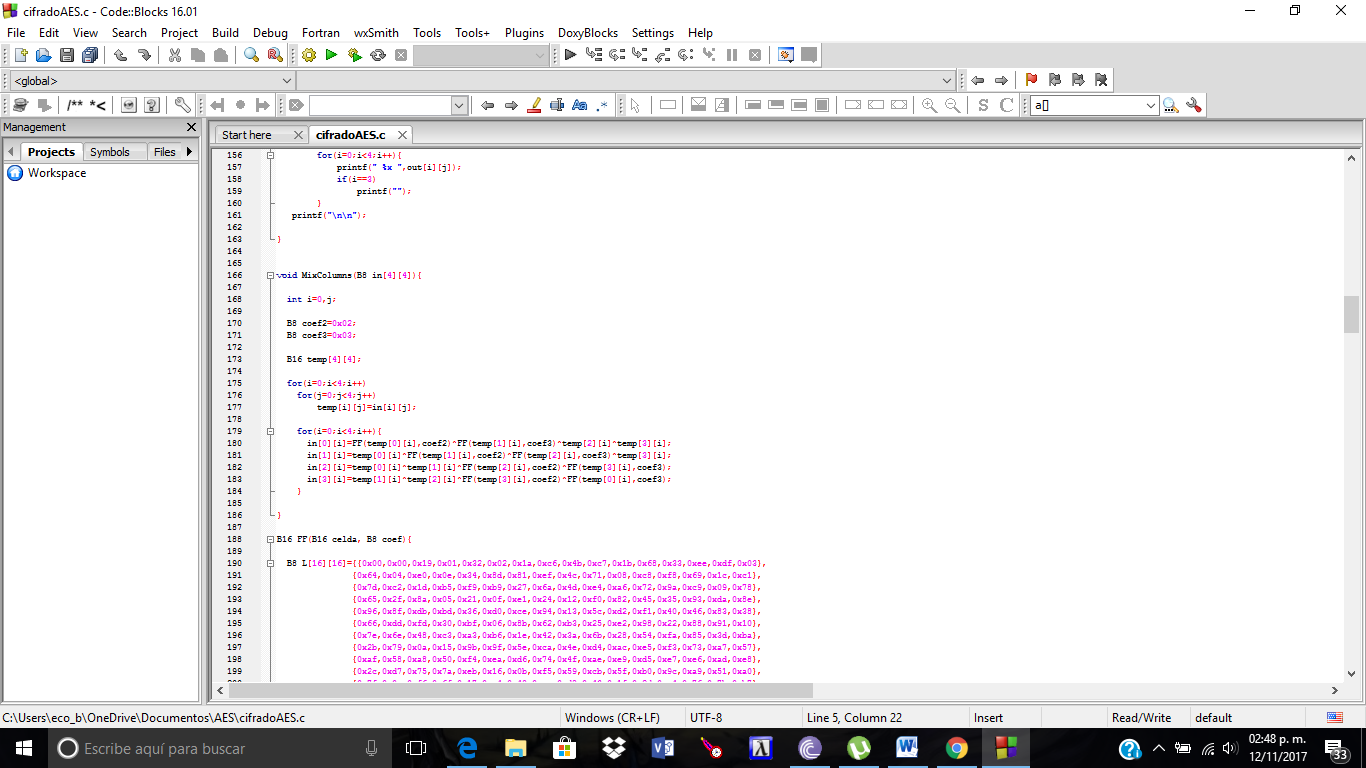




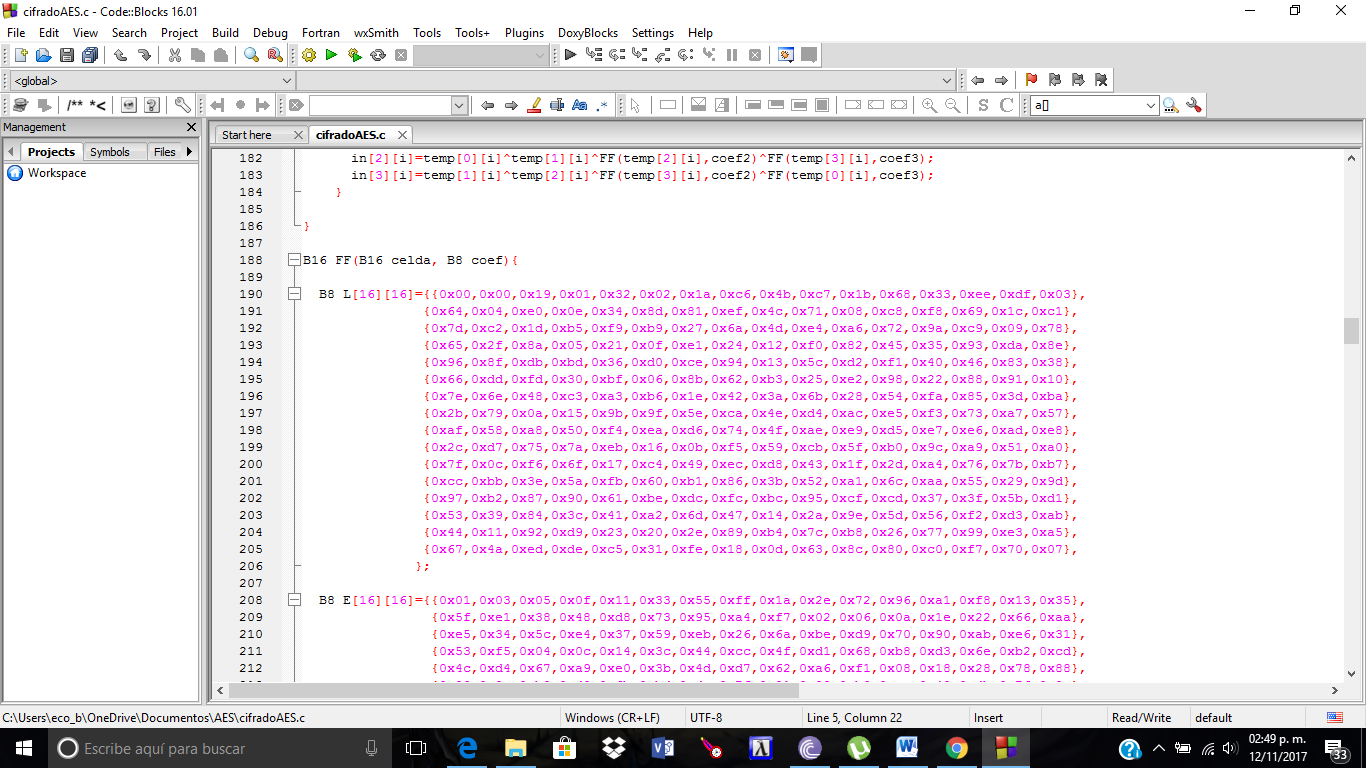
ShiftRows: Se acude a un vector de 4 elementos que almacene de forma temporal los elementos por renglón, para luego hacer las respectivas igualaciones para poder implementar el corrimiento de los renglones.

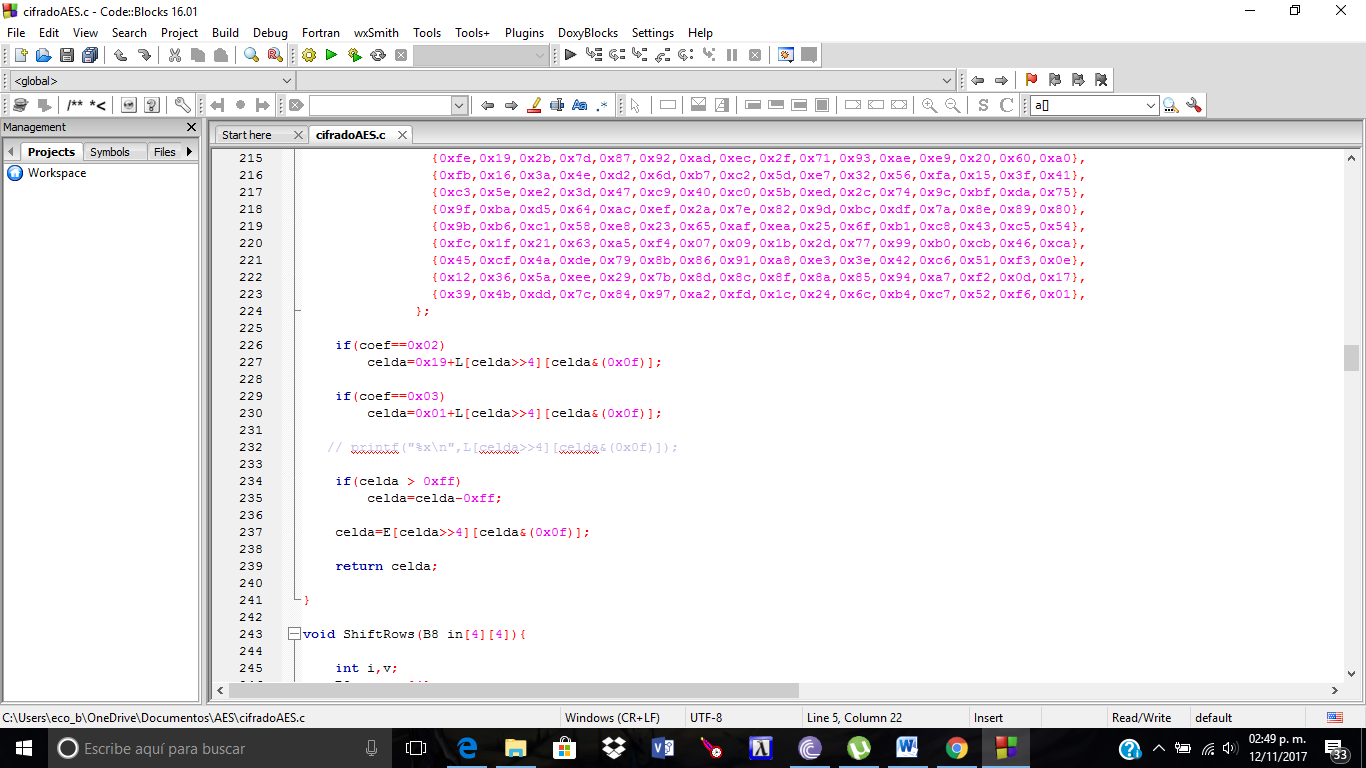


MixColumns: Se copia la matriz de estado en una matriz bidimensional temporal. Se efectúa el producto matricial, columna por columna, basándose para ello en la función FF.

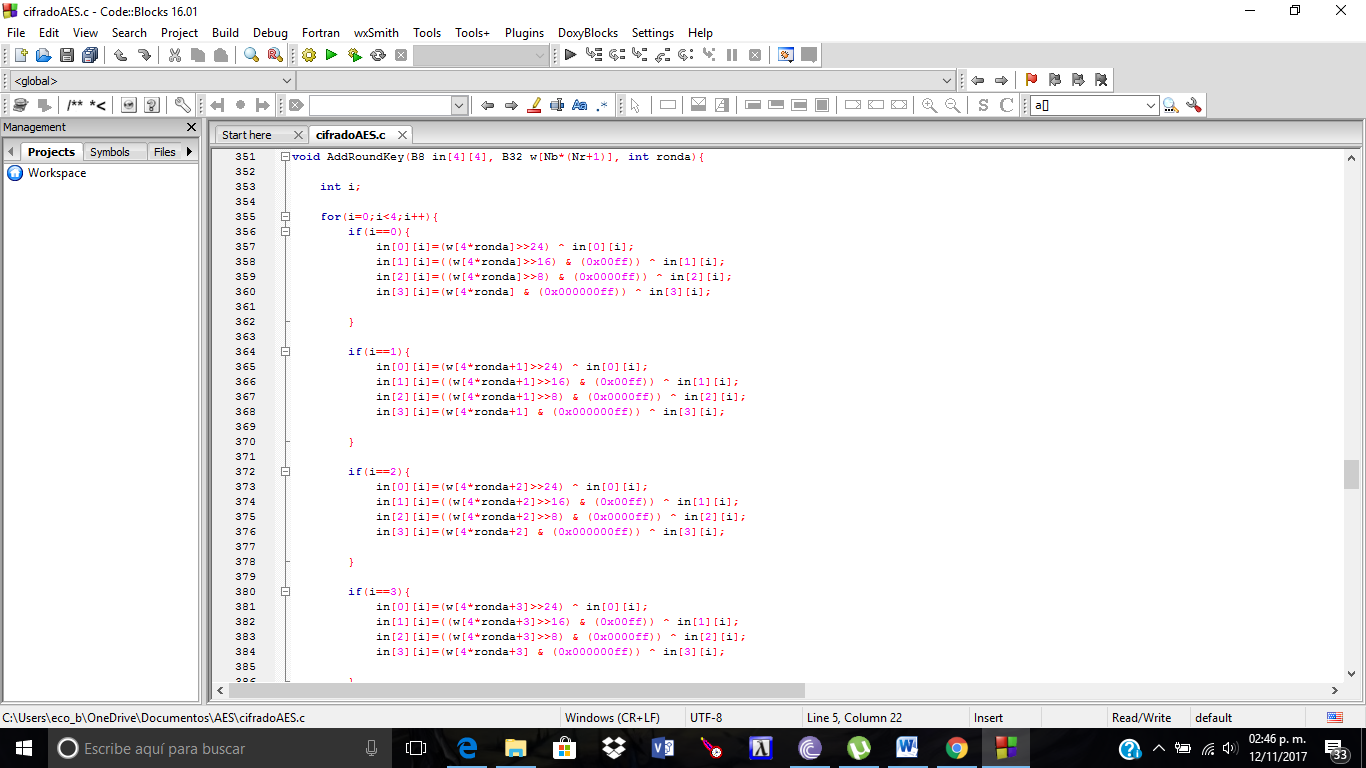


FF: Siglas de “Finite Field”, es la función encargada de desempeñar el producto matricial apoyándose en las tablas “L” y “E”, que además conservará el resultado del producto dentro del campo finito en módulo 0xff.

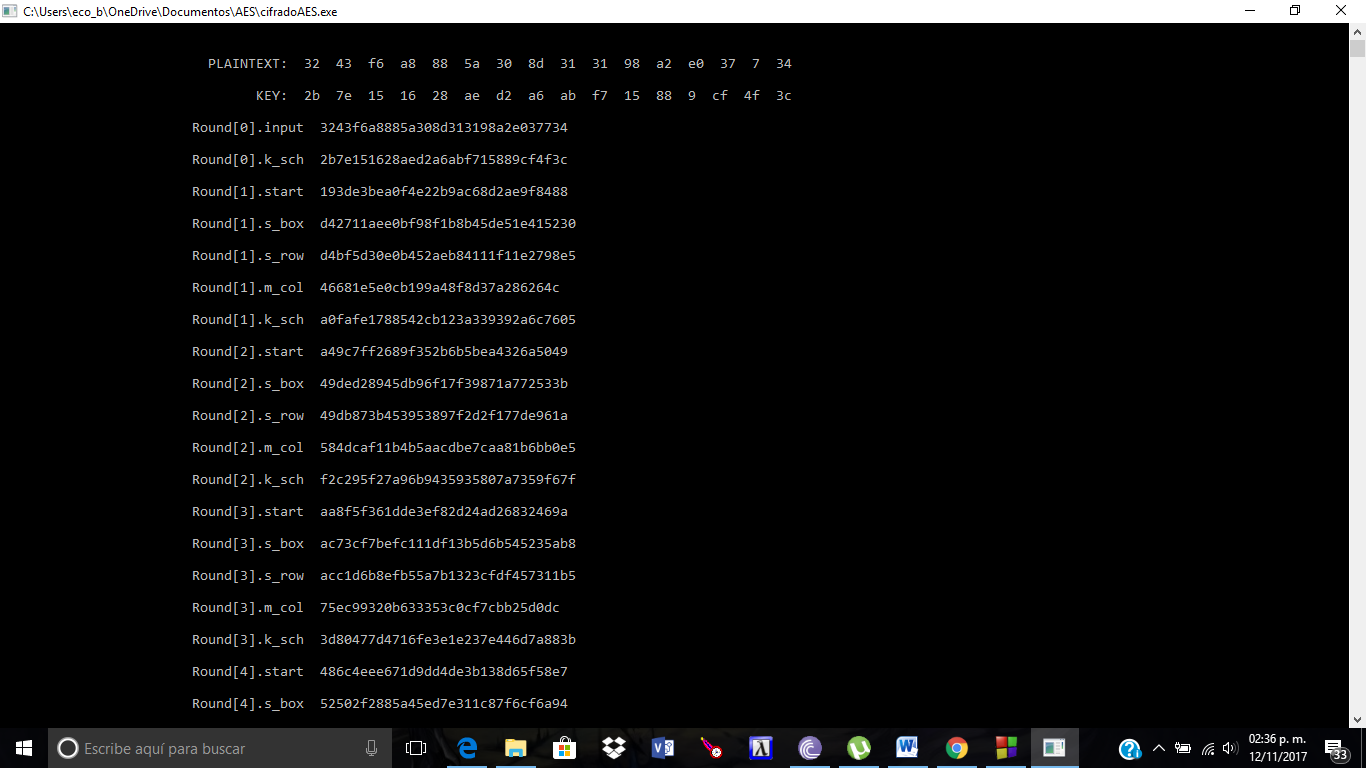


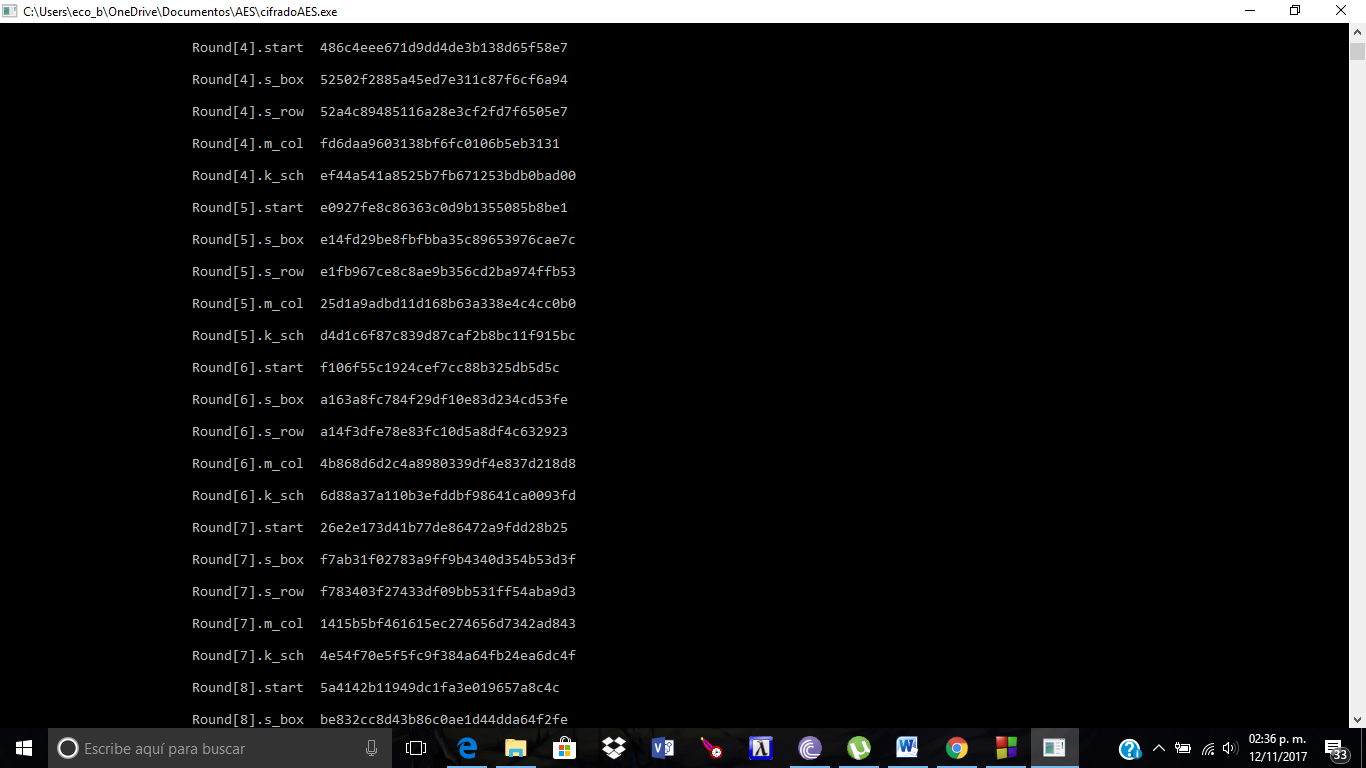


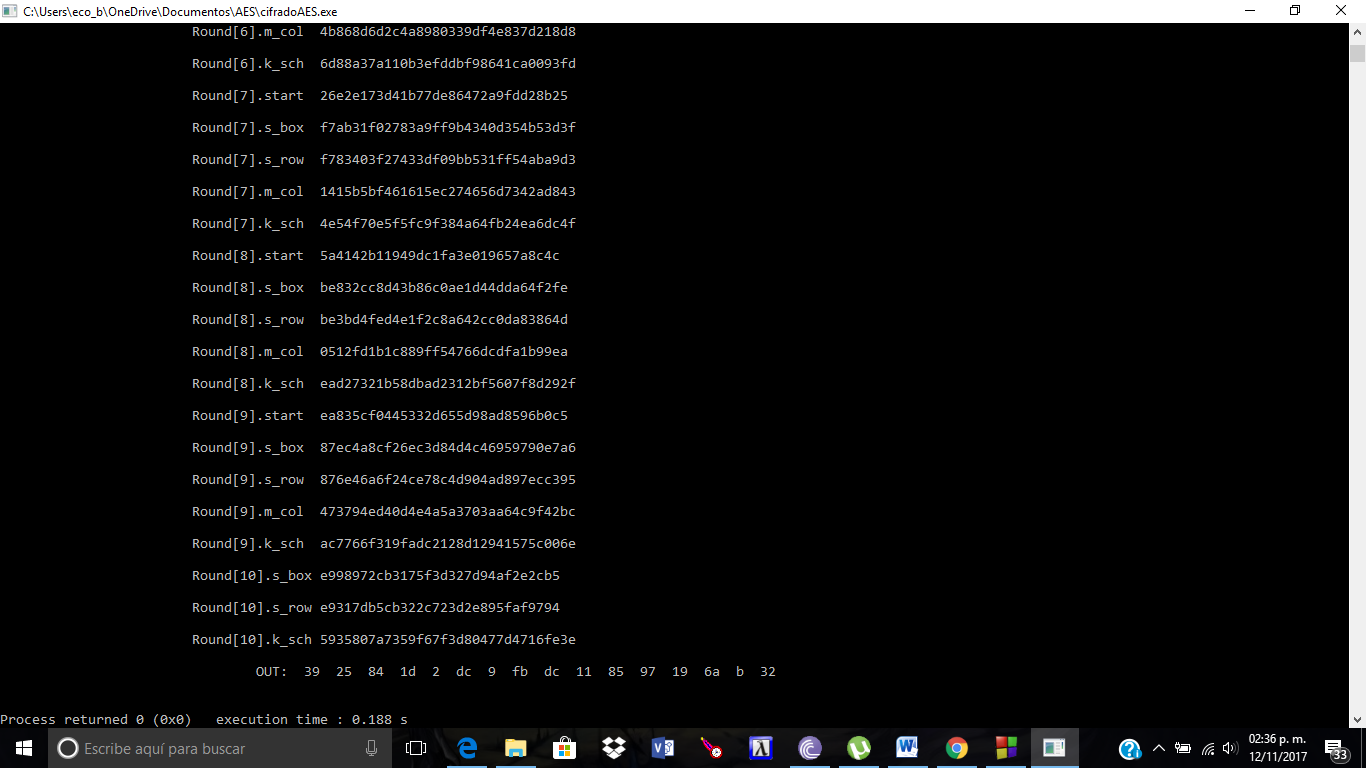
AddRoundKey: Se realizan los corrimientos pertinentes y las máscaras correspondientes para poder operar los valores adecuados, siendo la llave un vector de registros y la matriz de estado una matriz bidimensional, operando con una operación lógica de tipo XOR.



**Salida del programa:**







**Conclusiones:**

Para esta práctica de cifrado en AES, logramos observar de una mejor manera como es que el cifrado AES realiza el proceso para poder cifrar la información del texto plano junto con la llave, ya que en cada uno de los pasos pudimos observar como es que se llevaban a cabo los puntos más importantes como el s\_box, s\_row y el mix columns, llegando a ello al resultado que se nos proporcionó en clase.

**Banda Martínez César Eduardo**

El algoritmo prevé una implementación de 10 rondas de cifrado debido a la naturaleza en la longitud de la llave, la cual es de 128 bits. El empleo de una rutina que permita el agilizar los productos polinomiales en la función MixColumns, repercute en un mayor control de la misma. Al ser AES un algoritmo de cifrado que opera sobre 2 campos finitos, resultó factible el dividir la problemática en el tratamiento de las operaciones sobre los ampos finitos siendo en MixColumns el campo GF(16) y en la función “FF” el campo GF(256).

**Limón Hernández Raúl Rogelio**