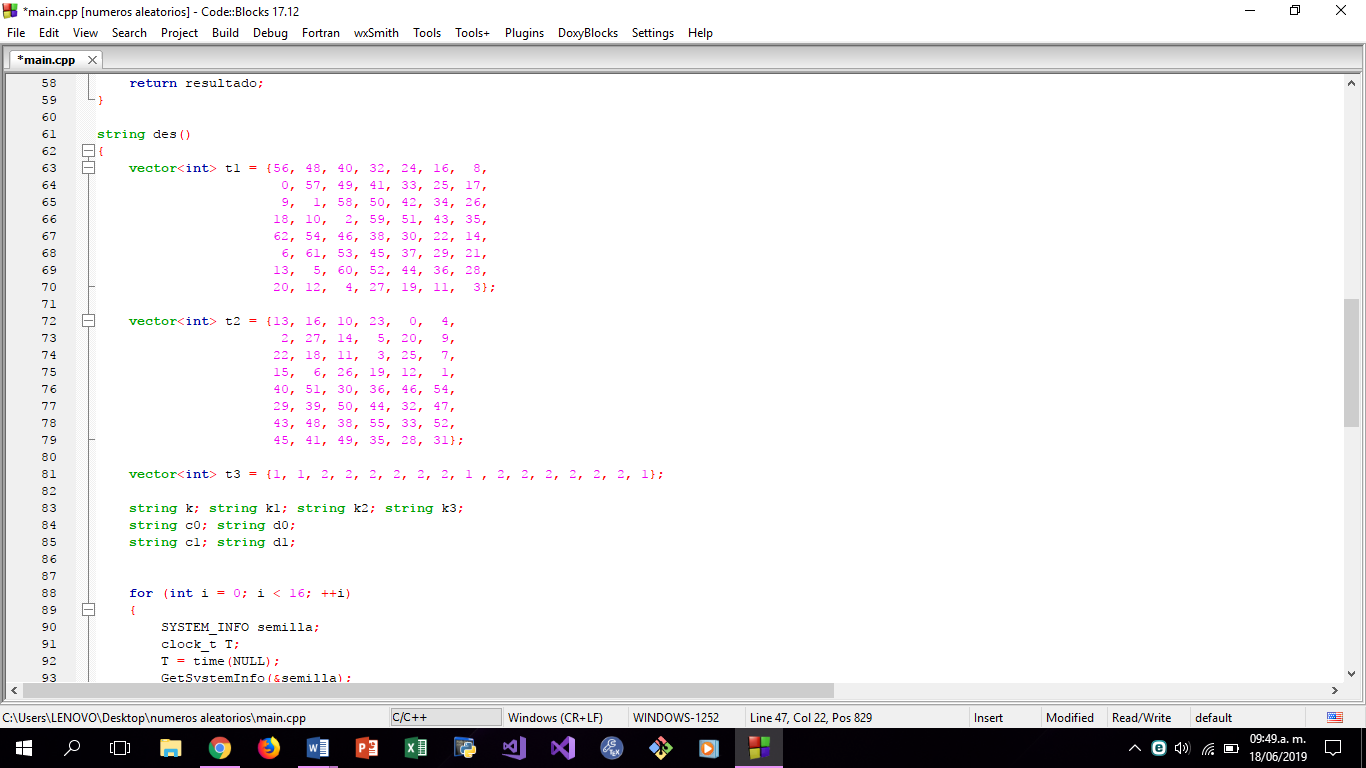
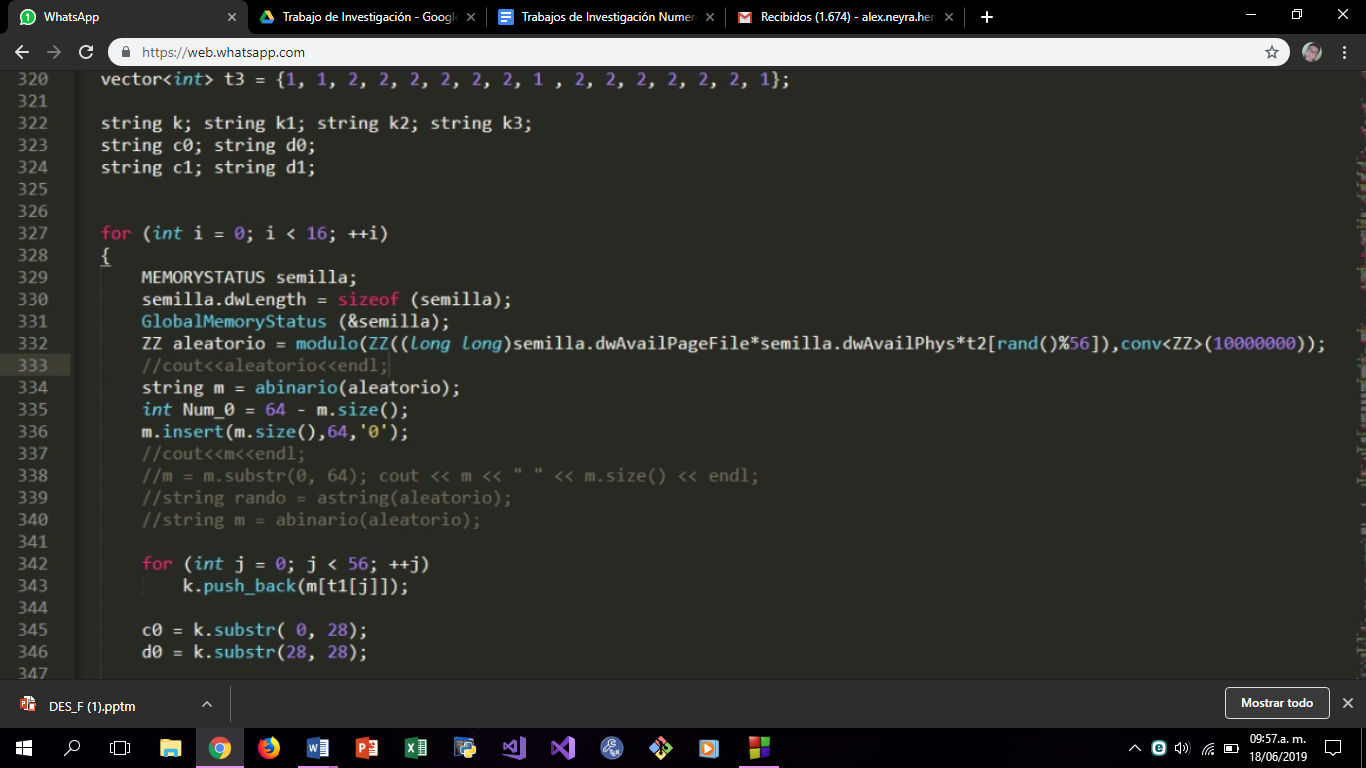
El algoritmo de generación de números aleatorios del cifrado DES requiere de dos tablas de permutación y nosotros creamos una tercera tabla para facilitar el número de corrimientos.

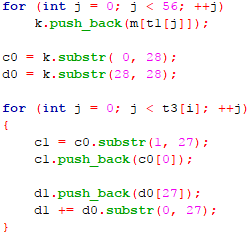


Generamos 16 semillas que serán números binarios de 64 bits de la siguiente manera

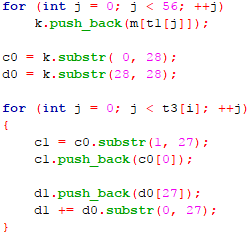


Sacamos datos del hardware específicamente del registro de memoria en tiempo real. Esta manera de generar la semilla se potencia cuando la computadora esta en constate uso.

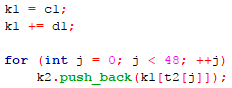
Una vez tenemos la semilla procederemos a realizar la primera permutación con la tabla 1 después de realizar este proceso obtendremos un numero de 56 bits



el cual dividiremos en dos mitades de 28 bits cada una a las cuales procederemos a realizarles corrimientos de bits a la derecha como a la izquierda según sea la mitad derecha o izquierda.



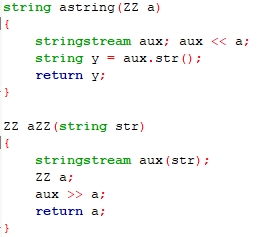
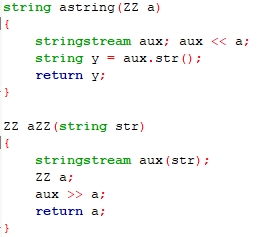
Luego de realizar los corrimientos correspondientes procedemos juntar las mitades para posteriormente realizar la segunda permutación con la tabla 2



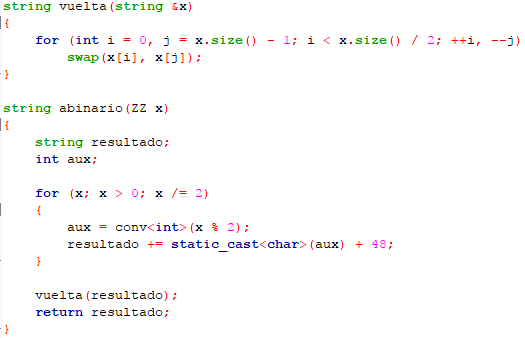
Y así ya obtenemos la primera clave, esto lo repetiremos 16 veces por lo que obtendremos una clave de 768 bits y para obtener claves de mayor cantidad de bits lo que hacemos es repetir este proceso más veces hasta llegar a la cantidad de bits deseada.

Funciones auxiliares:

* Casteo de String a ZZ y ZZ a String : para estas funciones incluimos la librería sstream la cual nos permite trabajar con strings de tamaño muy grande ya que funciona con lectura y escritura de registros entonces lo que hacemos es definir variables tipo stringstream y aquí guardamos el contenido de la variable a castear ya sea ZZ o string en el caso de ZZ a string esta librería tiene una función str() la cual realiza el casteo y para el caso string a ZZ simplemente se asigana ya que NTL tiene el constructor sobrecargado para recibir un string entonces solo lo asignamos.



* Transformación a binario: Para realizar esta acción usamos el método de divisiones sucesivas que consiste en dividir al número entre dos sucesivamente y concatenar los residuos de abajo hacia arriba de tal manera que se lea el numero ya transformado en binario



Seguimiento:

* semilla: 10001010 10001001 10100010 10101011 10001011 10001011 10001011 10001011
* primera permutación: 11111111000000000000110000001111110100000000111110110000
* mitad derecha: 1111111100000000000011000000
* mitad izquierda: 1111110100000000111110110000
* corrimiento a la izquierda: 1111111000000000000110000001
* corrimiento a la derecha: 0111111010000000011111011000
* juntar mitades: 11111110000000000001100000010111111010000000011111011000
* segunda permutación y clave 1: 000011110110000100010101011110100011010011101001