

**VERIFICACION PRE-SILICIO**

**Programación C/C++**

**Tarea 4**

MD5

**Presenta:**

ULLOA FLORES JORDAN OTONIEL

FRANCISCO ALEXIS LOPEZ AVILA

**Responsable:**

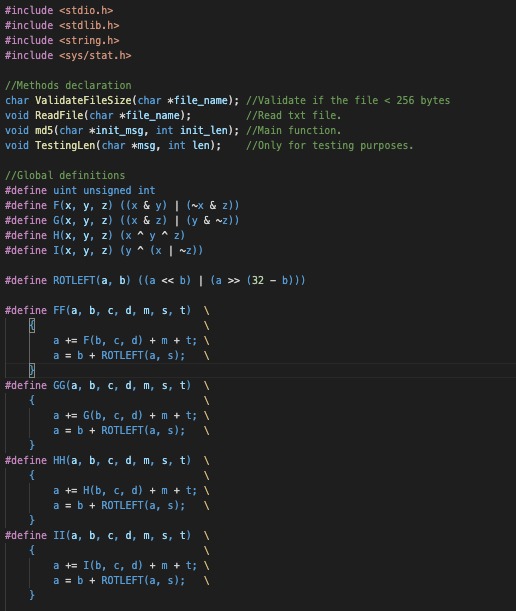
ERNA ENCISO EDGARDO

Octubre 2021

Como parte de la tarea 4, se realizo la implementacion del algoritmo de resumen del mensaje 5 es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

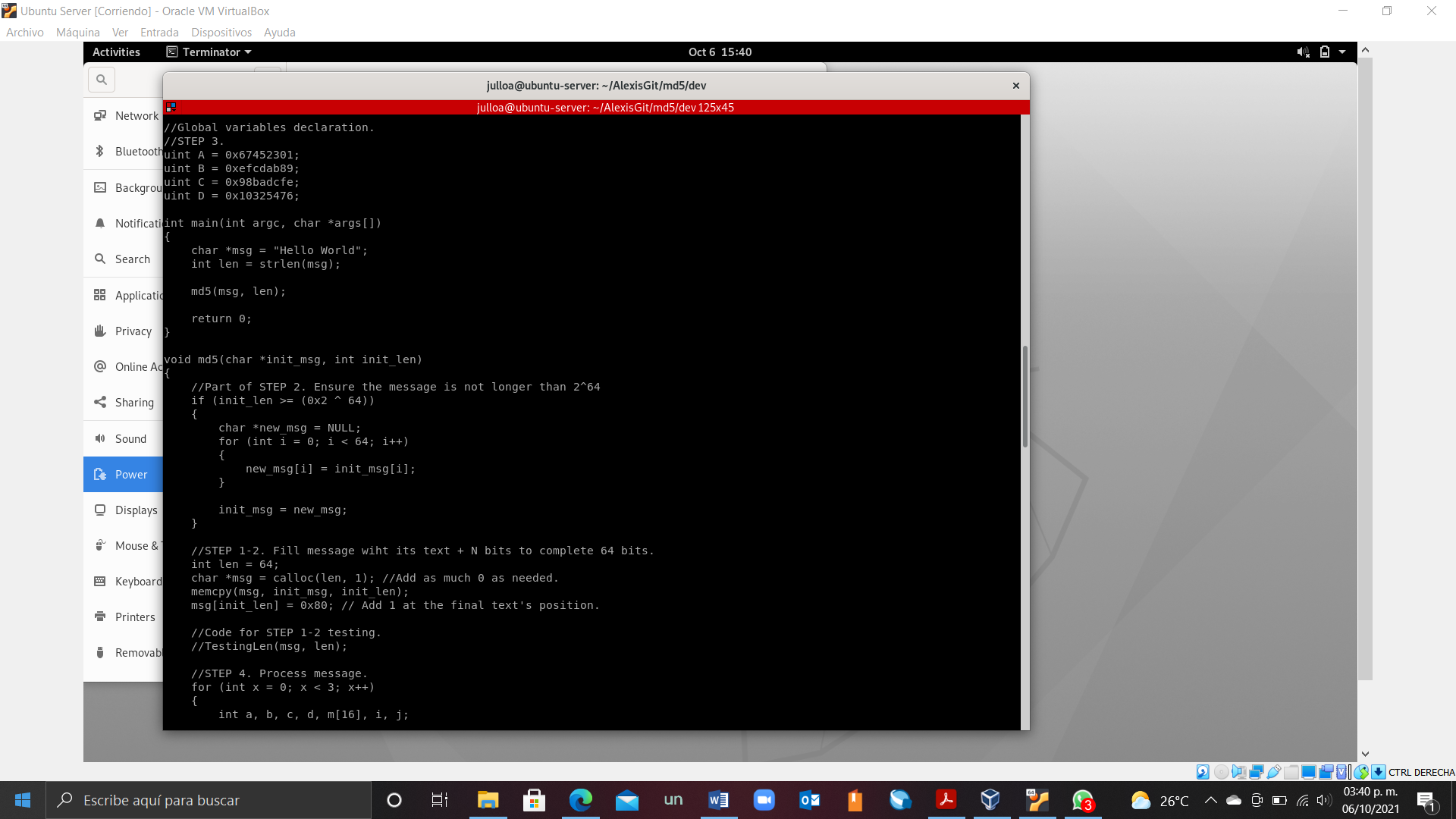
Uno de sus usos es el de comprobar que algún archivo no haya sido modificado

Estructura del codigo.



Al iniciar el codigo se definen la funciones que se utilizaran, las funciones F,G,H,I, las cuales represental el proceso que se llevara en los giros del algoritmo, se define la funcion para la rotacion del bit, y se define el procesimiento en la funcion FF, GG, HH, II.

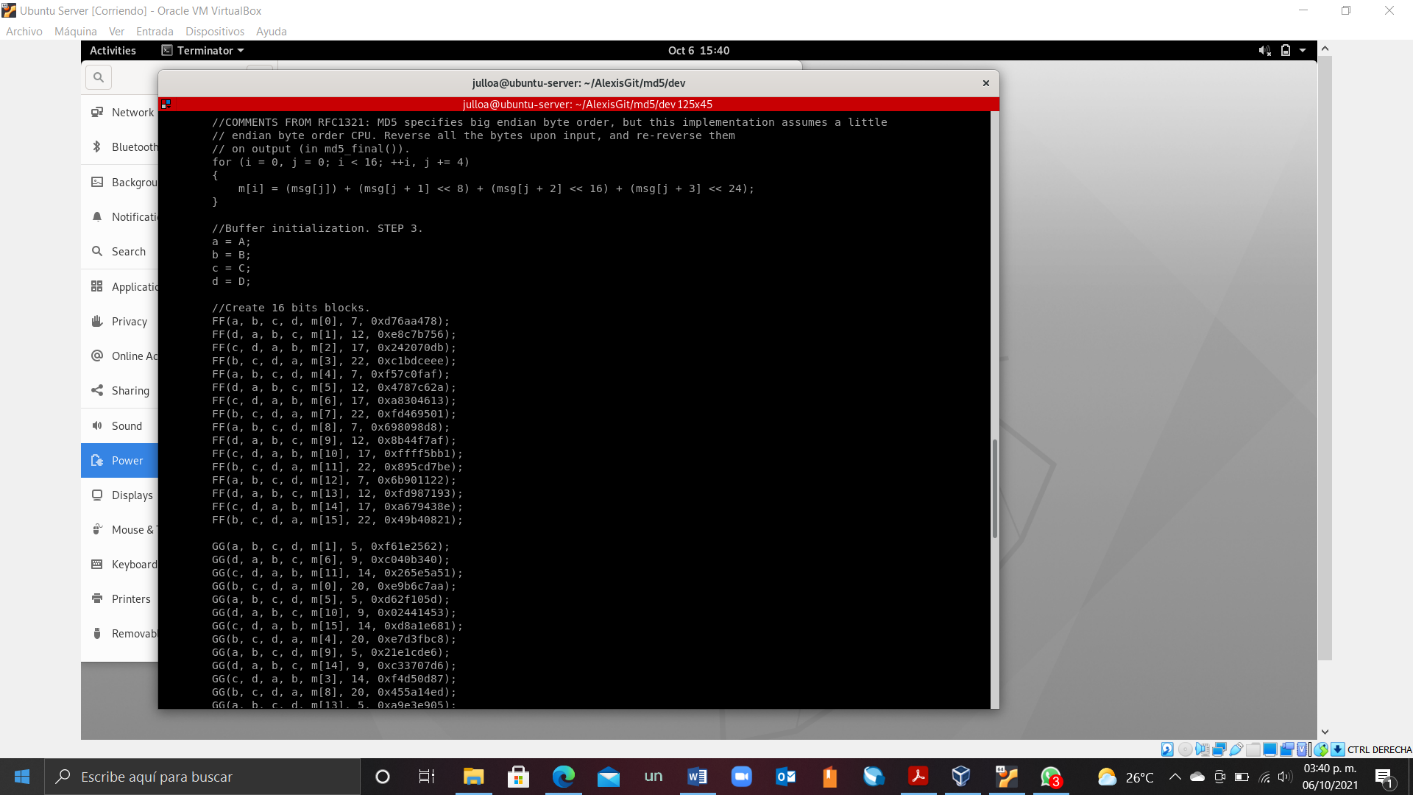
Las rotaciones que se le realizan al mensaje tienen operaciones espesificas con valores que cambian y otros que ya estan definidos en el algoritmo, Mj representa la palabra que se esta tomando en el momento para agregarse a la palabra inicial, tj y ts, tambie ya estan meramente definidad en el algoritmo.



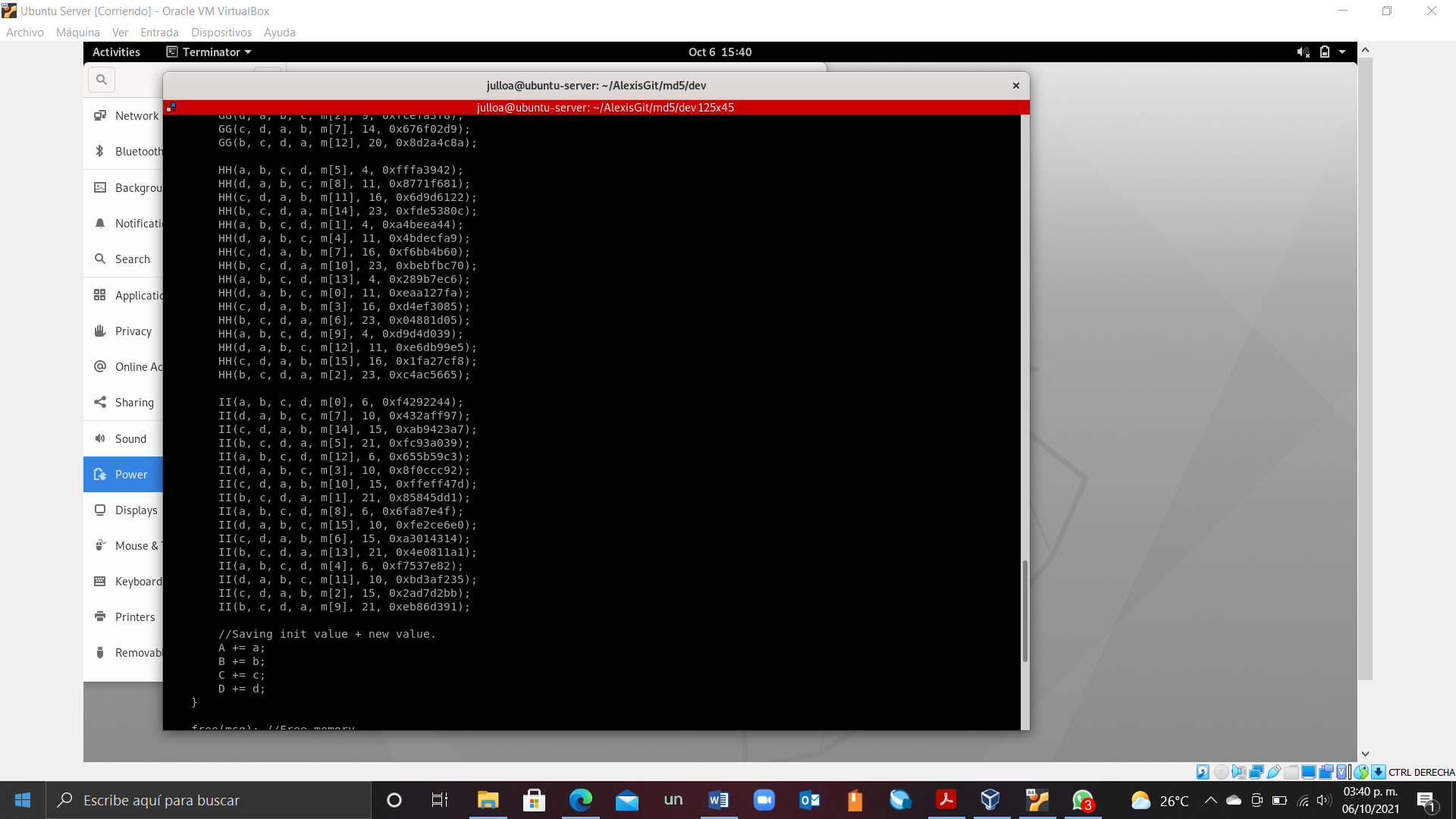
Se comienza a ejecutar la funcion main, la cual primero nos define la varible del mensaje, y otra variable para calcular la longitus dl mensaje, cuando la funcion llega a la otra funcion en ella llamada md5 se comienzan a llevar a cabo la funcion md5.

Se define el ingreso del texto en la funcion de main, recibe dos argumentos se toma el mensaje y el tamaño del mansaje para ingresar esos datos en la funcion de main, primero se evalua que el mensaje cumpla en noser mayor a dos ala sesenta y cuatro.

Despues de esto se realiza parte del paso 1 y 2, lo que consiste en llenar los bits de la palabra, con toso y el relleno, asta que este tenga solo dos palabras libres al final, las cuales se llenaran por el valor del tamaño del archivo.

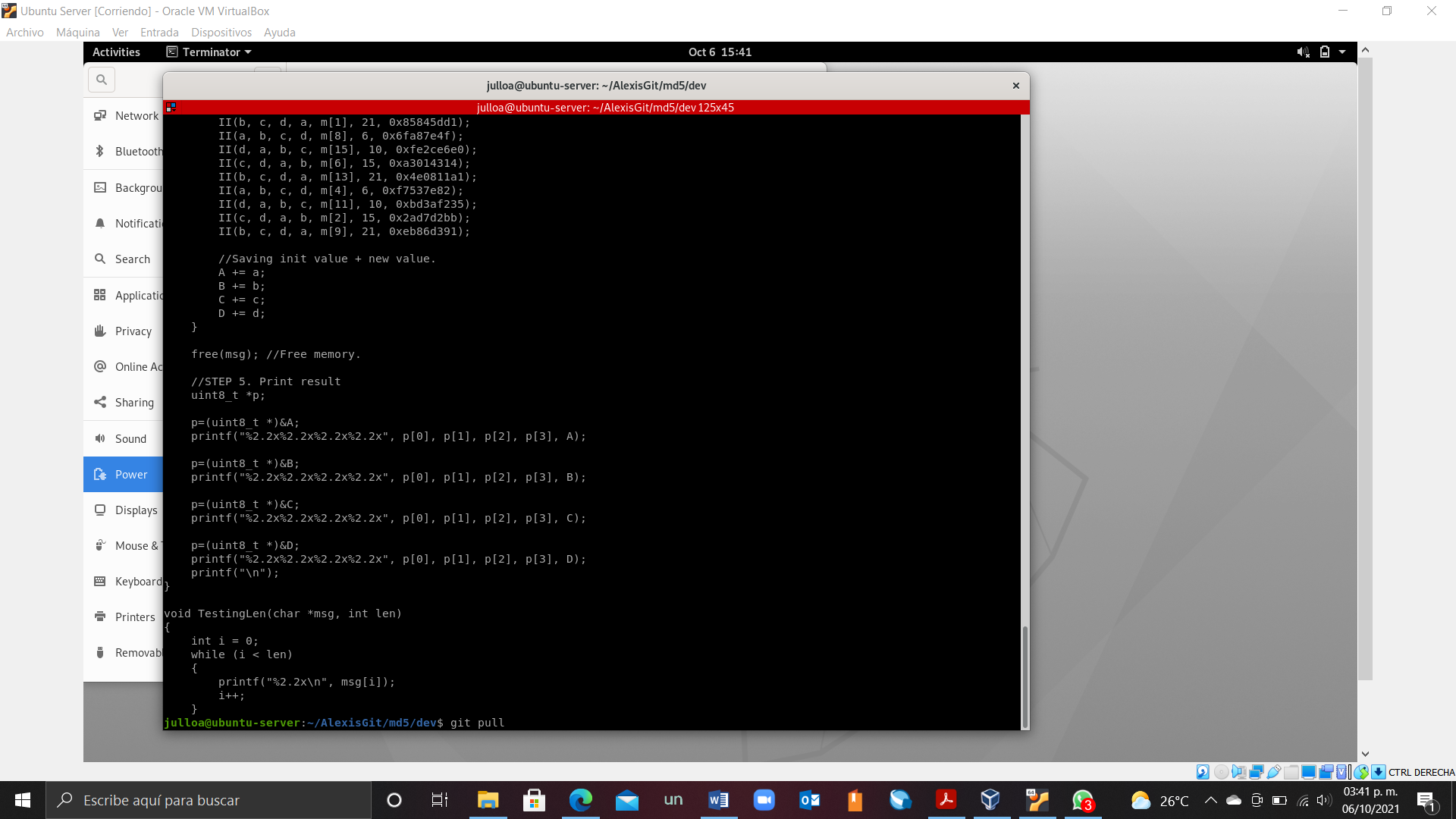


En la imagen anterior se especifica que este tipo de implementacion utiliza little endian, el cual realiza un ajuste en los byetes y los reacomoda del menos significativo a la ezquiera y asi sucesivamente con el resto asta llegar el mas significativo, se declaran los valores para a, b, c, d, los cuales contendran los valores que se estaran mesclando los el mensaje, esto para poder realizar la compresion del mensaje.



Se generan los 4 bloques con los cuales se mesclara el mensaje, a, b, c, y d, son los valos que se estran mesclando en todos los giros, mientras que los siguientes valos ya estan pre determinados a estar ahí, y tambien seran parte los giros en el archivo.

Se guardan los valores y se modifican a partir de que cada giro se realiza.



Por ultimo se tiene la salida despes de los 4 bloques, se tienen una salida de 4 palabras, 32 bits cada una, esto nos da un total de 128 bits, los cuales se re organizan utilizando de nuevo la logica de little endian esto aplicado a cada palabra por separado, reacomodando el mensaje y poniendo las 4 palabras juntas.