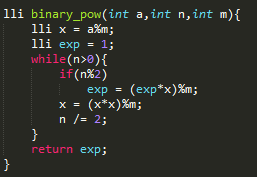
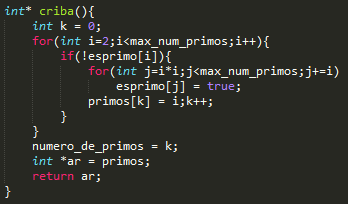
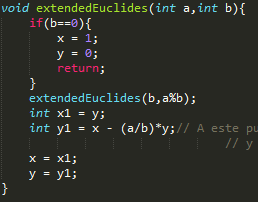
**Manual Técnico**

En este manual se explicarán por separado cada una de las funciones correspondientes a las librerías implementadas en el programa. Como lo son RSA.h y S-DES.h que contienen sus respectivos métodos para que trabajen en la función main (que se encuentra en Demo.cpp) en conjunto.

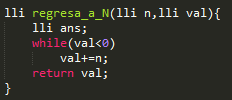
1. **Funciones de RSA.h**

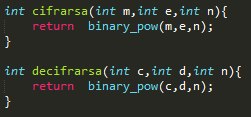
**Exponenciación Binaria:** Usamos la exponenciación binaria ya que es parte importante para que funcione eficientemente el algoritmo RSA. Anteriormente se analizó este algoritmo y su funcionamiento, en RSA es usado cifrar m de la forma m^e (mod n) y para descifrar c^d (mod n).

**Criba de Eratóstenes:** Para elegir los números p y q usamos el algoritmo de la Criba ya que no necesitamos para S-DES usar números primos tan grandes. La criba funciona simple; se empieza por el primer primo 2 y se van “tachando” en un bitset de C++ (estructura de datos eficiente en memoria) todos los múltiplos correspondientes dando saltos de 2 en 2 después se pasa al siguiente número que sería 3 y se hace lo mismo que en 2 y así sucesivamente, habrá que tener en cuenta que los múltiplos antes marcados no serán considerados. Al final devolvemos el arreglo en un apuntador a int.

**Algoritmo Extendido de Euclides:** Este algoritmo como sabemos nos servirá para que calculemos el inverso multiplicativo de e (o sea d) para que podamos descifrar la llave k de S-DES. Su magia parte del hecho de que gcd(a, b) = gcd(b, a - floor(a/b) \* b) ya que ax + by = gcd(a,b), así pues con esas ecuaciones se define nuestra función recursiva así:

Y su complejidad es O(log2 N) ya que al calcular el máximo común divisor de dos números implícitamente le estamos quitando factores primos a los números (a cualquiera de los dos) y en el peor de los casos serán primos tan pequeños como el 2.

**Función regresa\_a\_N**: Esta función lo único que hace es mantener un valor negativo dentro de su grupo es decir sumar su módulo hasta que dicho número se vuelva positivo.

**Cifrado y descifrado**: Estas funciones lo que hacen solo es mandar llamar a la función de exponenciación binaria para que a nuestra k la cifren y descifren respectivamente.