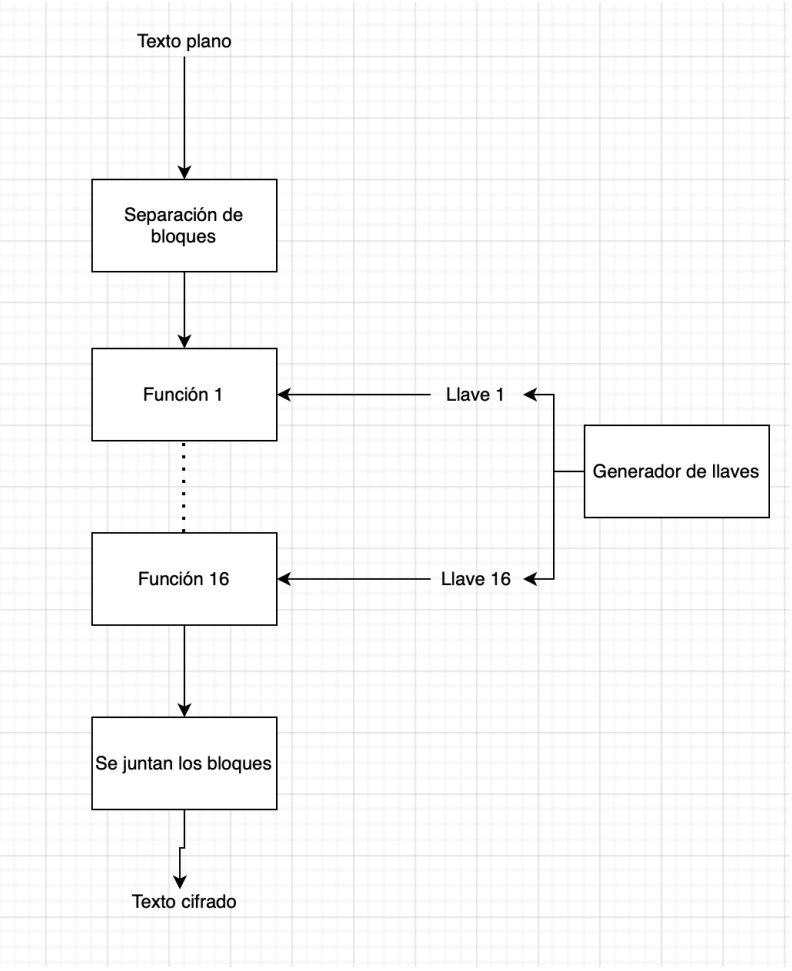
Andy Castillo 18040
Marco Fuentes 18188
Abril Palencia 18198

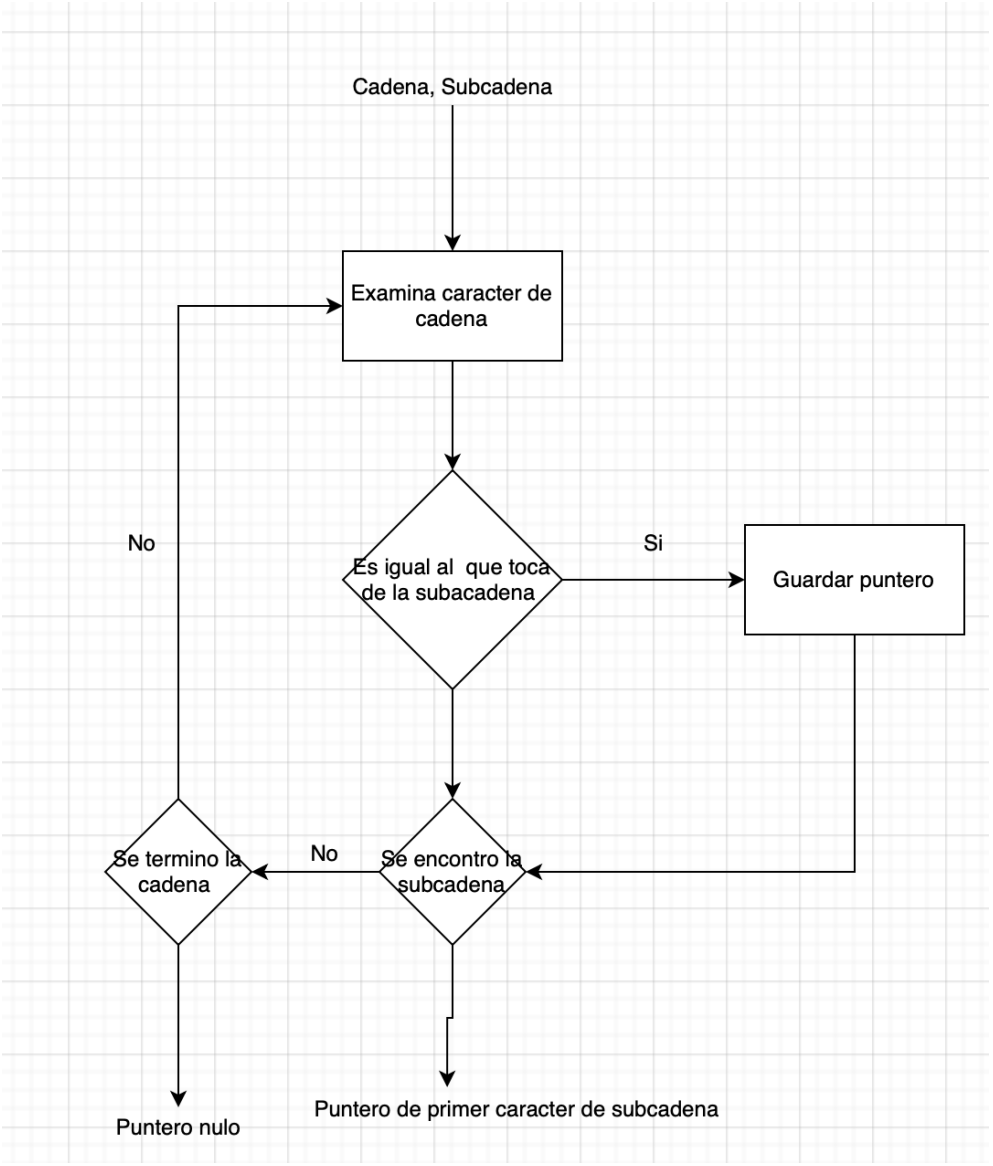
Proyecto 2

Definiciones y diagramas de funciones usadas

- DES
  El algoritmo DES (Data Encryption Algorithm) es un algoritmo simétrico de cifrado por bloques. Este algoritmo recibe como entrada una texto plano de 64 bits y lo que hace es dividir el mensaje en bloques y se opera un bloque a la vez. Lo que se hace cada vez que se va a operar un bloque es someterlos a 16 rondas de funciones de transposición y sustitución, las cuales son diferentes formas de cifrar. Tanto el orden como el tipo de las funciones de transposición y sustitución que son utilizadas, dependen del valor de la llave que sea utilizado para el algoritmo las cuales se generan cada vez que se aplica una función. Luego de hacer todas estas funciones, se vuelven a unir cada uno de estos bloques que fueron separados al inicio y el resultado y lo que nos devuelve este algoritmo DES es un texto cifrado con un tamaño de 64 bits.

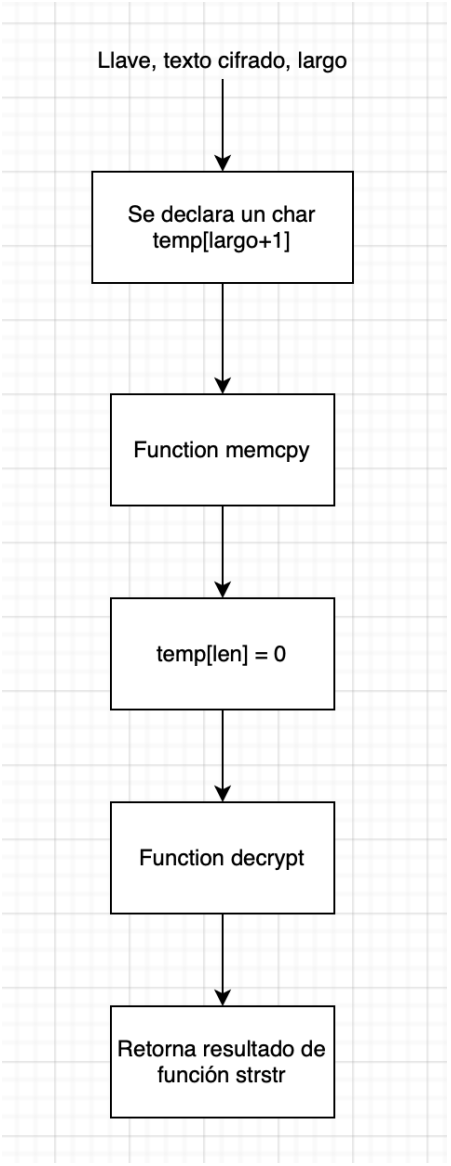


- strstr
  La función strstr() es una función la cual tiene como propósito encontrar un subcadena dentro de una cadena. Los parámetros que recibe son la cadena en la cual se va a buscar la subcadena y la subcadena a buscar. La función retorna en caso de que si este la subcadena un puntero apuntando al primer caracter de la subcadena encontrada dentro de la cadena y si no se encuentra un puntero nulo.



- tryKey
  La función tryKey tiene como propósito comprobar si la llave o palabra clave con la que se sabrá si se descifró bien, que se le pasa como parámetro es la correcta para el texto cifrado que se le pasa y que se quiere descifrar. Esta función utiliza varias

funciones, como la de memcpy, decrypt y strstr, las cuales se explican en el documento.



- memcpy:
  La función memcpy copia n caracteres del área de memoria src al área de memoria dest, donde dest es un puntero a la matriz de destino donde se va a copiar el contenido, y se convierte en un puntero de tipo void *, src es un puntero al origen de los datos que se copiarán, convertido en un puntero de tipo void * y n es la cantidad o número de bytes que se copiaran.
- decrypt:
  El método decrypt() descifra algunos datos cifrados. Toma como argumentos una clave para descifrar, algunos parámetros adicionales opcionales y los datos para descifrar. Devuelve una promesa que se cumplirá con los datos descifrados.

Mediciones de tiempo

Dada la complejidad del algoritmo, la medición del tiempo secuencial no fue posible. Sin embargo pudimos encontrar que el algoritmo tarda al menos 25 minutos para completarse.