Práctica de Lex, Modelos de Computación. Alumno: Víctor Bricio Blázquez.

El problema que he ideado se trata de usar Lex para encriptar y desenciptar un mensaje dado con una regla.
La regla es la siguiente:

-Siempre que Lex halle una letra minúscula, en el mensaje cifrado se escribirá otra letra minúscula (estrictamente distinta) seguida de un número de exactamente dos cifras. El significado es que al sumar la posición del alfabeto de la nueva letra minúscula a este número de dos cifras se obtiene la posición de la primera letra minúscula (en módulo 26, que es la longitud del abecedario sin contar la “ñ”).

- Siempre que Lex halle una letra mayúscula seguirá el mismo procedimiento que si fuera una letra minúscula, con el cambio de que se tratará siempre con letras mayúsculas en lugar de con minúsculas. Cabe destacar que las letras mayúsculas y las minúsculas se deben diferenciar, ya que tienen distinto valor en la tabla ASCII.

-Siempre que Lex halle un número de varias cifras, en el mensaje cifrado se escribirá:

- Inicialmente el carácter ¬.
- Después, por cada cifra un número aleatorio (no necesariamente distinto) seguido de otro número. El significado es que el número antiguo es la suma de los dos nuevos (en módulo 10).
- Finalmente el carácter ¬, otra vez.

Pongo el carácter ¬ tanto al iniciar los números como al finalizarlos con el objeto de poder diferenciarlos bien a la hora de desencriptar el mensaje.

- Siempre que Lex halle uno de los siguientes elementos : '?', '¿', ',', '_', '-', '(', ')', '.', '!', '¡', ' ', '"', '\', '/', '*', '+', '¬' y ':', en el mensaje cifrado se escribirán tal cual.

- Finalmente, como podemos ver, tenemos los siguientes tres bloques importantes para deesencriptar el mensaje: una minúscula seguida de un número de dos cifras; una mayúscula seguida de un número de dos cifras y el carácter ¬, seguido de un número par de cifras indeterminadas , seguido de el carácter ¬.
De modo que tanto al iniciar el mensaje, como entre dichos bloques, como al final del mensaje se escribirá un número aleatorio entre 0 y 5240 seguido de un número aleatorio entre 0 y 9 de letras aleatorias, estas letras serán mayúscula o minúscula de forma aleatoria.

Para usarlo se debe crear primero un archivo a_encriptar.txt con el mensaje que queremos encriptar. Luego debemos usar los siguientes comandos:

```
flex encriptador.l
gcc lex.yy.c -o encriptador -lfl
./encriptador a_encriptar.txt > encriptado.txt
```

De este modo crearemos el archivo encriptado.txt con el mensaje encriptado. Se puede probar que al encriptar un mismo mensaje dos veces, la probabilidad de que el mensaje encriptado sea el mismo en las dos ocasiones es casi nula. Una vez tenemos este archivo debemos usar los siguientes comandos para desencriptar el mensaje:

```
flex desenciptador.l
gcc lex.yy.c -o desencriptador -lfl
./desencriptador encriptado.txt > mensaje.txt
```

Así crearemos el archivo mensaje.txt en el que estará el mensaje inicial. Lo único destacable es que en el mensaje para encriptar no se pueden poner ni “ñ” ni tildes, pues en el proceso se eliminarán.