Práctica 3T
Cifrado FairPlay
1° DAM PROGRAMACIÓN

Contexto histórico

El cifrado de Playfair fue el primer sistema de cifrado en encriptar pares de letras. Wheatstone inventó el cifrado para encriptar mensajes enviados por telegrama, pero lleva el nombre de su amigo lord Playfair, quien lo promovió para uso militar.

El método de cifrado

La tabla se llena con una palabra o frase secreta descartando las letras repetidas. Se rellenan los espacios de la tabla con las letras del alfabeto en orden. Usualmente se omite la "W" y se utiliza la "V" en su lugar o se reemplazan las "J" por "I". Esto se hace debido a que la tabla tiene 25 espacios y el alfabeto tiene 26 símbolos. La frase secreta usualmente se ingresa a la tabla de izquierda a derecha y arriba hacia abajo o en forma de espiral, pero puede utilizarse algún otro patrón. La frase secreta junto con las convenciones para llenar la tabla de 5x5 constituyen la clave de encriptación.

Por ejemplo:

Si la frase secreta es "CRIPTOSISTEMA PLAYFAIR"

Llenaremos de izquierda a derecha y arriba hacia abajo y omitiremos las letras J y Ñ.

C	R	I	P	T
O	S	E	M	A
L	Y	F	B	D
G	H	K	N	Q
U	V	W	X	Z

Reglas para cifrar el texto.

Premisas:

1. El texto a cifrar estará sin espacios en blanco.

Reglas para cifrar dos caracteres **m1** y **m2**:

1. Si m1 y m2 se encuentran en la misma fila,
   escoger c1 y c2 situados a su derecha (circularmente).
2. Si m1 y m2 se encuentran en la misma columna,
   escoger c1 y c2 situados debajo (circularmente).
3. Si m1 y m2 se encuentran en distintas filas y columnas,
   escoger c1 y c2 situados en la diagonal opuesta (siempre de derecha a izquierda).
4. Si m1 = m2, insertar carácter sin significado entre m1 y m2 para evitar su repetición, y después aplicar las reglas 1-3.
5. Si el número de letras es impar, añadir una sin significado al final del texto.

Por lo tanto, si tenemos p.ej. este texto en claro: AT AQ UE CE RO HO RA SX (la X la ponemos al final porque al ser el texto de número de letras impar, tenemos que colocar una letra sin significado para rellenar y volver a la paridad). También podrían ponerse letras sin significado al final de cada palabra para evitar confusiones o hacer más claro el texto resultante.

Funcionalidades iniciales:

1. El usuario podrá cifrar o descifrar un mensaje. Se deberá preguntar al inicio que opción desea.

2. Se pedirá una clave al usuario (Introducir por teclado)

3. Se pedirá un mensaje a cifrar o descifrar (Introducir por teclado)

4. Proceso de cifrado o descifrado

   En ambos casos se mostrará por pantalla la clave, el mensaje en claro o cifrado (dependiendo de si estamos cifrando o descifrando), la matriz y el mensaje resultante en claro o cifrado (dependiendo de si estamos cifrando o descifrando)

Funcionalidades evolución

Teniendo en cuenta el proceso anterior se piden las siguientes modificaciones:

1. La clave se encontrará en un archivo asociada a la fecha del día. (Pueden existir más claves en este fichero)

   Nota cada línea del fichero tendrá este formato: "22/05/2022 Messi" la clave sería Messi.

2. A Parte de la presentación por pantalla del resultado, existirá un fichero de salida en el que por cada `proceso de cifrado o descifrado se añadirá información acerca de si estamos cifrando descifrando, la clave, el texto original, el texto final y la fecha.

   Ej: Cifrar- Messi- Ficha por PSG- NFBKMULURMDZ