**Introduccion**

Este proyecto se realizo con el objetivo de aplicar metodos de encriptacion los cuales se deducieron en la materia de criptografia y seguridad, la dificultad de los algoritmos se basan en el diferente lenguaje de programacion en el que se desarrollaron.

La encriptacion y desencriptacion de un texto plano se realizará unicamente a textos del alfabeto español, sin contar los numeros ni caracteres especiales, en algunos metodos no se pudo aplicar encriptacion con la letra ‘ñ’, en el resumen de cada meto especificaremos las precondiciones para poder encriptar un archivo de texto o una cadena cualquiera introducida por el usuario.

Existen ditintas maneras de representar estos metodos de encriptacion, las que hemos aplicado en este proyecto creemos que son las mas adecuadas y precisas para representarlos, tomando en cuenta el tiempo dado para el proyecto y la complejidad del lenguaje de programacion.

La interfaz está hecha mediante consola ya que el lenguaje de programacion en el que se desarrolló este proyecto es PERL. Para poder ejecutar el programa, se debe tener instalado en el entorno del sistema dicho lenguaje.

Acto seguido se debe abrir la consola del sistema (también conocido como simbolo del sistema). Debemos acudir mediante comandos de consola hasta la carpeta en la que se encuentra el archivo PROYECTO.pl, una vez en la carpeta, debemos ejecutar el comando ‘perl proyecto.pl’ y acto seguido el programa se inciará.

Se podrá encriptar y desencriptar archivos de textos guardados en el sistema y cadenas de texto ingresadas por el usuario.

**Metodos de encriptacion**

1. **Deslizamiento puro**

Como lo hice la encriptacion, problema que tube, como lo solucioné, como lo desencripté, precondiciones

1. **Deslizamiento puro con palabra clave**

Para realizar el cifrado y descifrado puro con Palabra clave se procedió a investigar previamente como se realizaba el cifrado con desplazamiento puro, que era mucho más sencillo, puesto que solo se realizaba el desplazamiento respectivo y se reconstruía el abecedario para su consiguiente sustitución de caracteres.

Para realizar el cifrado, se procedió a dividir los trabajos en funciones auxiliares para que no haya errores al momento de cifrar y descifrar. En primer lugar, el parámetro de entrada es una cadena, la palabra clave y el desplazamiento.

Como el mensaje a cifrar entra como una cadena, procedemos a convertirla a un arreglo para poder trabajar al momento de generar el nuevo alfabeto, con la ayuda de nuestra función ***CadToArraySinR***, eliminamos los caracteres repetidos. Luego de generamos el nuevo Alfabeto.

Para poder reconstruirlo, con la palabra clave ya modificada, generamos el nuevo alfabeto concatenando la palabra clave al principio con el abecedario, habiendo eliminado las letras del abecedario original previamente. En la función ***generarAlfConPalD*** *realizamos esto.*

Teniendo ya nuestras herramientas de apoyo, procedemos a cifrar nuestro mensaje. En nuestra función principal: **cifrarCesarP**, para cifrar el mensaje, o **descifrarCesarP**, para descifrar el mensaje.

1. **Transposicion por grupos**

Como lo hice la encriptacion, problema que tube, como lo solucioné, como lo desencripté, precondiciones

1. **Transposicion por series**

Esta encriptacion se realizó en base a una serie de numeros pares, el mayor problema al realizar el ejercicio fue que el metodo carecía de mas aseries para encriptar, asi que se decidió hacer la serie solo con numeros pares e intercalar las posiciones al intercalar. Para desencriptarlo solo se necesitó saber si la longitud era par o impar, y asi sacar carácter a carácter y luego unirlo en dos cadenas.

Este metodo es capaz de encriptar textos con la letra ñ y cualquier carácter, ya que solo las desplaza sobre sus indices.

1. **Transposicion por columnas**

Como lo hice la encriptacion, problema que tube, como lo solucioné, como lo desencripté, precondiciones

1. **Transposicion por filas**

Como lo hice la encriptacion, problema que tube, como lo solucioné, como lo desencripté, precondiciones

1. **Transposicion por zigzag**

Un metodo de encriptacion muy complicado para programarlo, ya que hay que considerar las longitudes en funcion a la altura de la matriz a crear para poder encriptar. EL mayor problema encontrado al hacer este ejercicio, fue sacar los caracteres que estan en el centro de las matrices creadas, ya que habian que hacer muchas deducciones para poder encontrar un patron logico a usar. Pero al usar la logica matematica y un poco de calculos aritmeticos se logró decifrar una formula para poder encriptar el texto. Para desencriptarlo se aplico una logica un poco inversa, con la diferencia que algunos calculos se los hace a la inversa del original. Las precondiciones para utilizar este metodo es que la altura del zigzag no sea extremadamente alta.

1. **Sustitucion monoAlfabetica**

Para la ecriptacion monoalfabetica se utiliza un alfabeto cualquiera y se reemplaza cada letra por la letra en la misma posicion del nuevo alfabeto. Es un metodo muy sencillo para programar y es uno de los menos seguros en el área de encriptacion. La forma para desencriptar es una de las mas faciles de resolver, por lo tanto no es muy segura para proteger tus datos. Las precondiciones para encriptar con este metodo es que el alfabeto nuevo no sea mas largo ni mas corto que nuestro alfabeto comun.

1. **Sustitucion poliAlfabetica**

Como lo hice la encriptacion, problema que tube, como lo solucioné, como lo desencripté, precondiciones