Práctica Nro. 3

Cifrado de Cesar

Fecha de Entrega: 23 de Abril del 2021

1. Objetivo:
   Implementar el Cifrado de Cesar e Investigar cómo se realiza el criptoanálisis (romper el Cifrado de Cesar)
2. Software
   C++
3. Conceptos teóricos
   Cifrado = (letra del mensaje + clave) mod Tamaño del Alfabeto
   Descifrado = (letra del mensaje - clave) mod Tamaño del Alfabeto

4. Actividades
   a) Implemente el Algoritmo de Cesar considerando:
      - Ingresar el texto plano y el factor de desplazamiento (clave)
      - Construya el objeto emisor y receptor
      - Salida, dependiendo del caso, el texto cifrado o el texto descifrado.
      - Solo debe de considerarse la declaración de variables tipo string

   b) Criptoanálisis: Aplicar la técnica de fuerza bruta para desencriptar el mensaje
      - Entrada: Un texto cifrado
      - Salida: El texto descifrado y el valor de la clave

5. Resultados
   El alumno es capaz de implementar el algoritmo de Cesar, al definir sus funciones de Cifrado y Descifrado, así como el rompimiento de la clave al realizar criptoanálisis.

Rubrica de Evaluación

Concepto	Cumple	Cumple con Obs.	No cumple
Plasma de manera clara en la función de cifrado las bases matemáticas propuestas	4.0	2.0	0.0
Plasma de manera clara en la función de descifrado las bases matemáticas propuestas	4.0	2.0	0.0

Utiliza programación orientada a objetos, modulariza su lógica computacional, usa string	4.0	2.0	0.0
Descifrar el mensaje cifrado que recibe (ejecución función de cifrado)	4.0	2.0	0.0
Cifran los mensajes (ejecución función de descifrado)	4.0	2.0	0.0

Rubrica de Auto-Evaluación Algoritmo de Cesar

Concepto	Si	Regular	No
Cifra los mensajes de al menos 4 de sus compañeros	4.0	2.0	0.0
Sus compañeros descifran sus mensajes, por lo menos 4	4.0	2.0	0.0
Propuso mejoras lógicas en la implementación de su código	2.0	1.0	0.0
Su generación de claves funciona correctamente	2.0	1.0	0.0
Su función de cifrado esta implementada correctamente	4.0	2.0	0.0
Su función de descifrado esta implementada correctamente	4.0	2.0	0.0

Rubrica de Auto-Evaluación Criptoanálisis de Cesar

Concepto	Si	Regular	No
Implementó las funciones para el criptoanálisis de Cesar	10.0	5.0	0.0
Ejecuta correctamente el criptoanálisis del algoritmo de Cesar	10.0	5.0	0.0