**INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO**

Nombres:



**PRÁCTICA 0.- IMPLEMENTACIÓN DE FUNCIÓN CRIPTOGRÁFICA**

Por equipos implementarán alguna función criptográfica DES haciendo uso de bibliotecas existentes para el cifrado/descifrado de un archivo de texto.

**Objetivo**

Seleccionar el lenguaje de programación de su preferencia e implementar una función criptográfica haciendo uso de bibliotecas existentes para el cifrado/descifrado del archivo de texto Marley.txt

**Instrucciones**

Demostración ordenada en clase, Alicia debe mostrar su pantalla, la mitad debe tener el código fuente y en la otra mitad deberá mostrar la ejecución del cifrado del archivo mientras va explicando. Le manda el mensaje a Betito por cualquier medio inseguro y en otra PC Betito hace la demostración del descifrado. Eva deberá modificar el archivo y explicar que pasa en esos casos.



|  |  |  |
| --- | --- | --- |
| **Criterio** | **Valor** | **Tu evaluación** |
| **El programa cuenta con interfaz gráfica que le permita al usuario elegir la opción deseada:**  **cifrado o descifrado y que reciba los parámetros (en caso de ser necesario)** | **0.5** |  |
| **En la demostración se muestra el proceso de cifrado que realiza Alicia (mencionando si se trata de un algoritmo de criptografía simétrica así como el tamaño e importancia de la llave)** | **0.5** |  |
| **La interfaz permite seleccionar el archivo que se va a cifrar/descifrar** | **0.5** |  |
| **Su programa genera el archivo cifrado con el mismo nombre del archivo de entrada más la**  **extensión \_C** | **0.5** |  |
| **Se cierra el programa y se vuelve a ejecutar para el proceso de descifrado (simulando el hecho de que Alicia cifra en una PC mientras que Betito lo descifra en una PC diferente).** | **0.5** |  |
| **Se explica a detalle el proceso de descifrado que realiza Betito y se da una conclusión final.** | **0.5** |  |
| **La interfaz genera el archivo descifrado con el mismo nombre del archivo de entrada más**  **la extensión \_D** | **0.5** |  |
| **Se explica los ataques que puede realizar Eva y se demuestra lo que sucedería en cada caso.** | **0.5** |  |
| **Hay fluidez y dominio del tema** | **0.5** |  |
| **Se entregó en tiempo y se respeta la duración solicitada (3-5 min)** | **0.5** |  |
| **TOTAL** | **5** |  |

Nota: No se requiere ningún reporte por escrito, para esta práctica solo se considerará la demostración en clase. En caso de no hacerlo a tiempo solo se podrá entregar por video el mismo dia, de lo contrario contara con una penalización de 2pts.

M. en C. Nidia A. Cortez Duarte