Máster Universitario en Ciberseguridad e Inteligencia de Datos

Práctica 1: Implementación básica de sistema de cifrado y ataque por fuerza bruta

Objetivo:

Conocer sistemas básicos de cifrado (sustitución/trasposición) e implementar algunos de esos métodos a través de programación, así como analizar las posibilidades de un ataque de fuerza bruta.

Desarrollo de la práctica:

Nota: para los mensajes consideraremos el alfabeto: ABCDEFGHIJKLMNÑOPQRSTUVWXYZ

1. **Implementación de métodos de sustitución**:
    a. Realizar en pseudocódigo los pasos necesarios para generar un cifrado por sustitución empleando el siguiente alfabeto de sustitución:

       "ÑOPQRSTUVWXYZABCDEFGHIJKLMN"

    b. Implementar el algoritmo anterior en Python usando Google Collab. El programa debe solicitar la siguiente información:
        i. Mensaje a cifrar
        ii. Mecanismo a aplicar: cifrado o descifrado
    c. ¿Qué mensaje resulta al descifrar el siguiente texto?

       "IA QVÑ JV IAÑ JÑPÑ JRGHVQÑ QR IAVSCFZR"

    d. ¿Qué modificaciones serían necesarias para utilizar 2 alfabetos de sustitución, de tal manera que las letras impares utilizaran el primer alfabeto y las pares el segundo alfabeto?
    e. Realiza un programa en Python que realiza el cifrado en base a estos 2 alfabetos de sustitución según lo indicado en el apartado anterior:

       Alfabeto 1: "ÑOPQRSTUVWXYZABCDEFGHIJKLMN"
       Alfabeto 2: "ZYXWVUTSRQPOÑNMLKJIHGFEDCBA"

    f. ¿Qué mensaje oculta el texto siguiente?
       GR SÑH OYVTZQL SÑHHZ ZEFÍ HV VGKRIÑN IRGCH ÑIB RAGRIRHÑNHVG RN GI SFHFFL KFLLRZL

Máster Universitario en Ciberseguridad e Inteligencia de Datos

2. Cifrado César y ataque por fuerza bruta

a. Realizar en pseudocódigo los pasos necesarios para implementar un cifrado César.

b. Trasladar el pseudocódigo a un programa en Python con las siguientes características:

   i. Utilizará un alfabeto de 27 caracteres:

      "ABCDEFGHIJKLMNÑOPQRSTUVWXYZ"

   ii. Debe solicitar el mensaje a cifrar y la clave a utilizar

   iii. Como salida del programa, se debe mostrar en pantalla el mensaje original y el mensaje cifrado

c. Realizar en pseudo código los pasos necesarios para hacer un programa que ataque por fuerza bruta un mensaje previamente cifrado con César

d. Trasladar el pseudocódigo a un programa en Python con las siguientes características:

   i. Partimos de la hipótesis de que trabajamos con un alfabeto de 27 caracteres: "ABCDEFGHIJKLMNÑOPQRSTUVWXYZ"

   ii. Debe solicitar el mensaje cifrado, objeto del ataque

   iii. Mostrará como salidas todos los intentos de descifrado