Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad
Semestre 2025-1

Práctica 4: Cifrados Clásicos

Equipo:
Barrientos Sánchez José Antonio
Hernandez Gonzalez Yun
Ortiz Castañeda José Ramón

Fecha de entrega:
10 de septiembre de 2024

Profesor:
Anayanzi Delia Martínez Hernández

Ayudantes:
Cecilia del Carmen Villatoro Ramos
José Angel Arévalo Avalos
Ivan Daniel Galindo Perez
David Armando Silva de Paz

Contents

1 Introducción

2 Desarrollo.

3 Preguntas.

1. ¿Cuántos primos relativos hay en Z_{256}?

   Primero, vamos a descomponer en factores primos a 256:

   $$256 = 2^8$$

   Con la fórmula del totiente de Euler podemos saber el númerp de primos relativos:

   $$\phi(256) = 256 \times \frac{1}{2} = 128$$

   Por lo tanto, el número de primos relativos en Z_{256} es $\phi(256) = 128$.

2. Sea, con A un alfabeto cualquiera. ¿qué se debe cumplir para que f sea una función biyectiva?

3. ¿Cuántas posibles combinaciones no triviales existen para cifrar bytes con César, Decimado y Afin?

   - **Cifrado Cesar**

     Primero debemos notar que los bytes tienen 256 valores. Para el **Cifrado César**, sabemos funciona con un desplazamiento, en el que cada byte se reemplaza con $(x + k)mod256$ donde k es la llave del desplazamiento. Por lo tanto, si se está usando un desplazamiento, solo tenemos tantas combinaciones como valores, por lo que tenemos **256 combinaciones**.

4. ¿Por qué el sistema de archivos de UNIX, aunque un archivo tenga una extensión diferente (o incluso no tenga), sigue reconociendo al archivo original?

5. ¿Por qué los archivos descifrados tienen exactamente el mismo tamaño que antes de cifrar, pero no pudimos leerlos? ¿Por qué no tuvimos que agregar/quitar nada?

6. Ya que base64 no es un cifrado, sino codificación, ¿en qué casos podemos usarlo?

7. Supongamos que estuvieras en Hogwarts y tuvieras que utilizar un búho para comunicarte, ¿cuál crees que sería la mejor opción para mandar mensajes seguros a través de la lechuza?

4 Conclusiones