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. pregunta2

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 $(x + k) mod 256$ 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**.
   - **Cifrado Decimado** El cifrado decimado funciona cuando multiplicamos el valor del byte x por un llave k, para después hacer $mod 256$. Entonces, si qieremos invertir esta operación, k debe der ser primo relativo de 256, y como ya vimos anteriormente, 256 solo tiene 1**28 primos relativos**

- **Cifrado Afin** El cifrado afín es una combinación del cifrado César y el cifrado Decimado, el cuál utiliza la siguiente función $(a \cdot x + b) mod 256$ en el que a es una constante primo relativo y b es una constante de desplazamiento. Así que la combinación de los dos nos da $128 \cdot 255 = 32,640$

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? Ya que el sistema de archivos en UNIX no usa las extensiones para reconocer archivos, se debe a que UNIX trabaja directamente con el contenido del archivo, utilizando propiedades internas como los *números mágicos* para identificar el tipo de archivo, por lo que permite que los archivos sean reconocidos y gestionados independientemente de su nombre o extensión. **linux**

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? Porque el tamaño no es relavante a la hora de cifrar, ya que no se añade o eliminan bytes, solo se modifican con el cifrado.

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

   - Incrustación de datos binarios (como imágenes o archivos de sonido) en HTML, CSS, EML y otros documentos de texto.
   - Garantizar la transferencia, el almacenamiento o la salida seguros de datos que puedan no estar respaldados o dañados.
   - Codificación de certificados SSL, archivos adjuntos de correo electrónico y otra información que requiera el escape de caracteres especiales. **base64**

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?

   Para este caso, y con ayuda del video, se puede utilizar Three-pass-protocol, el cual un método para enviar mensajes seguros sin necesidad de intercambiar claves secretas. Para ello, suponiendo que somos Harry Potter, y le queremos enviar un mensaje a Hermione.

   (a) Primero ciframos el mensaje M con mi clave K_{Harry} y enviamos el mensaje cifrado M' a Hermione
   (b) Ahora, Hermione cifra el mensaje cifrado M' con su clave K_{He} obteniendo M'' y lo envía de vuelta a nosotros.
   (c) Después, desciframos M'' con nuestra clave, eliminando el cifrado y enviamos M''' de vuelta a Hermione.
   (d) Finalmente, Hermione descifra M''' con su clave K_{He} y obtiene el mensaje original M.

4 Conclusiones