Facultad de Ciencias UNAM

Criptografía y Seguridad

Tarea 02

Uziel Vidal Cruz Vargas
Emilio Arsenio Raudry Rico

1. Para un alfabeto de 26 letras ¿Cuántas matrices de 2x2 hay que nos permitan cifrar mediante Hill? Justifica tu respuesta.

2. Investiga un caso de la vida real donde se rompió la seguridad con máximas de Kerckhoffs.

   Las máximas de Kerckhoffs establecen que la seguridad de un sistema criptográfico debe residir únicamente en el secreto de la clave, y no en la confidencialidad del algoritmo. Un caso real donde se violó este principio fue en el diseño del protocolo WEP (Wired Equivalent Privacy) para redes Wi-Fi.

   Inicialmente, el algoritmo de WEP se mantuvo en secreto, confiando en la seguridad por oscuridad. Sin embargo, una vez que el algoritmo se hizo público y fue analizado por la comunidad, se descubrieron múltiples vulnerabilidades, como la reutilización de vectores de inicialización y la debilidad del algoritmo RC4 con claves pequeñas. Esto permitió que atacantes pudieran recuperar claves WEP con herramientas automatizadas en pocos minutos. Este caso demuestra que la falta de transparencia en el diseño criptográfico puede llevar a una falsa sensación de seguridad. [2].

3. Usando el polinomio $x^4 + x + 1$, da la lista de bits de salida de un LFSR asociado usando como semilla una secuencia de ceros, y cualquier otra que escojas.

4. Supón que se manda un criptotexto $c = c_1, c_2, c_3 \ldots$ pero se pierde el bloque c_2, así que se recibe $c = c_1, c_3, c_4, \ldots$ Al descifrar el mensaje ¿Cuál es el efecto de un bloque no recibido al usar los modos de operación CBC, OFB y CTR?

   - **CBC (Cipher Block Chaining):** Para descifrar un bloque c_i se necesita el bloque c_{i-1}. Por lo tanto, al perder c_2:
     - No se puede recuperar el mensaje correspondiente a c_2.
     - El mensaje correspondiente a c_3 será incorrecto.
     - A partir de c_4, el descifrado vuelve a funcionar, pero el resultado estará afectado por el error de c_3.
   - **OFB (Output Feedback):** Es un modo de cifrado por flujo donde la clave de cada bloque se genera independientemente del mensaje. Por tanto:
     - Solo se pierde el mensaje correspondiente a c_2.
     - Los demás bloques pueden descifrarse correctamente.
   - **CTR (Counter Mode):** Similar a OFB, cada bloque se cifra usando una clave generada por un contador, lo que permite paralelismo. Entonces:
     - Solo se pierde el bloque correspondiente a c_2.
     - Los demás bloques no se ven afectados.

5. Investiga qué es el cifrado RC4. Da la descripción de su funcionamiento y sus debilidades.

6. Determina si a es residuo cuadrático módulo n. Muestra tu procedimiento.

   a) $a = 6007, n = 1902$

Se factoriza $n = 2 \cdot 3 \cdot 317$, por lo que usamos el símbolo de Jacobi:

$$\left(\frac{6007}{1902}\right) = \left(\frac{6007}{2}\right)\left(\frac{6007}{3}\right)\left(\frac{6007}{317}\right)$$

Calculamos cada uno:

- $6007 \mod 8 = 7 \Rightarrow \left(\frac{6007}{2}\right) = 1$ (pues $7 \equiv 7 \mod 8$)
- $6007 \mod 3 = 1 \Rightarrow \left(\frac{6007}{3}\right) = \left(\frac{1}{3}\right) = 1$
- $\left(\frac{6007}{317}\right) = 1$ (Fendt, s. f.)

$$\left(\frac{6007}{2}\right) = 1, \quad \left(\frac{6007}{3}\right) = 1, \quad \left(\frac{6007}{317}\right) = 1$$

$$\left(\frac{6007}{1902}\right) = 1 \cdot 1 \cdot 1 = 1$$

El símbolo de Jacobi da 1, lo cual sugiere que podría ser un residuo cuadrático, pero no garantiza que lo sea (pues n no es primo).

b) $a = 83, n = 593$

Como n es primo, se usa el símbolo de Legendre:

$$\left(\frac{83}{593}\right) = 1$$

Entonces, 83 es un residuo cuadrático módulo 593. (Fendt, s. f.)

c) $a = 3677176, n = 4568731$

Como n es primo:

$$\left(\frac{3677176}{4568731}\right) = 1$$

Por lo tanto, 3677176 es un residuo cuadrático módulo 4568731. (Fendt, s. f.)

d) $a = 4568723, n = 4568731$

Nuevamente n es primo:

$$\left(\frac{4568723}{4568731}\right) = 1$$

Entonces, 4568723 es un residuo cuadrático módulo 4568731. (Fendt, s. f.)

Los cálculos se apoyaron en una herramienta online para obtener los símbolos de Legendre y Jacobi [1].

Referencias

[1] Walter Fendt. Online calculator legendre, jacobi, and kronecker symbol. `https://www.walter-fendt.de/html5/men/legendresymbol_en.htm`, n.d. Recuperado el 4 de abril de 2025.

[2] Ezebuike Michael. Kerckhoffs' principle: The backbone of cryptography, 2024. Recuperado el 4 de abril de 2025.