Pregunta 1
Se tiene el siguiente mecanismo de cifrado para mensajes de una sola letra:

$$\mathcal{M} = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, w, x, y, z\}$$
$$K = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, ñ, o, p, q, r, s, t, u, w, x, y, z\}$$
$$E(k, m) := k + m \bmod 26$$
$$D(k, c) := c - k \bmod 26$$

a) ¿ Es perfectamente seguro este mecanismo? Justifica.

b) Si quitamos la llave ñ y lo demás se mantiene igual. ¿Cambia la seguridad del mexanismo? Justifica.

Solución:

a) No es perfectamente seguro pues no cumple la siguiente propiedad:

“Las cardinalidades de los conjuntos claves, mensajes y criptogramas son iguales”

Mostraremos por que:

Al tener una suma en la encriptación y una resta en la decriptación asumimos que:

1. Operamos los índices de los caractéres tanto del mensaje plano como el de la contraseña (en su respectivo alfabeto).

2. El mensaje cifrado es un número.

Sin aún delimitar el alfabeto del criptograma(siguiente pregunta) ya sabemos que la cardinalidad de conjuntos claves es 27 pero de mensajes es 26.

Por lo tanto no es perfectamente seguro.

b) Bajo este criterio la cardinalidad de conjuntos clave y mensaje sí son iguales, veremos que el de criptogramas no y que además no cumplen con la siguiente propiedad:

“Para toda pareja (c, m), existe **una** k tal que m se cifra como c usando k.”

No importa si consideramos que los alfabetos estan en índice base cero o uno, llegaremos a la misma conclusión. Como en la operación usan módulo veintiseis consideramos pertinente usar índice base uno.

Ahora tenemos como posibles claves los elementos del alfebeto utilizado en E.E.U.U.A (26 crácteres), así digamos para el mensaje ’a’, tenemos los siguientes posibles valores comenzando con la llave ’a’ y en orden cronologico hasta llegar a ’z’:

$$[27, 26, 25, 24, 23, 22, 21, 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2]$$

Para el cáracter ’z’ los siguientes:

$$[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]$$

Observamos que es imposible para el mensaje ’a’ producir el criptograma 1, pues el índice de ’a’ ya es 1 y con las claves operamos en un rango $\{1, .., 26\}$.

No existe una clave k tal que ’a’ se cifré como 1 usando k.

Y aún más importante la longitud del conjunto de cripogtamas, $\{1, .., 27\}$ no es igual a la de claves ni mensajes.

Pregunta 2
Considera los mecanismos de cifrado adaptados a cadenas de bytes y descifra los siguientes criptotextos con la llave correspondiente.

a) Sustitución monoalfabética.
C = `0xfb0762a891`,
llave de cifrado k es la permutación ($04 \mapsto 91$, $01 \mapsto 32$, $75 \mapsto 62$, `ff` $\mapsto$ `fb`)
y los demás bytes quedan fijos.

b) Vigenére. $c =$ `0x00ab23cd45`, $k =$ `0xfa03`.

c) Afín. $c =$ `0x23aa7f`, $k = (255, 7)$.

Pregunta 3
El siguiente texto fue crifrado con una sustitución monoalfabética. Encuentra el texto claro en español y describe tu procedimiento de criptoanálisis. Puedes apoyarte del programa Ganzua [a] u otro.

[a] Ganzüa

Pregunta 4

Pregunta 5
Considera la siguiente modificación al sistema one-time real pad; se usan mensajes de longitud arbitraria pero acotada, es decir, $\mathcal{M})\{0,1\}^{\leq \updownarrow}$ (cadenas de bits de longitud entre 1 y $\updownarrow$). Oara encriptar se usan llaves de tamaño $\updownarrow$ y al aplicar el XOR solo se usa el número de bits necesarios de la llave, es decir, $K = \{0,1\}^{\updownarrow}$ y $E(k, m) := k_{|m|} \oplus m$.

a) Muestra que este mecanismo no es perfectamente seguro.

b) Construye un mecanismo perfectamente seguro para $\mathcal{M}$. Justifica la seguridad de tu respuesta.

Pregunta 6

Pregunta 7

Pregunta 8

Pregunta 9

p

Pregunta 10