Pregunta **1**

Enunciado de la pregunta

Notación:

- "a_b" quiere decir "a sub b", indica que b es el subíndice de a
- a xor b quiere decir "a operado con b con xor, es decir, con suma bit a bit en base dos"

Supongamos que definimos, para una clave k (k_1||k_2||..|| k_45) de 45 bits, un cifrador en bloque F_k con tamaño de bloque 90 de la siguiente forma:

F_k(b_1||...||b_90)
=
(b_1 xor k_1, b_2 xor k_2,...,b_45 xor k_45, b_46 xor b_1, b_47 xor b_2, ... , b_90 xor b_45)

a) escribe cómo se utiliza , **en general**, el modo CBC para cifrar y descifrar con un cifrador en bloque.

b) encuentra un método por el que un adversario, **evaluando F_k en una única cadena de bits (distinta de la cadena con únicamente ceros)**, puede obtener la clave subyacente k.

Pregunta **2**

Enunciado de la pregunta

Razona en **una frase o dos** si las siguientes afirmaciones son o no ciertas:

a) Si un problema de decisión está en la clase de complejidad P, siempre existe

un algoritmo polinomial para comprobar una solución propuesta al mismo.

b) // notación: XOR (suma binaria bit a bit), "a_b" representa (a sub b, es decir, "b es subíndice de a")

Un generador pseudoaleatorio F sirve para generar a partir de una semilla corta s, una secuencia más larga F(s) que sirve como contador para cifrar en modo CTR . Así, en cada iteración se hace

clave_i =F(clave_{i+1})

bloque cifrado_ i = bloque texto claro _i XOR clave_i

Pregunta **3**

Enunciado de la pregunta

Definimos una función H que, dada una cadena x de bits de entrada, calcula la salida así:

1. si x tiene más de 160 bits, se queda con los 160 bits más significativos de x

2. si x tiene a lo sumo 160 bits, completa con ceros (en las posiciones menos significativas) para tener una cadena de 160 bits

3. modifica los 80 bits más significativos haciendo un xor con una cadena de ochenta unos

4. modifica los 80 bits menos significativos haciendo un xor con una cadena alternante de ochenta bits, es decir, una cadena del tipo 10101010101...1010

5. da como salida la cadena resultante

¿Es H una función hash?

Si lo es, ¿es CR, PR o TCR?

Pregunta **4**

Enunciado de la pregunta

NOTACIÓN:

- XOR (suma binaria),
- || concatenación
- a_b "a sub b"

Sea f una función que toma una cadena de 5 bits b_1|| ...||b_5 y la transforma en una cadena de 25 bits de la siguiente manera:

- escribimos una cadena de longitud 10 intercalando unos y ceros en la cadena original (empezando por uno)

1 || b_1|| 0 ||b_2 ||1 ||b_3|| 0|| b_4|| 1|| b_5

- copiamos esa cadena y a continuación, su complementaria (es decir, la que se construye reescribiendo cada 1 como un 0 y viceversa) . Dado un bit b, recuerda que su complementario es b xor 1.

así, tenemos:

1 || b_1|| 0 ||b_2 ||1 ||b_3|| 0|| b_4|| 1|| b_5

0 || b_1 xor 1|| 1 ||b_2 xor 1||0 ||b_3 xor 1 || 1|| b_4 xor 1|| 0|| b_5 xor 1

- se añaden de nuevo los cinco bits originales

salida:

1 || b_1|| 0 ||b_2 ||1 ||b_3|| 0|| b_4|| 1|| b_5

0 || b_1 xor 1|| 1 ||b_2 xor 1||0 ||b_3 xor 1 || 1|| b_4 xor 1|| 0|| b_5 xor 1

b_1|| ...||b_5

Por ejemplo; si entra 01011, saldría 1001100111011001100010011001111

Supongamos que se diseña un cifrado simétrico donde dada una clave k de 5 bits, un mensaje m de 25 bits se cifra como $c = m \oplus f(k)$

a) ¿qué tipo de esquema de cifrado es el resultante?

b) ¿qué puedes comentar sobre su seguridad?

Pregunta **5**

Enunciado de la pregunta

NOTACIÓN: a*b es "a multiplicado por b"

Considera un algoritmo que recibe como entrada un número N y dos enteros a y b en {1,..., N-1} , con 1<b < a, y realiza la operación

a*(a-1)*(a-2)*...*(a-b) mod N

Supón que a, b y N son todos números que se escriben con "n" bits. Efectuamos esta tarea con un algoritmo que responde a este diseño:

- y:=1

- j:=0

```
mientras (a-j>0)
y = y * (a-j) mod N
j:=j+1
fin mientras
salida: y
```

¿ Es este algoritmo correcto? ¿es su complejidad lineal en n?

Cuenta, como operaciones relevantes, los productos y las reducciones módulo N.