AUTOESTUDIO CIFRADO DE FLUJO

Curso 15-16. Fundamentos de Seguridad

Entre las tribus de Australia Central, cada hombre, mujer y niño tiene un nombre secreto o sagrado que el más anciano decide al poco de nacer él o ella, y que no conoce nadie sino los miembros totalmente integrados en el grupo. Este nombre secreto nunca se menciona excepto en las ocasiones más solemnes; pronunciarlo al oído de un hombre de otro grupo sería una seria violación de la costumbre tribal. Cuando se menciona uno de esos nombres, se hace con voz muy baja y tomando todas las precauciones para que nadie de otro grupo pueda oírlo. Los nativos creen que un extraño que conozca su nombre secreto tendría poder especial para causarle algún mal por medio de la magia.

***La rama dorada*, SIR JAMES GEORGE FRAZER**

Para la realización de esta práctica se utilizará la herramienta FlujoLab que se puede descargar de la red temática Criptored en http://www.criptored.upm.es/software/sw_m001m.htm.

Tares 1

Pregunta 1. Encuentra la secuencia de salida del generador NLFSR de 4 etapas para las cuatro opciones posibles de sus puertas lógicas (OR y AND) y la semilla 1111. La operación que tienes que realizar es la siguiente:

$$S_4 \oplus \big((NOT\ S_3)\ operación1\ (S_2\ operación2\ S_1)\big)$$

Las operaciones operación1 y operación2 pueden ser un AND o un OR.

Debes rellenar la tabla siguiente:

Semilla	Operación de bit que se realiza	Secuencia Cifrante	Periodo

Pregunta 2. Indica y explica qué sucede cuando se intenta obtener una secuencia cifrante con un generador NLFSR de 4 etapas donde las únicas operaciones que se realizan con los bits de la semilla son OR y AND y la semilla 000000.

Tarea 2. Para el generador LFSR de 3 etapas con el polinomio $x^3 + x^2 + 1$ y la semilla 101.

Pregunta 3. Encuentra la secuencia cifrante y su periodo, rellenando la tabla siguiente.

Iteración	Semilla	Operación	Bit de reemplazo	Bit de salida

Pregunta 4. ¿Es de periodo máximo? Justifica la respuesta

Pregunta 5. ¿Cumple los postulados de Golomb? Justifica la respuesta.

1011100

Tarea 3

Pregunta 6. Con la secuencia cifrante

```
10010100 01100001 00000111 11101010 11001101 11011010 01001110 0010111
```

Cifra el texto SUERTE. Indica la operación lógica que has realizado y el criptograma en bits.

Previamente tendrás que codificar la palabra SUERTE en bits, puedes utilizar cualquier conversor, en la plataforma hay enlaces a dichos conversores. ¿Puedes convertir el criptograma obtenido en texto?

Pregunta 7. Con la secuencia cifrante anterior, indica el tamaño del texto que será necesario para utilizar 10 veces la secuencia cifrante completa.

Tarea 4. Aquí es necesario la utilización del software FlujoLab. Con la secuencia cifrante obtenida utilizando la semilla 1010 y el polinomio primitivo 4, 3, 0, cifra de forma independiente estas tres palabras de 3, 4 y 5 caracteres lee, anda y mucho. Dichas palabras se han tomado de la frase "El que lee mucho y anda mucho, ve mucho y sabe mucho" (Mirar http://cvc.cervantes.es/literatura/clasicos/quijote/default.htm)

Pregunta 8. ¿Cuál es la secuencia cifrante?

Pregunta 9. Rellena la siguiente tabla.

Texto	Cifrado en código 64	Número de caracteres distinto del relleno

Pregunta 10. Justifica la aparición del carácter de relleno en los tres cifrados anteriores, rellenando la siguiente tabla.

Palabra	Texto cifrado en binario	Relleno en código 64	Justificación

Tarea 5

Después de formar un mensaje con la palabra anda repetida muchas veces (andaandaanda) y cifrándolo con la misma secuencia cifrante, el resultado es el que se muestra a continuación. Se observa que la cadena se repite cada 80 caracteres

P0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC26MF3P0fSKRn7n1GDCqqz6M59OkfdIxz7kFuGCqW57c5yMELdLBb+kFSMD6W258tyP0jYLBn0lVSDBaC2

Pregunta 11. Justifica la razón por la cual dicha cadena se repite cada 80 caracteres.

Tarea 6

Pregunta 12. Obtener una secuencia cifrante de 50 bits a través del algoritmo A5/1. Utilizar para ello la siguiente semilla de 64 bits

R1: 1000000000000000001

R2: 0111111111111111111110

R3: 10101010101010101010101

Indica la secuencia obtenida.

Pregunta 13. Explica con detalle la secuencia de pasos que han tenido lugar en la pregunta anterior hasta obtener los cuatros primeros bits de la misma. Te ayudamos mostrando cómo se ha obtenido el primer bit

A5/1	**R1** **R2** **R3**	**Realimentación**	**S_i**
Paso 1	1000000000000000001 0111111111111111111110 10101010101010101010101	No Desplaza 1 xor 0 = 1 0 xor 1 xor 0 xor 1 = 0	1 xor 0 xor 1= 0

Tarea 7

Pregunta 14. Con estos 8 bits 10010001 de un LFSR de 4 celdas. Plantea y resuelve el sistema de ecuaciones que aparece al realizar un ataque de Berlekamp-Massey. Escribe el polinomio encontrado