Casos prácticos

Cifrado en flujo

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

Software: FlujoLab: http://www.criptored.upm.es/software/sw_m001m.htm

1 | Generadores LFSR y m-secuencias

Tenemos estos tres generadores LFSR de 6 etapas que se indican:

- LFSR1: 6, 3, 0
- LFSR2: 6, 4, 1, 0
- LFSR3: 6, 5, 2, 1, 0

Pregunta 1.1. Encuentra la secuencia la salida para las semillas 100101 y 101001.

Pregunta 1.2. Para cada una de las secuencias comprueba los Postulados de Golomb.

Pregunta 1.3. Indica qué secuencias son de período máximo y si son m-secuencias o no.

Pregunta 1.4. Justifica si los polinomios propuestos son factorizables, irreducibles o primitivos.

2 | Ataque de Berlekamp-Massey

Se conocen estos 20 bits 11100111000110101001 consecutivos de la secuencia completa de un LFSR primitivo de 10 celdas:

Pregunta 2.1. Haz un ataque por Berlekamp-Massey y encuentra el polinomio utilizado en el registro de desplazamiento. Puedes mirar el informe que te entrega FlujoLab pero no lo incluyas en el informe.

Pregunta 2.2. Genera la secuencia completa suponiendo que la semilla es 1111111111. Muestra en el informe sólo los primeros 64 bits.

Pregunta 2.3. La clave que has generado tiene todas las posibilidades de no estar en fase con la usada en la cifra. Si el criptograma resultado de esa cifra Base 64 es el que se indica más abajo, ¿cómo podrías encontrar ahora la clave en fase con la usada en la cifra? Observación: no se pide que la encuentres, sólo que digas cómo lo haría un programa de forma eficiente. Criptograma: wh/PykVs6cpFeyIlydkRhROO4BuC+/k+hVMKZ5x1ixjtw/uR7PAvuBhMJ+SGkjlb1O8v4a7jS03/

Pregunta 2.4. Conociendo que la semilla era 1000000001, descifra ese criptograma. ¿Cuál es el mensaje en claro?

3 | Cifrado con A5/1

Introduce como semillas en los tres registros del algoritmo A5/1 del software FlujoLab los valores que se indican (usar copiar y pegar):

1. Semilla R1: 1000101010101010010
2. Semilla R2: 0001010011010100101001
3. Semilla R3: 11101010101110100101001

Genera los 10 primeros bits de la secuencia cifrante paso a paso.

Pregunta 3.1. Justifica los 6 primeros bits de salida de esa secuencia, indicando en cada momento de reloj los siguientes datos:

4. Valor de los bits en las celdas de salida de R1, R2 y R3.
5. Suma xor de la salida.
6. Valor de los bits en celdas función mayoría C9 en R1, C11 en R2 y C11 en R3.
7. Resultado de la función mayoría, qué registros desplazan.
8. Repetir desde el paso 1 hasta obtener el sexto bit de salida.

Vuelve a cargar las semillas, genera ahora 6.000 bits de secuencia de clave y descifra este criptograma:

XlKzcCAIcO8lJ9cgjaJdJ+niQBPDXArDvrR9UhNnt6LTuaWRnTNtSBli1kk7lBmhSiziTlRArMJ2bBPxMYNcF29ap0kR4SJ1D+PNlC+FqspSlyNxB9qcGgyiRrWQgh1TNom8Q3bf8J+OBXFiLfY0EZ
0w7WOdXFfCgykhEzKChd3AiYjPcG46kX8j/FBY/qvdHZXhtZMx4iOri2EfKBRH5L5SyOKa9lgjYDB0VWNq5XM1OwZJulh3TXBT7hRAe/u3tiJGla4OcUqcVcxWejz4P/
ftiL+6VT5F5WcUP9ZPkLD0coUEnjSVjADiAnaQYRA+tnpnQNCjPUQvDsy0OukHQM97BSzLIpVI9i8mmAPx2Z5+W3zHpISOf/Dx5zC6qJoayYckDC+U/
PvH57Rl9h5u66EOpEZ5GWISPV9Al1bdb5WqBSv5wybNOJ5NYsqnUZIzsSF7cNN8Tdf/KAujV7JITHAN2FA5VljQB0Og41Z0yMmGvYGPfi8bdZeeYKx14TejGz0SN3zIdT91/
B1RWXfxdguLTbEO21DSmeKmwRiq2RHQQMqBlXlgcyAFn8sATGmgT5f8t95ch5VZUogN+fNFllr5cGeXrYlOGSHmx1bAy7jDOgD5nmKDJc+xEWup9Lb/
mJuuNq+MRAWQ2/YclQQ4d27/GivX+RGecQyscisMALSBgxaDcb1YQnCAsbTA3uJ0dPejbAQ30eDAh/
ybtEjyLSmz6KaPlGw2yJed2RV7smFyqPueiGSk16oNG4JTGso5cJki42xP3ptlmFsQHy9P6nZn30VkcNpqC88cBqLnuGzagLBjnLLHwuXtaPzbKzhD8lXXkoPHknNv17lgpElTioAsAdlNtM5
uZHlGmRnq5mWqeHqKBSPU9i+tfPSlqY75JMwMMh2i6tbJQ+jKxZuN2qfYk+CRNnkc4vURRgq2eSOP2MpkL8eChWwunIFAapNhUXrmXnhwvPkPNJw4nxgWYtNkcXA=

Pregunta 3.2. ¿Cuál es el mensaje?

Pregunta 3.3. Para este ejemplo concreto, ¿por qué es suficiente generar tan sólo 6.000 bits de la secuencia cifrante?

Telefónica EDUCACIÓN DIGITAL