Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

"Simmetric cryptosystems: Stream ciphers"

Exercises

Exercise 1:

Golomb's postulates

a) Given the sequence: 00101001110110 Are Golomb's postulates fulfilled?

Solution:

a)

- G1. Number of '1' = 7 ; Number of '0' = 7. Then, the first postulate is fulfilled.
- G2.

Run: 00 → length 2

Run: 1 → length 1

Run 0 → length 1

Run 1 → length 1

Run 00 → length 2

Run 111 → length 3

Run 0 → length 1

Run 11→ length 2

Run 0 → length 1

Total: 9 Runs.

4 or 5 runs of length 1? Yes

2 or 3 runs of length 2? Yes

1 or 2 runs of length 3? Yes

Then, the second postulate is fulfilled

- G3. We calculate autocorrelation, AC(k)

K=1

00101001110110

01010011101100

AC(1) = (A-F) / T = 6-8 /14 = -2/14

K=2

00101001110110

10100111011000

AC(2) = (A-F) / T = 6-8 /14 = -2/14

K=3

00101001110110

01001110110001

AC(3) = (A-F) / T = 6-8 /14 = -2/14

K=4

00101001110110

10011101100010

AC(4) = (A-F) / T = 8-6 /14 = 2/14

AC is not constant and then, the third postulate is not fulfilled.

Exercise 2:

Cipher the following plaintext: 101001111, with the key 010010001, randomly generated, assuming it is encrypted using a Vernam cipher.

Solution:

101001111 XOR 010010001 = 111011110

Exercise 3:

Consider a bit generator comprising a linear feedback shift register (LFRS) of 4 cells:

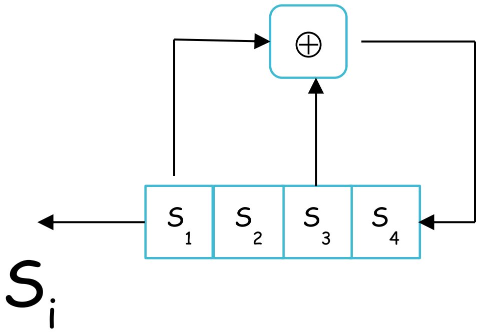
a) If the seed of the generator is S1S2S3S4=0111 and the polynomial f(x)=x4+x2+1, obtain the resulting record sequence and indicate its associated period and Linear Complexity.

b) If the seed of the generator is S1S2S3S4=1101 and the polynomial f(x)=x4+x2+1, obtain the resulting record sequence and indicate its associated period and Linear Complexity.

c) If the seed of the generator is S1S2S3S4=1110 and the polynomial (primitive) f(x)=x4+x+1, obtain the resulting record sequence and indicate its associated period and Linear Complexity.

Solution:

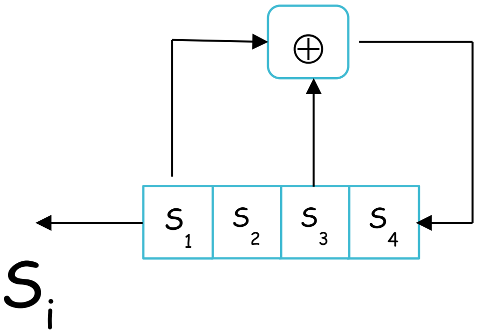
a)



Registry state	Generated bit
0111	0
1111	1
1110	1
1100	1
1001	1
0011	0
0111	0
1111	1

Period= 6; LC= 4

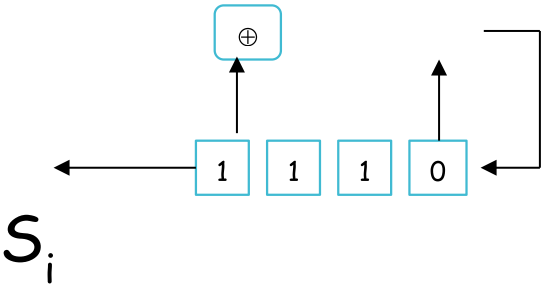
b)



Registry state	Generated bit
1101	1
1011	1
0110	0
1101	1
1011	1

Period= 3; LC= 4

c)



Registry state	Generated bit
1110	1
1101	1
1010	1
0101	0
1011	1
0110	0
1100	1
1001	1

0010	0
0100	0
1000	1
0001	0
0011	0
0111	0
1111	1
1110	1

Period =15; LC= 4

Exercise 3:

Consider the RC4 stream cipher. Which is the value of the key that leaves the state S without changes in initialization phase? – that is, after the initialization phase, vector S must contain the values 0-255 in ascending order.

Solution:

The key has a length of 256 bytes. We have to achieve j=i for each step so that after Swap (S[i],S[j]), S remains unchanged. This is done with the following values: K[0]=K[1]=0, K[2]=255, K[3]=254… K[255]=2.