



“Simmetric cryptosystems: Stream ciphers”

Exercises

Exercise 1:

Golomb's postulates

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

Exercise 2:

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

Exercise 3:

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

- If the seed of the generator is $S_1S_2S_3S_4=0111$ and the polynomial $f(x)=x^4+x^2+1$, obtain the resulting record sequence and indicate its associated period and Linear Complexity.
- If the seed of the generator is $S_1S_2S_3S_4=1101$ and the polynomial $f(x)=x^4+x^2+1$, obtain the resulting record sequence and indicate its associated period and Linear Complexity.
- If the seed of the generator is $S_1S_2S_3S_4=1110$ and the polynomial (primitive) $f(x)=x^4+x+1$, obtain the resulting record sequence and indicate its associated period and Linear Complexity.

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.