Cryptography
Lecture five

Stream Cipher(2)

Assis prof. Dr. Saja Jasem Mohammed

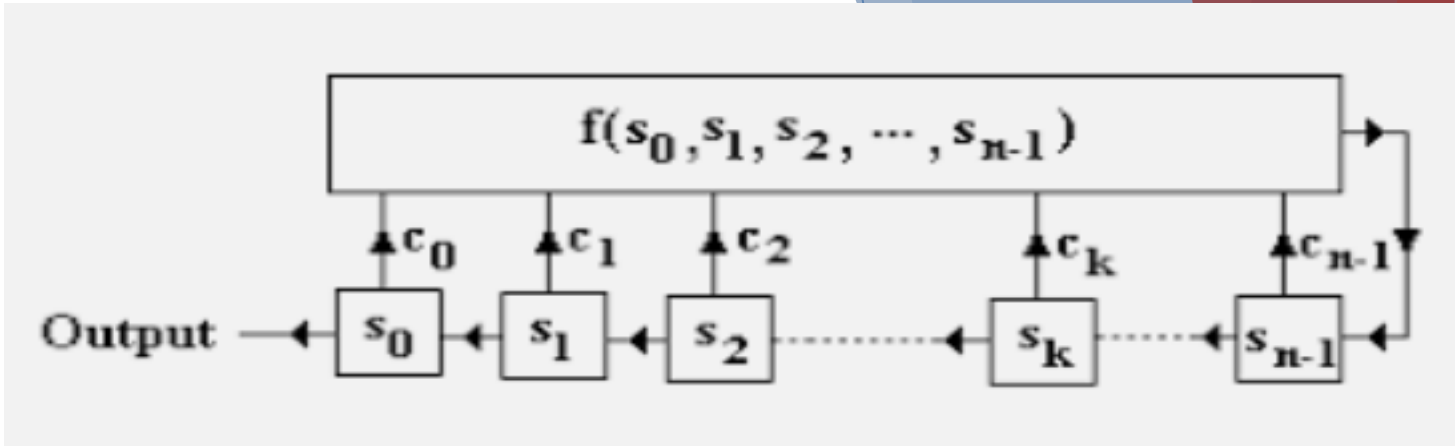
PRNG methods

- Linear feedback shift register (LFSR)
- Non linear feedback shift register (NLFSR)

Feedback Shift Registers (FSRs) are the basic components of many keystream generators used in stream ciphers. Each time the system is clocked, the internal state is shifted right, outputting one symbol, and the new left bit is computed from the previous state by a function f.

1. The Linear Feedback Shift registers (LFSRs) use a linear function f, and are the most commonly used and studied.
2. The Nonlinear Feedback Shift Registers (NLFSRs) use a nonlinear function f.

Linear Feedback Shift Registers:



- A **linear feedback shift register (LFSR)** of length ***n*** consists of ***n*** stages (or flipflops) numbered 0, 1, …, ***n***-1, each capable of **storing one bit** and having **one input and one output**; and a **clock** which controls the movement of data. These stages are connected with each others by a **feedback function**.
- During each unit of time the following operations are performed:

1- The content of stage 0 is output and forms part of the output sequence.

2- The content of stage ***i*** is moved to stage *i*-1 for each *i*, $1 \leq i \leq n-1$.

3- The new content of stage ***n***-1 is the feedback of previous contents of a fixed subset of stages 0, 1, …, ***n***-1 (according to f(S0,S1,S2,S3,….,Sn-1))

- **The output is gotten from S0**

Linear Feedback Shift Registers

- A general form of feed back function

$$S_{n-1}(t+1) = \sum^{n-1}_{i=0} C_i S_i(t)$$
$$= C_0S_0 + C_1S_1 + C_2S_2 + \ldots + C_{n-1}S_{n-1}$$

Where :

- S : State
- C : Coefficients
- T : time
- N : no. of states

Notes

- The sequence generated from the LFSR **is periodic**, The best sequence is the long period sequences.
- If we have LFSR of n stages, there are 2^n-1 of possible output states.
- A sequence produced by a length n LFSR which has period 2^n-1 is called a **PN-sequence** (or a Pseudo-Noise sequence).
- The initail value and the coefficients determine the length of sequence (it mean the generator do not always generat the maximum length)

Example1:

- Give the random sequence when :

- N =4
- Initial state: 0101
- Coefficients = 1 0 0 1

- Solution :

Using the coefficients, we can find the feedback function

C=1001➔ F=S0+S3

t	S0	S1	S2	S3
0	0	1	0	1
1	1	0	1	1
2	0	1	1	0
3	1	1	0	0
4	1	0	0	1
5	0	0	1	0
6	0	1	0	0
7	1	0	0	0
8	0	0	0	1
9	0	0	1	1
10	0	1	1	1
11	1	1	1	1
12	1	1	1	0
13	1	1	0	1
14	1	0	1	0
15	0	1	0	1

- At the end of table, the column of (S_0) is considered the correct sequence for solution.

= **0101100010001111**

- Try to encrypt the plaintext= 'X Y' = (88 & 89)
- X = 01011000 & Y= 01011001

- P = 0101100001011001
- Key = 0101100100011110
- (XOR)
- C =

- **H.W.:**
- **Find the out put of each LFSRs below if you have the initial states [1,1] and [1,1,1] respectively**
- **Note the solution must include:**

  Figure of LFSR

  The generating table

  The output sequence.