Stream Ciphers

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Classifications**
- **Feedback Based Stream Ciphers**
  - **Linear Feedback Shift Registers**
  - **m sequences**

Block vs Stream Ciphers

- **Differences are not definitive.**
- **Blocks Ciphers process plaintext in large blocks.**
- **Stream Ciphers process plaintext in small blocks, even bits**
- **Pure Block ciphers are memory-less.**
- **Stream cipher encryption depends not only on the plaintext, key but also on the current state,**

One Time Pad

- **A Vernam cipher over the binary alphabet is defined by:**

$$c_i = m_i \oplus k_i, \text{ for } i = 1, 2, 3, \ldots$$

- **Unconditionally secured, H(K)≥H(M)**

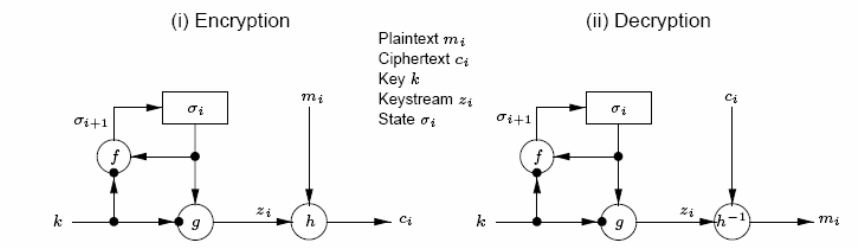
One Time Pad

- **Drawback: key as long as the plaintext.**
- **This motivates the design of stream ciphers where the key stream is generated from a small key.**
- **The intent is protection against computationally bounded adversary.**

Synchronous Stream Ciphers

- **Keystream is generated independently of the plaintext message and of the ciphertext.**
- **Encryption process:**
  - **Updating a state variable using $\sigma_{i+1} = f(\sigma_i, k)$**
  - **Generating a key stream, $z_i = g(\sigma_i, k)$**
  - **Producing the ciphertext stream, $Ci = h(z_i, m_i)$**
- **E.g.: Binary Additive Stream Cipher:**
  - **streams are binary and h is $\oplus$**

General Model of a synchronous stream cipher



Properties of Synchronous Stream Ciphers

1. **Synchronization Requirements:**
   1. **Sender and Receiver must be synchronized – using the same key and operating at the same state within that key**
   2. **Insertion/Deletion may cause loss of synchronization**
   3. **Re-synchronization may need re-initialization and/or special marks in the stream at regular intervals.**
2. **No Error Propagation:**
   1. **Modified digit does not affect decryption of other digits**
3. **Active Attacks:**
   1. **Insertion/Deletion/Replay cause loss of synchronization, thus is detected by the decryptor.**
   2. **Due to lack of error propagation, the adversary can determine ciphertext and plaintext pairs.**

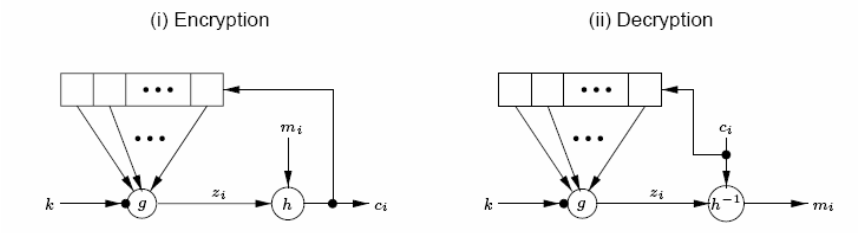
Self Synchronization Stream Ciphers

- **A self-synchronizing or asynchronous stream cipher is one in which the key stream is generated as a function of:**
  - **the key**
  - **a fixed number of previous ciphertext digits.**

Self Synchronization Stream Ciphers

- **$\sigma_i = (C_{i-t}, C_{i-t+1}, \ldots, C_{i-1})$**
- **$z_i = g(\sigma_i, k)$ $C_i = h(z_i, m_i)$**
- **where $\sigma_0 = (C_{-t}, C_{-t+1}, \ldots, C_{-1})$ is the initial state**
- **and z_i is the keystream**
- **and c_i is the cipher-stream**

General Model of a self-synchronization stream cipher



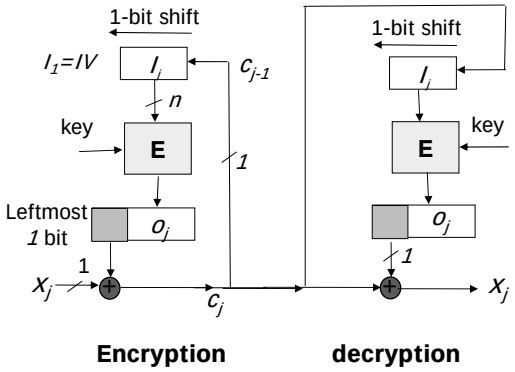
Properties

- **Self-synchronization:**
  - **possible with insertions/deletions (at most t digits may be lost)**
- **Limited Error Propagation:**
  - **1 digit modification/insertion/deletion may cause incorrect decryption of up to t digits.**
- **Active Attacks**
  - **Modification can be detected due to incorrect decryption – better than synchronous stream ciphers.**
  - **It is more difficult than for synch. stream ciphers to detect insertion / deletion / replay of ciphertext digits.**
- **Diffusion of plaintext statistics: Better**

Need for Modes of Block Ciphers

- **Block Ciphers deal with blocks of data**
- **In real life there are two important issues:**
  - **plaintext much larger than a typical block length of 128 bits**
  - **plaintext not a multiple of the block length**
- **The obvious solution is the first mode, called the Electronic Code Book (ECB)**
- **These modes were first standardized in FIPS Publication 81 in 1980.**

Example: 1 bit CFB



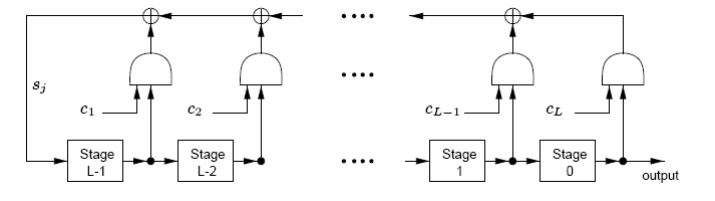
Feedback Shift Registers

- **They are the basic blocks of many keystream generators.**
  - **Linear Feedback Shift Registers (LFSRs)**
  - **well suited for hardware implementations**
  - **can produce sequences of large period**
  - **good statistical properties**
  - **can be analyzed by algebraic techniques**

Linear Feedback Shift Registers

- **An LFSR of length L consists of**
  - **L stages (or delay elements) capable of storing 1 bit each and**
  - **a clock controlling the movement of data.**
- **During each unit of time:**
  - **Content of stage 0 is output**
  - **Content of stage j is moved to stage j-1 for each j (1 to L-1)**
  - **New content of stage L-1 is the feedback bit computed as sum without carry of previous contents of a fixed subset of stages.**

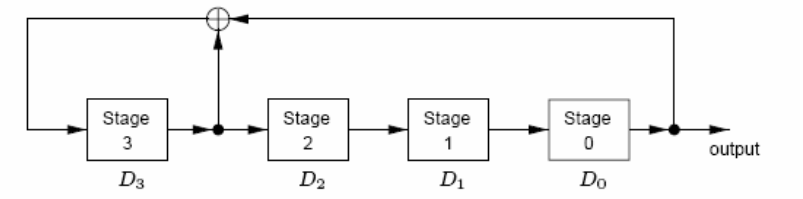
An LFSR of length L



- **Denoted as <L,C(D)>**
  - **$C(D)=1+c_1D+\ldots+c_LD^L$ is called the connection polynomial.**
  - **L is the length of the LFSR**

Example

- **Consider the LFSR <4,1+D+D^4>**



Sequence of the LFSR

t	D_3	D_2	D_1	D_0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1
3	0	1	0	0
4	0	0	1	0
5	0	0	0	1
6	1	0	0	0
7	1	1	0	0

Sequence of the LFSR

t	D_3	D_2	D_1	D_0
8	1	1	1	0
9	1	1	1	1
10	0	1	1	1
11	1	0	1	1
12	0	1	0	1
13	1	0	1	0
14	1	1	0	1
15	0	1	1	0

Periodicity of the LFSR sequences

- **If C(D) is a connection polynomial of degree L**
  - **and is irreducible over Z_2, then each of the 2^L-1 non-zero initial states of the LFSR produces an output sequence with period equal to the least positive integer N, such that C(D) divides $1+D^n$**

Periodicity of the LFSR sequences

- **For some polynomials all the cycle lengths are equal to 2^L-1.**
- **These polynomials are called primitive polynomials.**
- **The sequence is then called m-sequence.**
- **It has good statistical properties.**
- **Example: $1+D+D^4$ was also primitive and thus we obtained a maximum length LFSR.**

Reconstructing the LFSR?

- **Given a sequence can we reconstruct the LFSR which generates the sequence.**

Generating the sequence

- **An LFSR is said to generate a sequence s if there is some initial state for which the output sequence of an LFSR is s.**
- **A sequence of finite length n is denoted by s^n.**

Linear Complexity

Linear Complexity of an infinite binary sequence s, denoted L(s) is defined as:

1. If s is the 0 sequence, L(s)=0

2. If no LFSR generates s, L(s)=∞

3. otherwise, L(s) is the length of the shortest LFSR that generates s.

Linear Complexity for a finite sequence

- **Linear Complexity for a finite sequence s^n, is the shortest LFSR that generates a sequence having s^n as its first n terms.**

Example

- **Reconstruct an LFSR (of the shortest length) which generates the sequence 00111011.**

Points to Ponder!

- **Can you modify the LFSR with connection polynomial primitive to include the all 0 state?**

Further Reading

- **D. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC**
- **A. Menezes, P. Van Oorschot, Scott Vanstone, “Handbook of Applied Cryptography” (Available online)**

Next Days Topic

- **Stream Ciphers (contd.)**