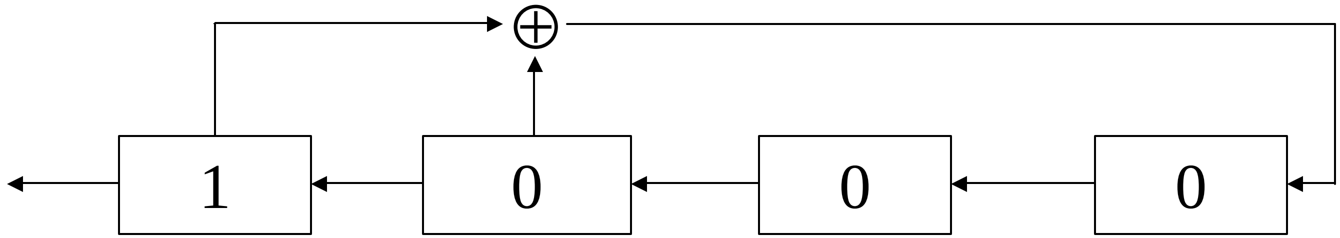
Introduction to Cryptography CS 355

Lecture 10

Linear Feedback Shift Register

Linear Feedback Shift Register (LFSR)

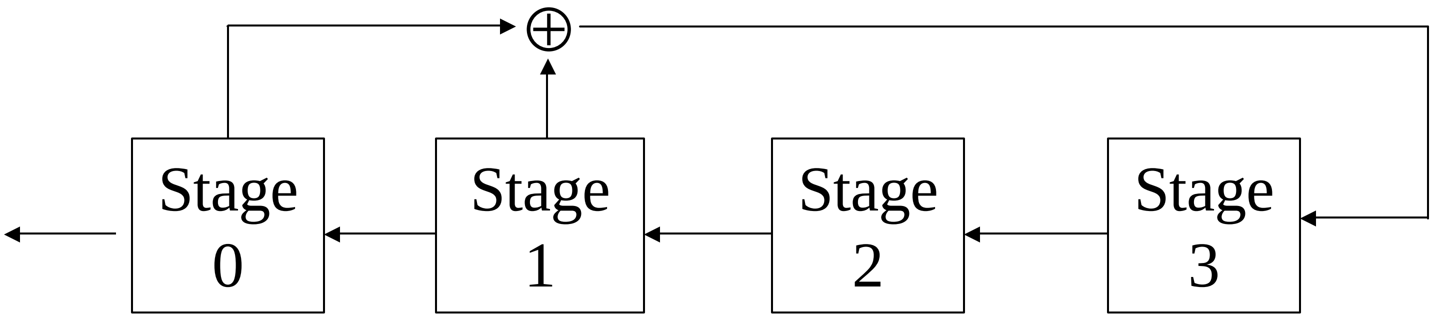
- Example:



- Starting with 1000, the output stream is
  - 1000 1001 1010 1111 000
- Repeat every $2^4 - 1$ bit
- The seed is the key

Linear Feedback Shift Register (LFSR)

- Example:



- $z_i \quad = z_{i-4}+z_{i-3} \bmod 2$
  $= 0 \cdot z_{i-1} + 0 \cdot z_{i-2} + 1 \cdot z_{i-3} + 1 \cdot z_{i-4} \bmod 2$

- I.e., stages 0 & 1 are selected.

Properties of LFSR

- Fact: given an L-stage LFSR, every output sequence is periodic if and only if stage 0 is selected
- Definition: An L-stage LFSR is maximum-length if some initial state will results a sequence that repeats every $2^L – 1$ bit
- Whether an LFSR is maximum-length or not depends on which stages are selected.

Maximum-length LFSR

- Fact: Given an L-stage maximum-length LFSR, any non-zero initial state produces an output sequence with period equal to 2^L-1, this is called a m-sequence.

- Fact: The distribution of patterns having fixed length is almost uniform in a m-sequence.

Cryptanalysis of LFSR

- Vulnerable to know-plaintext attack
  - A LFSR can be described as
    $z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2$
  - Knowing 2*m* output bits, one can
    - construct *m* linear equations with *m* unknown variables $c_0, \ldots, c_{m-1}$
    - recover $c_0, \ldots, c_{m-1}$

Cryptanalysis of LFSR

- Given a 4-stage LFSR, we know
  - $z_4=z_3c_3+z_2c_2+z_1c_1+z_0c_0$ mod 2
  - $z_5=z_4c_3+z_3c_2+z_2c_1+z_1c_0$ mod 2
  - $z_6=z_5c_3+z_4c_2+z_3c_1+z_2c_0$ mod 2
  - $z_7=z_6c_3+z_5c_2+z_4c_1+z_3c_0$ mod 2
- Knowing $z_0,z_1,\ldots,z_7$, one can compute c_0,c_1,c_2,c_4.
- In general, knowing 2n output bits, one can solve an n-stage LFSR

Usage of LFSR

- Easy to implement in hardware
- Multiple LFSR's are often combined to achieve better security

Content Scrambling System (CSS)

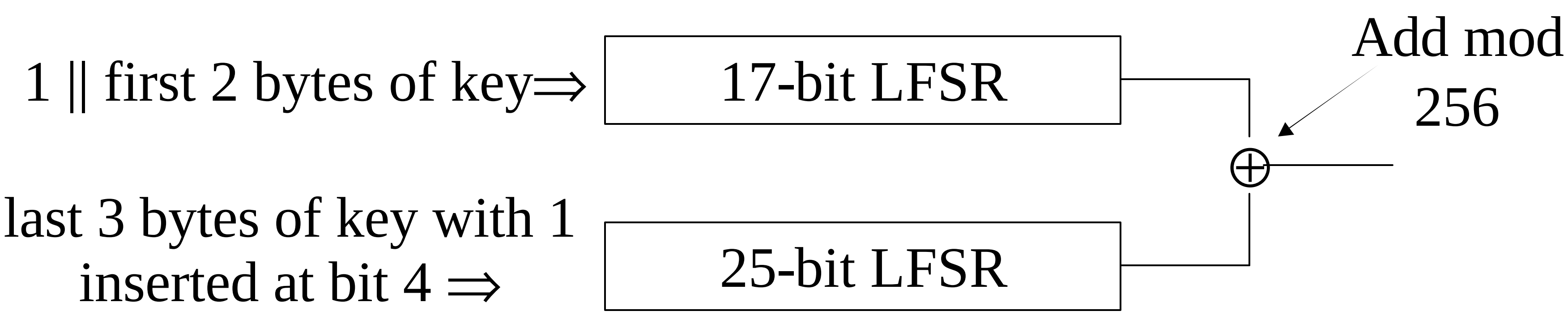
- Designed by Matsushita and Toshiba, and used for encrypting DVD videos
- There is a set of 409 player keys
- Each DVD player has one player key
- Each disk has a key data block
  - the disk key encrypted under the disk key (hash)
  - disk key encrypted with player key 1
  - …
  - disk key encrypted with player key 409
- Knowing the disk key, one can decrypt the DVD

Attacking CSS

- Knowing a disk key, by attacking the CSS cipher, one can recover all player keys
  - takes about 2^{25} time
  - breaks the revocation model of CSS
- It is possible to attack the hash to recover the disk key
  - takes about 2^{25} time

CSS Stream Cipher

- Key = 5 bytes = 40 bits
  - brute-force attack is possible
  - more efficient attacks exist



Given 6 output bytes, a trivial 2^{16} attack exists

A similar attack with 5 output bytes exists

Coming Attractions …

- Modular Exponentiation
- Fermat's Little theorem
- Euler's Theorem

- Recommended reading for next lecture:
  - Trappe & Washington: 3.5, 3.6