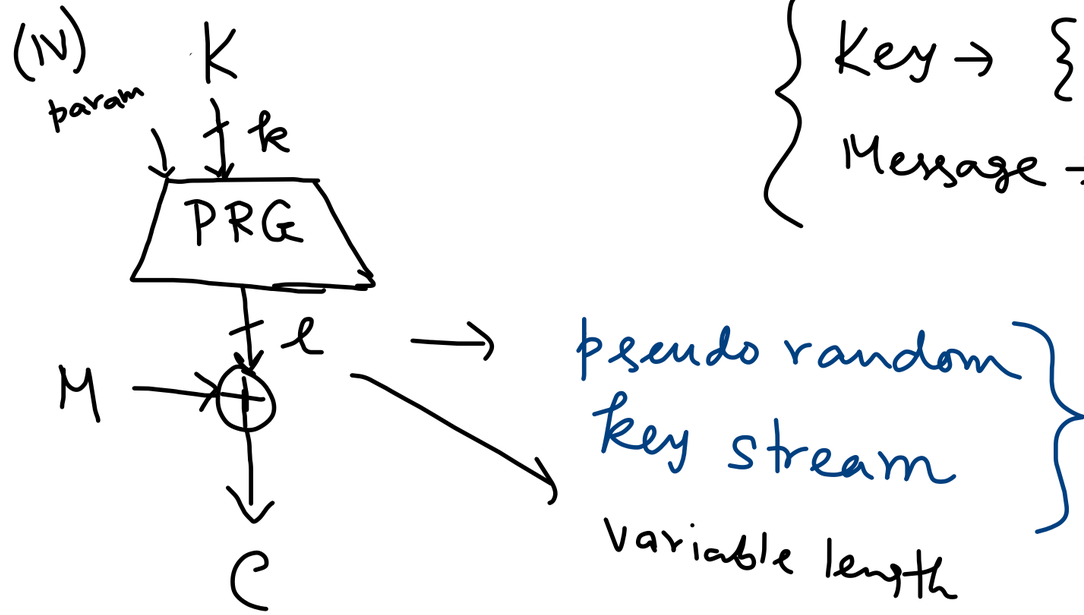
Stream Cipher

M → l-bit



Key → $\{0,1\}^k$

Message → $\{0,1\}^*$

→ pseudo random key stream

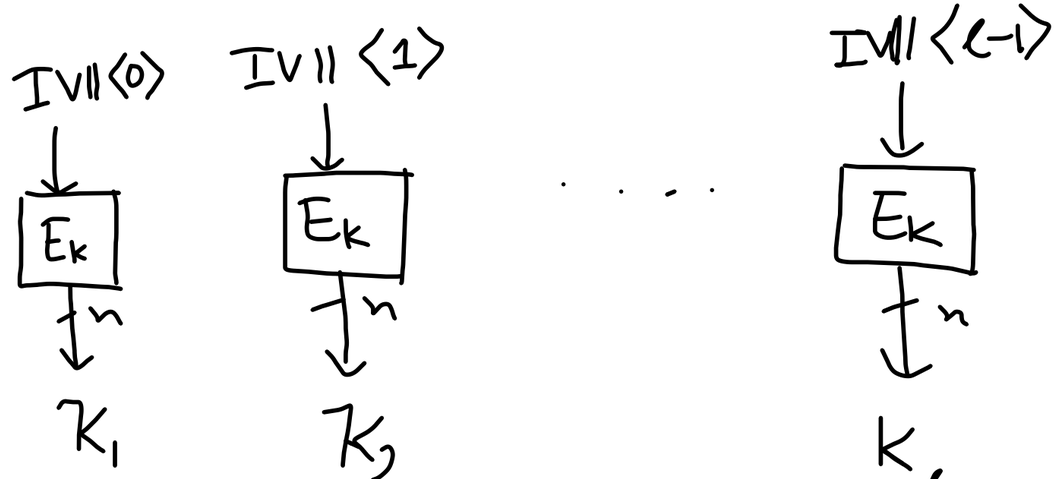
Variable length

Stream-Cipher Design

(Stream generation)

- Block-cipher / PRF based
- Dedicated
  - FSR (Feedback Shift Register) based
  - Others

Block-Cipher based Stream generation



ℓ - bit

$\left\lceil \frac{\ell}{n} \right\rceil$ - block-cipher invocation

Feedback Shift Register

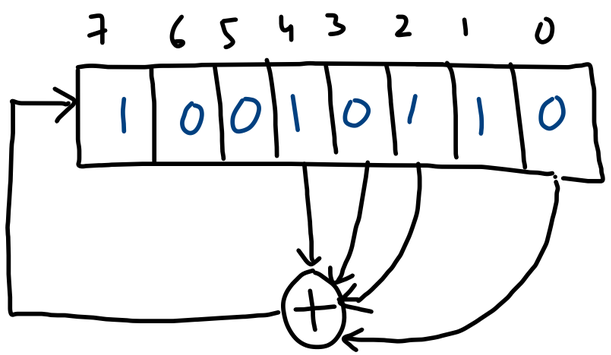
$M \rightarrow C$

$K = M \oplus C$

Linear Feedback Shift Register (LFSR)

max period

$\hookrightarrow (2^n - 1)$



- O/P → 0-th position
- 1 Right Shift
- Update 7-th position

Size → 8

tap position → {0, 2, 3, 4}

$z_8 = z_4 \oplus z_3 \oplus z_2 \oplus z_0$

$z_9 = z_5 \oplus z_4 \oplus z_3 \oplus z_1$

$z_{i+8} = z_{i+4} \oplus z_{i+3} \oplus z_{i+2} \oplus$

{ 0110100100 ....

Not Secure if message length > State Size

(assuming you know state-size & tap positions)

$n = 8$

$$z_{i+8} = c_7 \cdot z_{i+7} \oplus c_6 \cdot z_{i+6} \oplus \cdots \oplus c_0 \cdot z_i$$

$z_8 = \cdots$

$z_9 = \cdots$

$\vdots$

$z_{15} = \cdots$

$\Downarrow$

Unique solution if maximal LFSR.

} 8 eqn, 8 unknowns

→ Calculate the tap positions.

Observed
$z_0 z_1 \ldots z_{15}$

Remedy

- Output a non-linear function of the tap bits.
- Run multiple LFSRs together. Output one non-linear combinations of the outputs.

Trivium

State size → 288

3 - NFSR

- A, B, C
- Size 93, 84, 111

(K||0*) (IV||0*) (0*111)

Initialize

K → 80 bit

IV → 80 bit

No o/p for 4×288 = 1152 rounds

Content Scrambling System

- DVD encryption
- 40-bit → key

I/P : seed $s \in \{0,1\}^{40}$

O/P : l-bytes

Attack

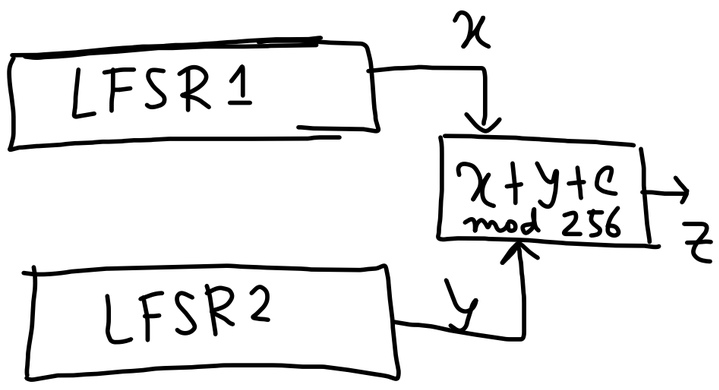
2^{16}

$s = s_1 \| s_2$

16 | 24

LFSR1 (17 bit) → load $1 \| s_1$

LFSR2 (25 bit) → load $1 \| s_2$



$(x+y) \rightarrow 0 \ldots 510$

if $x+y > 255$

else $c=1$

$c=0$

Content Scrambling System

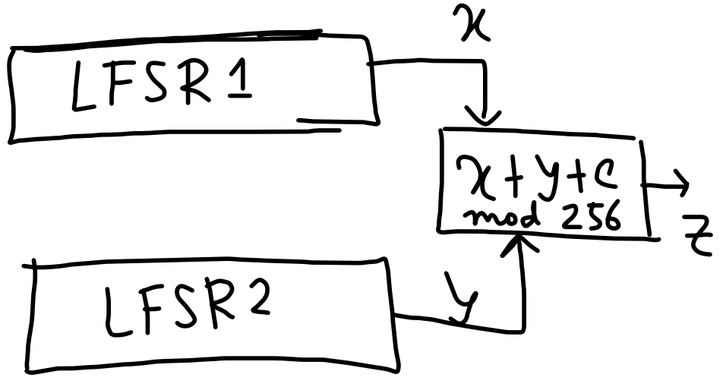
- DVD encryption
- 40-bit → Key

LFSR1 → $x_1\ x_2\ x_3$

LFSR2 → $y_1\ y_2\ y_3$

O/P → $z_1\ z_2\ z_3$

$x_i, y_i \in \{0,1\}^8$



$(x+y) \rightarrow 0..510$

if $x+y > 255$

else $c=1$

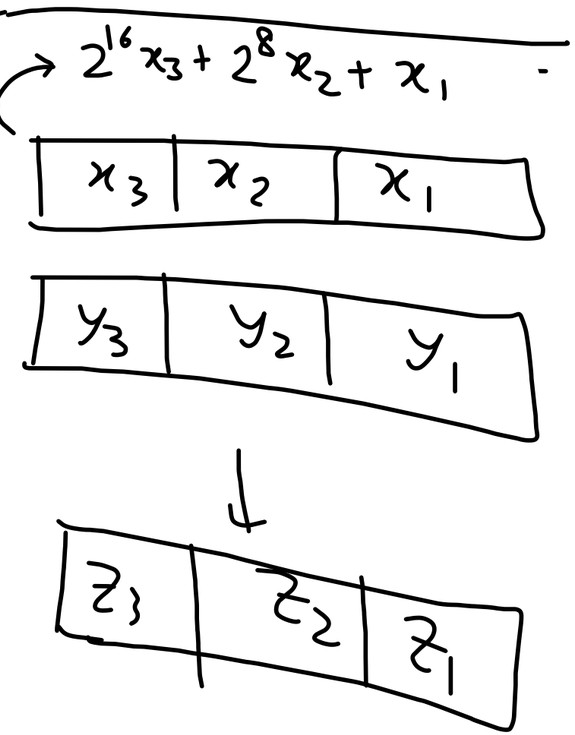
$c=0$

$2^{16}x_3 + 2^8 x_2 + x_1$

$+ 2^{16}y_3 + 2^8 y_2 + y_1$

$= (2^{16}z_3 + 2^8 z_2 + z_1) \bmod 2^{24}$

Guess $s_1 \rightarrow 2^{16}$



1001

↓

9

1001 1001

↓

128+25=153

144 + 9

↓

24 · 9

RC4 (Mantin-Shamir Bias)

$E \rightarrow 2^{nd}$ byte $\rightarrow 0$

$$Pr[Z_2 = 0] = Pr[Z_2 = 0 \mid \bar{P}] \cdot Pr[\bar{P}] + Pr[Z_2 = 0 \mid P] \cdot Pr[P]$$

$$= 1 \cdot \frac{1}{256} + \frac{1}{256} \cdot \frac{255}{256}$$

$$\simeq \frac{2}{256}$$

Boneh-Shoup