Stream Ciphers.

$E_{K,i}$ — characters from an alphabet

pl.-text $m = m_1 m_2 \dots m_N$

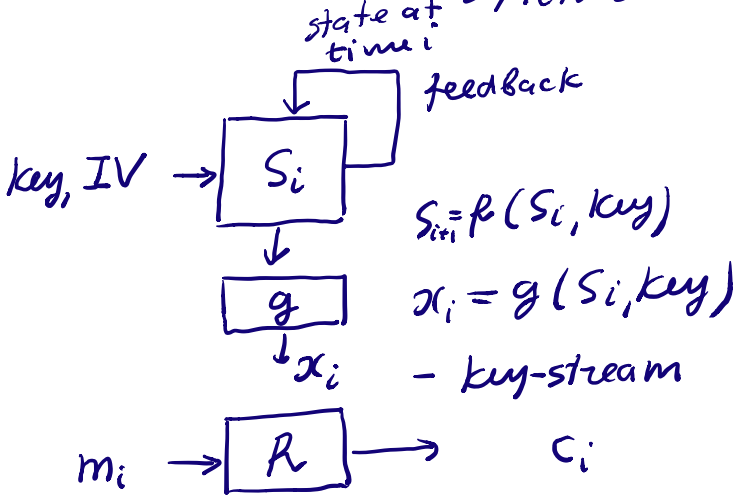
cipher-text $c = E_{K,1}(m_1), E_{K,2}(m_2), \dots, E_{K,N}(m_N)$

Block cipher is a particula case $E_{K,i} = E_K$

Two types of stream ciphers

1) synchronous 2) self-synchronizing

Synchronous (Hagelin type)



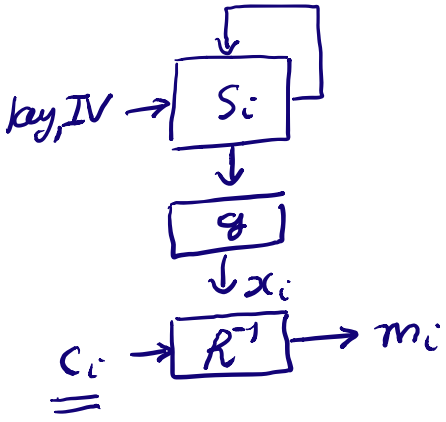
$S_{i+1} = f(S_i, key)$

$x_i = g(S_i, key)$

x_i - key-stream

$c_i = R(m_i, x_i)$

at the sender



$m_i = R^{-1}(c_i, x_i)$

in Hagelin $c_i \equiv x_i - m_i \bmod 26$

at the receiver.

1) the devices have to be synchronized.

2) if c_i was altered then only m_i won't be decrypted properly.

3) if c_i was deleted during transmission (inserted) then all next cipher-text won't be properly decrypted $\Rightarrow$ synchronization is lost.

4) IV initial value, like message key

IV sent before the cipher-text as a prefix.

5) initialization

a) key, IV are introduced into the device

b) the cipher clocks a number of times without generating key-stream.

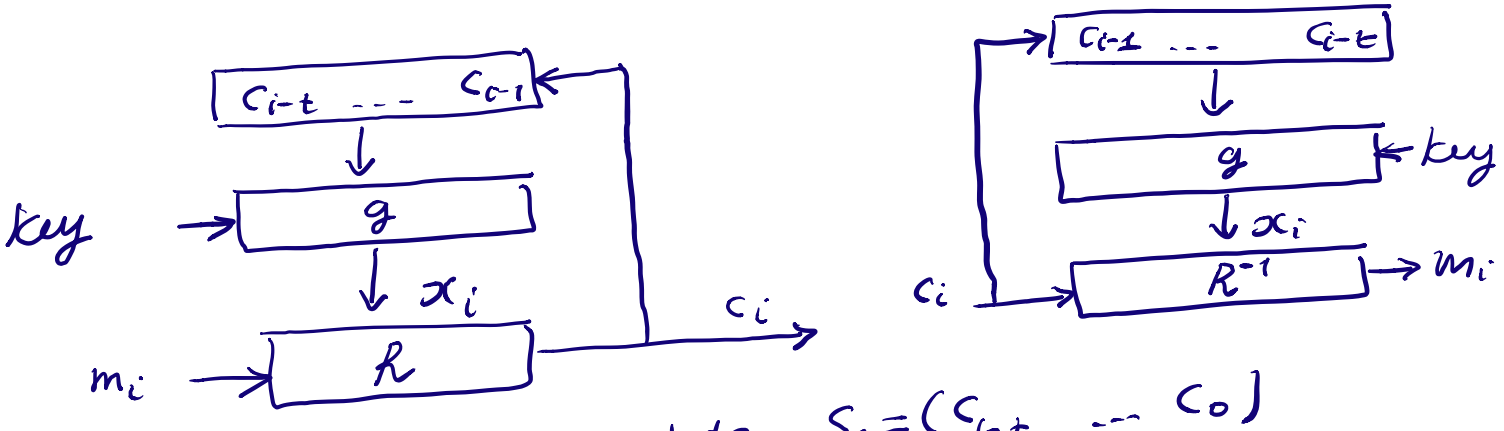
c) the cipher clocks and generates the key-stream, encrypts data.

goal: every bit of the states S_i depends on every bit of the key and of the IV.

Self-Synchronizing.

state $S_i = (c_{i-t}\ c_{i-t+1} \cdots c_{i-1})$

↑ cipher-text characters.



IV may be initial state $S_t = (c_{t-t} \cdots c_0)$

at the sender at the receiver

if c_i was altered (deleted, inserted) then next t cipher-text characters won't be decrypted properly

But after that decryption works again.

Block ciphers

E_K : block of bits (128) $\rightarrow$ block of bits (128)

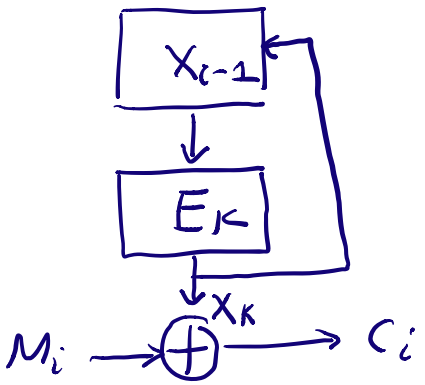
e.g. AES-128

OFB (Output FeedBack)

$X_0 = E_K(IV)$

$X_i = E_K(X_{i-1})$, $i = 1, 2, \ldots$ key-stream

$C_i = M_i \oplus X_i$

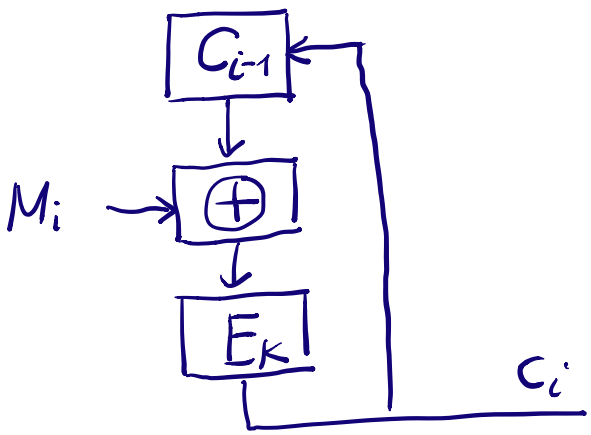


synchronous stream cipher

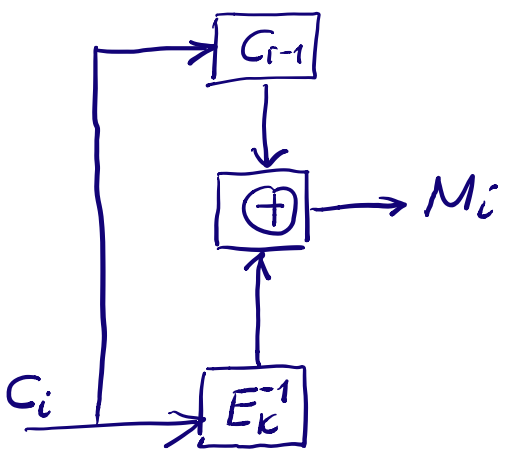
CBC (Cipher Block Chaining)

$C_0 = IV$

$C_i = E_K(C_{i-1} \oplus M_i)$, $i = 1, 2, \ldots$



self-synchronizing stream cipher at the sender



at the receiver

Linear Feedback Shift Registers (LFSR)

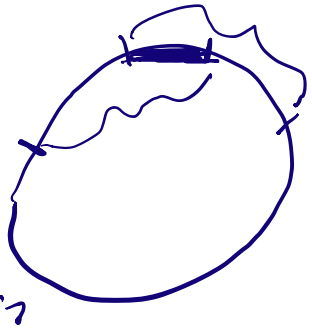
long period sequences

period of the key-stream in Hagelin (M-209)

$26 \cdot 25 \cdot 23 \cdot 21 \cdot 19 \cdot 17 \approx 10^8$

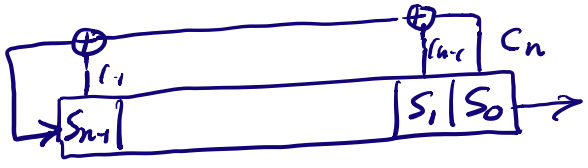
$\Rightarrow$

at-depth-cryptanalysis



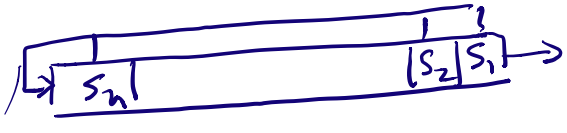
$(C_1 \dots C_{n-1} C_n)$ string of bits

$(S_{n-1} \dots S_1 S_0)$ initial state



register with n cells

$$S_n = C_1 \cdot S_{n-1} \oplus \dots \oplus C_{n-1} S_1 \oplus C_n \cdot S_0$$



....

this generates a sequence of bits

$S_0 S_1 \dots S_{n-2} S_n S_{n+1} \dots$

characteristic polynomial

$$P(x) = X^n + C_1 \cdot X^{n-1} + \dots + C_{n-1} X + C_n \in F_2[X]$$

$F_2[X]$: ring of polynomials over Binary field $F_2 = \{0,1\}$

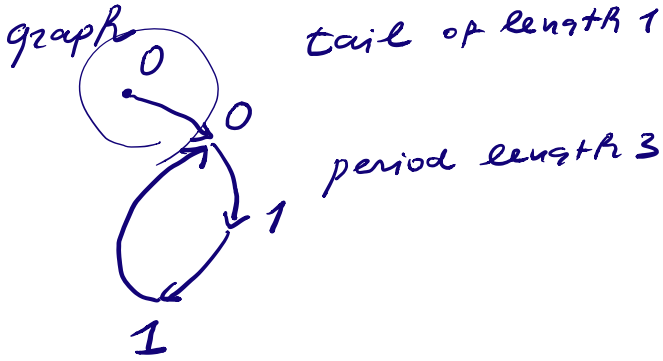
generating polynomial.

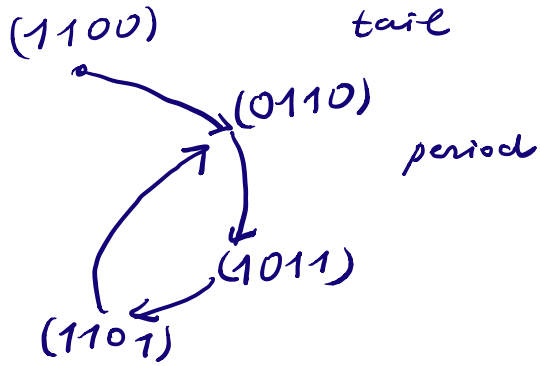
Problem: How to choose $c_1 c_2 \dots c_n$ to provide a sequence of a long period

if $c_n = 1$ LFSR is called non-singular
0 singular

Example. $X^4 + t_1 X^3 + t_2 X^2 + 0X + 0 \Rightarrow$ LFSR is singular

states	bits
1 1 0 0	0
0 1 1 0	0
1 0 1 1	1
1 1 0 1	1
0 1 1 0	0
1 0 1 1	1
1 1 0 1	1
...	





graph for bits ≡ graph for states.

Lemma 1. $\overbrace{s_0 \dots s_{\ell-1}}^{\text{tail}} \overbrace{s_\ell \dots s_{\ell+t-1}}^{\text{period}} \overbrace{s_{\ell+t} \dots s_{\ell+2t-1}}^{\text{period}} \dots$

Bits from LFSR with min. length tail ℓ, min. period t

$\overbrace{s_0 \dots s_{\ell_1-1}}^{\text{tail}} \overbrace{s_{\ell_1} \dots s_{\ell_1+t_1-1}}^{\text{period}} \overbrace{s_{\ell_1+t_1} \dots s_{\ell_1+2t_1-1}}^{} \dots$

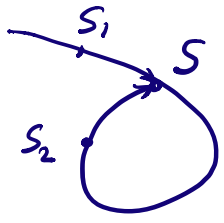
states from LFSR, min. length tail ℓ_1, min. period t_1

$\Rightarrow \quad \ell = \ell_1$ and $t = t_1$

Lemma 2. 1) aperiodic sequence is generated by an LFSR $\Rightarrow$ LFSR is singular.

2) LFSR is singular, then for some initial state the sequence is aperiodic.

Proof. 1)



$S_1 \to S$ collision

$S_2 \to S$

$S_1 = (S_{n-1} \dots S_1 S_0) \to S = (S_n S_{n-1} \dots S_1)$

$S_2 = (S_{n-1} \dots S_1 \overline{S_0})$

$\overline{S_0} = S_0 \oplus 1 = S_0 + 1 \bmod 2$.

$$\begin{cases} S_n = c_1 \cdot S_{n-1} + \dots + c_{n-1} S_1 + c_n \cdot S_0 \\ S_n = c_1 \cdot S_{n-1} + \dots + c_{n-1} S_1 + c_n \cdot \overline{S_0} \end{cases}$$

$\Rightarrow c_n \cdot S_0 = c_n \cdot \overline{S_0} = c_n S_0 + c_n \Rightarrow c_n = 0 \Rightarrow$ LFSR singular

2) assume LFSR singular $\Rightarrow c_n = 0$

two states $(0 \dots 00) \to (0 \dots 00)$

$(0 \dots 01)$

graph

sequence of bits is aperiodic

$1\overline{00}\dots0\dots$

$\Rightarrow c_n = 1$ for getting more periodic sequence from LFSR.

LFSR implement a ... states.

$$f(x) = X^n + c_1 X^{n-1} + \cdots + c_n$$

$$(s_{j+n-1} \cdots s_{j+1} s_j) \begin{pmatrix} c_1 & 1 & & 0 \\ \vdots & & \ddots & \\ c_{n-1} & & & 1 \\ c_n & 0 & & \end{pmatrix} = (s_{j+n} s_{j+n-1} \cdots s_{j+1})$$

$(s_{j+n-1} \cdots s_{j+1} s_j)$ ↑ LFSR state at time j, s_j

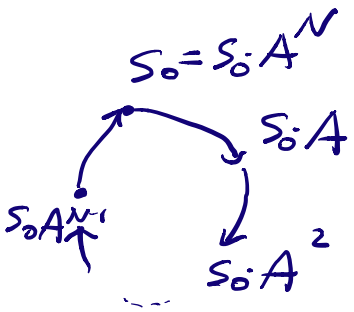
$(s_{j+n} s_{j+n-1} \cdots s_{j+1})$ ↑ s_{j+1}

↑ A companion matrix for $f(x)$.

$s_0 = (s_{n-1} \cdots s_1 s_0$ | initial state

$s_0 s_1 \cdots s_{n-1} \cdots$ pure periodic of period N

$\Leftrightarrow \quad s_0 A^N = s_0$



Recollect some linear algebra (mod 2)

$a + b \bmod 2 \equiv a - b$

1. A $n \times n$ matrix mod 2

characteristic polyn. of A

$$f_A(x) = \det(X \cdot I + A) = X^n + c_1 X^{n-1} + \cdots + c_n$$

↑ unity $n \times n$ matrix $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

Property: $f_A(A) = A^n + c_1 A^{n-1} + \cdots + c_n \cdot I = 0\text{-matrix}$.

If A is a companion matrix for $f(x) = X^n + c_1 X^{n-1} + \cdots$ then $f_A(x) = f(x)$.

2. minimal polynomial for A.

$m_A(x)$ non-zero polynomial of smallest degree s.t. $m_A(A) = 0$-matrix.

Property: if $g(x) \neq 0$ polynomial and $g(A) = 0$-matrix, then $m_A(x) \mid g(x)$.

3. z any non-zero vector of const$\mathbb{R}^n$.

minimal polyn. of z in respect with A.

$m_{z,A}(x)$ non-zero polyn. of smallest degree s.t.

$$z \cdot \underbrace{m_{z,A}(A)}_{\text{matrix}} = 0\text{-vector}.$$

z: vector

Property: $g(x) \neq 0$ polyn. s.t. $z \cdot g(A) = 0$-vector. Then $m_{z,A}(x) \mid g(x)$.

$$\Rightarrow \quad m_{z,A}(x) \mid m_A(x) \mid f_A(x).$$

Example. $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

char. polynomial

$$f_A = \det\left(x\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = \det\begin{pmatrix} x+1 & 0 \\ 1 & x+1 \end{pmatrix} =$$

$$= (x+1)^2$$

$\ldots \mid (x+1)^2 \Rightarrow m_A(x) = 1, x+1, (x+1)^2$

min. polyn. $m_A(x) \mid (x+1)^2$ ⇒ $m_A(x) = (x+1)^2$ (eliminate)

vector $z = (1,0)$, $m_{z,A}(x) = x+1$

really, $(1,0)\left(\begin{pmatrix}1&0\\1&1\end{pmatrix} + \begin{pmatrix}1&0\\0&1\end{pmatrix}\right) = (1,0)\begin{pmatrix}0&0\\1&0\end{pmatrix} = (0,0)$

Definitions from Polynomial Algebra (mod 2)

1) $f(x)$ polynomial of degree ≥ 1
reducible if $f(x) = f_1(x) \cdot f_2(x)$
$\deg f_1, \deg f_2 < \deg f$.
if impossible
$f(x)$ called irreducible.

e.g. $x^2+1 = (x+1)(x+1) = x^2+2x+1 = x^2+1$ (mod 2)
↑ reducible.

x^2+x+1 irreducible.

2) $f(x) \neq x$ irreducible, then smallest N s.t. $f(x) \mid x^N+1$ is called period of $f(x)$.

Periods of irreducible polynomials

irred. polyn. of deg ≥ 1	period
$x+1$	1
x^2+x+1	3
x^3+x+1	7
x^3+x^2+1	7

$x+1 \mid x^1+1$
$x^2+x+1 \mid x^3+1$
$(x+1)(x^2+x+1)$

$x^5+x^3+x^2+x+1$	5
x^4+x+1	15
x^4+x^3+1	15
- - -	