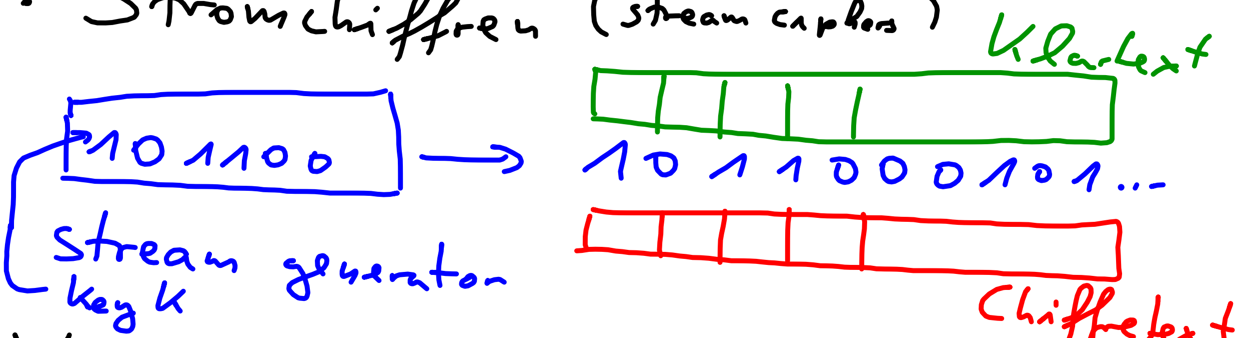
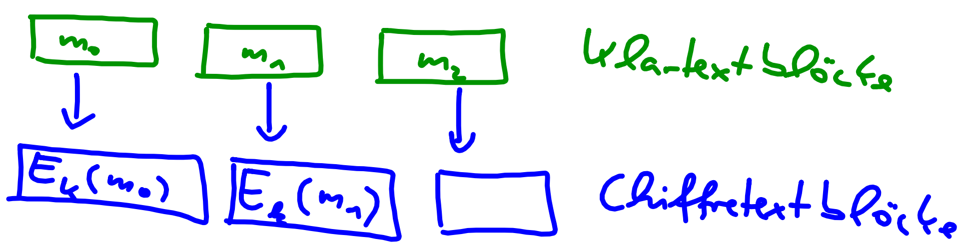
Symmetrische Verfahren

- Stromchiffren (stream ciphers)



Vorlage: One-time-pad (1949, Shannon)
falls zufällig → absolut sicher

- Blockchiffren (block ciphers)



Stromchiffren

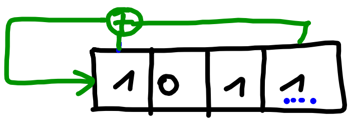
RC4 einer der ersten Vertreter, aber gebrochen

heute: ESTREAM-Wettbewerb

Finalisten, u.a. Trivium, Grain v1

Grundlage:

LFSR = linear feedback shift register



1 1 0 1 0 1 1 0
0 1 0 0 0 1 1 1

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

0	1	0	1
1	0	1	0
1	1	0	1
0	1	1	0
0	0	1	1
1	0	0	1
0	1	0	0
0	0	1	0
0	0	0	1
1	0	0	0
1	1	0	0
1	1	1	0
1	1	1	1
0	1	1	1
1	0	1	1

15 Bits

"Zufallsfolge"

$a \oplus b = b \oplus a$

$a \oplus a = 0$

(Verschlüsseln:

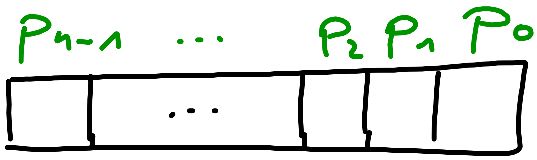
$a \oplus k = c$

$(a \oplus k) \oplus k = a$)

Bemerkung: bei einem n-Bit LFSR sind

$2^n - 1$ Bits als Periode maximal

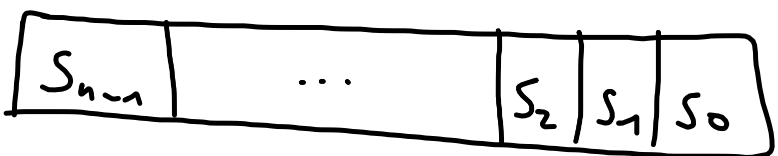
Wann Periode maximal?



n-Bit LFSR

$$p_i = \begin{cases} 0 & \text{Bit } i \text{ wird nicht verknüpft} \\ 1 & \text{Bit } i \text{ wird verknüpft} \end{cases}$$

Startzustand des LFSR:



Iterationsformel:

$s_n = p_{n-1} \cdot s_{n-1} \oplus \ldots \oplus p_1 \cdot s_1 \oplus p_0 \cdot s_0$ für das erste neue Bit

$$s_i = p_{n-1} \cdot s_{i-1} \oplus p_{n-2} \cdot s_{i-2} \oplus \ldots \oplus p_1 \cdot s_{i-(n-1)} \oplus p_0 \cdot s_{i-n}$$

Polynom:

$$P(x) = x^n \oplus p_{n-1} \cdot x^{n-1} \oplus p_{n-2} x^{n-2} \oplus \ldots \oplus p_1 x \oplus p_0$$

dieses Polynom entscheidet über Periodenlänge

Eigenschaften von $P(X)$

$$P(X) = X^n + p_{n-1} X^{n-1} + p_{n-2} X^{n-2} + \dots + p_1 X + p_0$$

(ab hier $+ = \oplus$)

- irreduzibel
- primitiv

} max. Periodenlänge des LFSR

irreduzibel

Polynom nicht weiter in (echte) Faktoren zerlegbar

Beispiel:
$$X^2 + 1 = (x+1) \cdot (x+1)$$
$$= x^2 + \underbrace{x + x}_{0} + 1$$

Nullstellen $\hat{=}$ Linearfaktoren
(dies funktioniert bis Grad 3 auf jeden Fall)

primitiv

$X \bmod P(X)$ hat maximale Ordnung $2^n - 1$

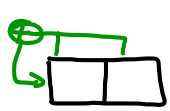
Beispiel:
$$P(X) = X^2 + X + 1 \quad \text{(irreduzibel)}$$

$$X^1 \bmod (X^2+X+1) \neq 1$$

$$X^2 \bmod (X^2+X+1) = X+1 \neq 1$$

$$X^3 \bmod (x^2+X+1) = X \cdot (X+1)$$
$$= X^2 + X = 1 \checkmark$$

Ordnung 3

$\Rightarrow P(x) = x^2 + x + 1$ ist primitiv $\longrightarrow$  hat Periode 3