1) Linearni rekurzivni šifri (LFSR) sta podani z rekurzivnima enačbama. Za vsako od šifer poiščite periode za vsakega od začetnih ključev.

a) $z_{i+4} = z_i + z_{i+1} + z_{i+2} + z_{i+3} \mod 2$

0000 0000... perioda 1

0001 10001100... perioda 5
0011 perioda 5
0110 perioda 5
1100 perioda 5
1000 perioda 5

0010 10010100... perioda 5
0101 perioda 5
1010 perioda 5
1001 perioda 5

1111 01111011... perioda 5
1110 perioda 5
1101 perioda 5
1011 perioda 5
0111

b) $z_{i+3} = z_i + z_{i+1} + z_{i+2} \mod 2$

000 000... perioda 1

001 10011001... perioda 4
011
110
100

101 010101... perioda 2
010

111 111... perioda 1

LFSR lahko priredimo polinom:

$z_{i+n} = c_1 z_{i+n-1} + c_2 z_{i+n-2} + \dots + c_n z_i \mod d$

$\rightsquigarrow c(x) = 1 + \sum_{i=1}^{n} c_i x^i \mod d$

Red LFSR:

Najmanjši t, da $c(x)$ deli $1 - x^t$:

---

2) Linearnima rekurzivnima šiframa iz naloge (1) priredite ustrezna polinoma. Preverite, ali sta nerazcepna in izračunajte njun red.

a) $c_1 = c_2 = c_3 = c_4 = 1$

$\Rightarrow c(x) = 1 + x + x^2 + x^3 + x^4 \mod 2$

Denimo: $c(x) = (x - a)(x^3 + \dots)$

$a=0: \quad c(0)=1\neq 0$
$a=1: \quad c(1)=1\neq 0$

$\Rightarrow$ $c(x)$ nima linearnih faktorjev

Denimo: $c(x)=(ax^2+bx+c)(dx^2+ex+f)$

$a=d=1$
$c=f=1$

$x^4+x^3+x^2+x+1=(x^2+bx+1)(x^2+cx+1)=x^4+(b+e)x^3+bex^2+(b+e)x+1$

$b+e=1$
$be=1$

Ni rešljivo nad $\mathbb{Z}_2$

$\Rightarrow$ $c(x)$ nima kvadratnih faktorjev

$\Rightarrow$ $c(x)$ neraszcepen

Red:

$1-x^5=(1-x)(1+x+x^2+x^3+x^4)$

$\Rightarrow t=5$

b) $c_1=c_2=c_3=1$

$\Rightarrow c(x) = 1+x+x^2+x^3$

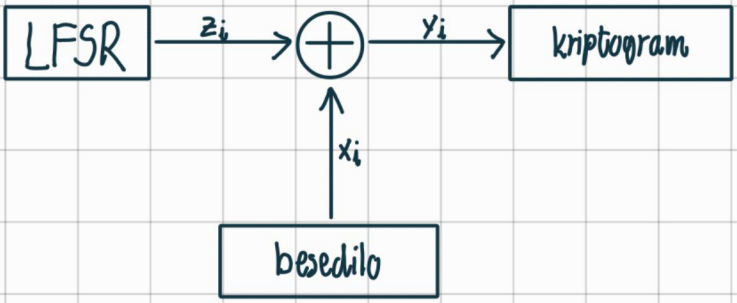
$c(x) = (1+x)(1+x^2)$

$\Rightarrow c(x)$ razcepen

Red:

$1-x^4 = (1-x)(1+x+x^2+x^3)$

$\Rightarrow t = 4$



$z_{i+m} = c_1 z_{i+m-1} + c_2 z_{i+m-2} + \dots + c_m z_i \mod d$

Matrična oblika:

$$\begin{bmatrix} z_{m+1} \\ z_{m+2} \\ \vdots \\ z_{m+m} \end{bmatrix} = \begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & & & \vdots \\ z_m & z_{m+1} & \cdots & z_{m+m} \end{bmatrix} \begin{bmatrix} c_m \\ c_{m-1} \\ \vdots \\ c_1 \end{bmatrix}$$

$z_i = x_i + y_i \mod d$

---

3) Prestregli smo kriptogram $y = 01000100$ in uganili, da je ustrezno besedilo $x = 1011010$. Vemo, da je bilo besedilo zašifrirano z LFSR. Izračunajte koeficiente ustrezne enačbe.

Opazimo: $m \leq 4$

$$m=4: \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_4 \\ c_3 \\ c_2 \\ c_1 \end{bmatrix}$$

$$c_4 + c_1 = 1$$
$$c_2 + c_1 = 1$$
$$c_3 + c_2 + c_1 = 1$$
$$c_4 + c_3 + c_2 + c_1 = 0$$

$$\Rightarrow c_1 = 0$$
$$c_2 = 1$$
$$c_3 = 0$$
$$c_4 = 1$$

Če se ne bi izšlo, bi postopoma poskušali za vedno manjše m.

Rešitev bo vedno enolična.

---

4) Preverite, ali je dano zaporedje generirano z LFSR reda 4:

1011010000101

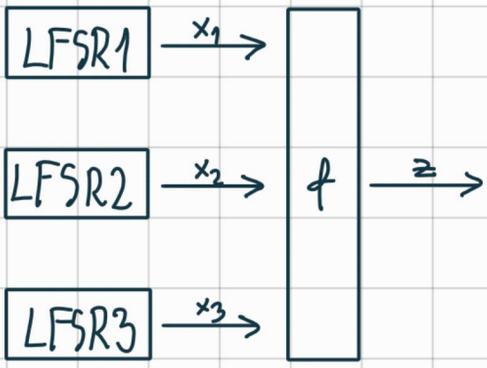
DN

GEFFEJEV GENERATOR

Geffejev generator pseudonaključnih števil je sestavljen iz treh LFSR z redi m_1, m_2 in m_3 ter periodami $2^{m_1}-1$, $2^{m_2}-1$, $2^{m_3}-1$.

Označimo izhodne bite posameznih registrov z X_1, X_2 in X_3.

Potem je izhodni bit generatorja $z = X_1 \cdot X_2 + X_2 \cdot X_3 + X_3 \bmod 2$.



---

5) Obravnavajte Geffejev generator.

a) Pokažite, da se izhoda LFSR1 in LFSR3 ujemata z izhodom Geffejevega generatorja v približno $\frac{3}{4}$ primerov, medtem ko se izhod LFSR2 ujema z izhodom Geffejevega generatorja v približno $\frac{1}{2}$ primerov.

b) S pomočjo ugotovitve iz (a) sestavite napad na Geffejev generator, ki najde začetne ključe vseh treh LFSR v času $O(2^{m_1} + 2^{m_2} + 2^{m_3})$.

a)

X_1	X_2	X_3	z
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

LFSR1: $\frac{6}{8} = \frac{3}{4}$

LFSR2: $\frac{4}{8} = \frac{1}{2}$

LFSR3: $\frac{6}{8} = \frac{3}{4}$

b) Napademo vsak LFSR posebej:

Napad na LFSR1:

for $i = 1, \ldots, (2^{m_1} - 1)$:

$X_i = LFSR1(i)$

če se X_i ujema z Z v $\frac{3}{4}$ primerov, shrani i

Napad na LFSR3:

for $j = 1, \ldots, (2^{m_3} - 1)$:

$X_j = LFSR3(j)$

če se X_j ujema z Z v $\frac{3}{4}$ primerov, shrani j

Napad na LFSR2:

for $k = 1, \ldots, (2^{m_2} - 1)$:

$y = GEFFE(i, j, k)$

če se y ujema z Z, shrani k

$\Rightarrow$ Ključ je (i, j, k)

$\sim O(2^{m_1} + 2^{m_2} + 2^{m_3})$