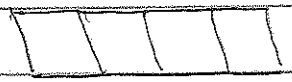
LFSR

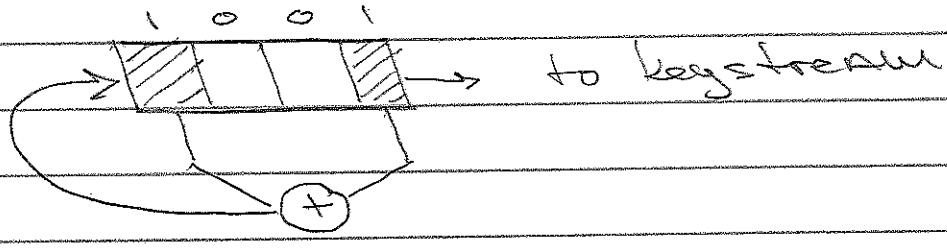
4-cell register



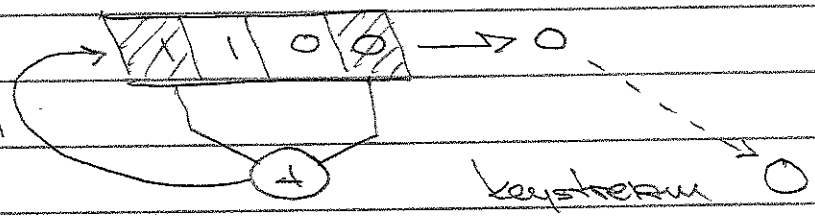
4-bit seed

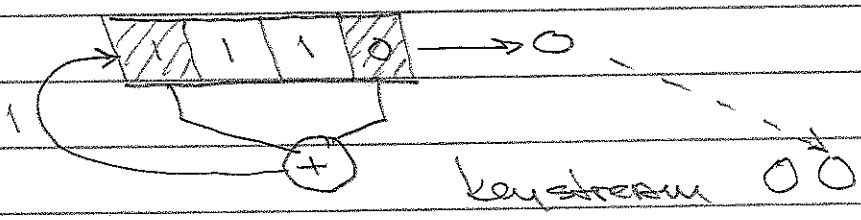
max period $= 2^4 - 1 = 15$

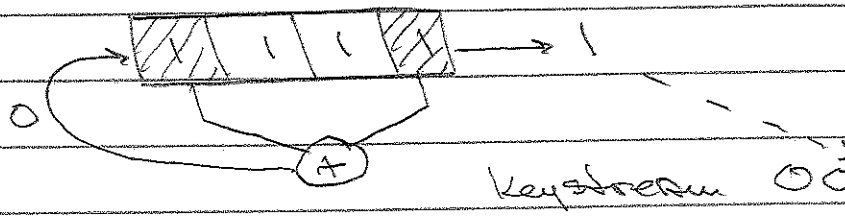
taps 9 1001

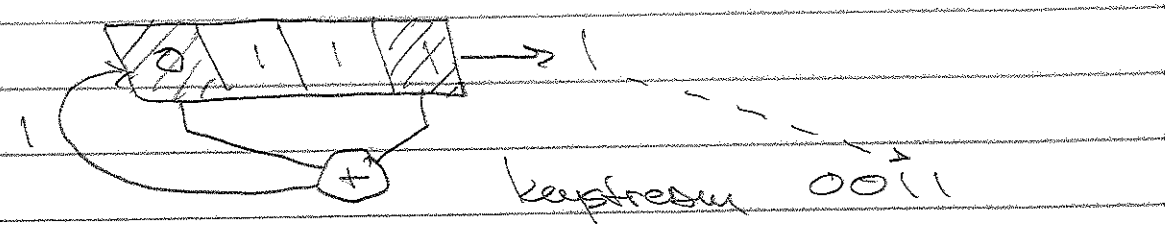


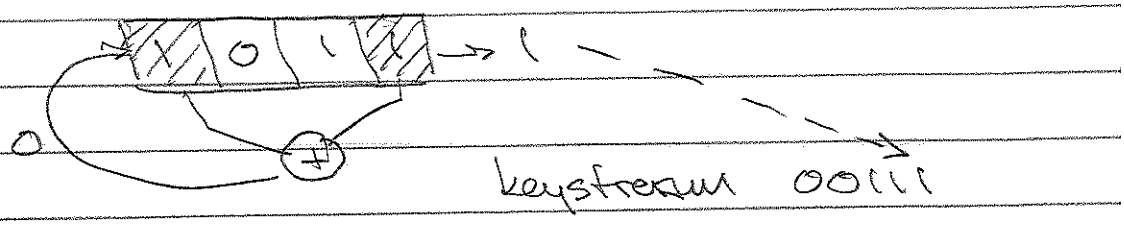
seed C 1100

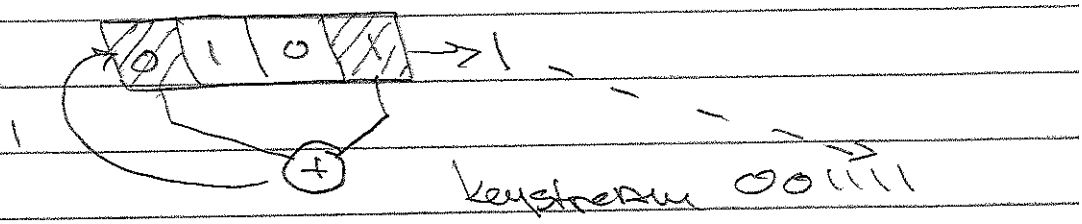


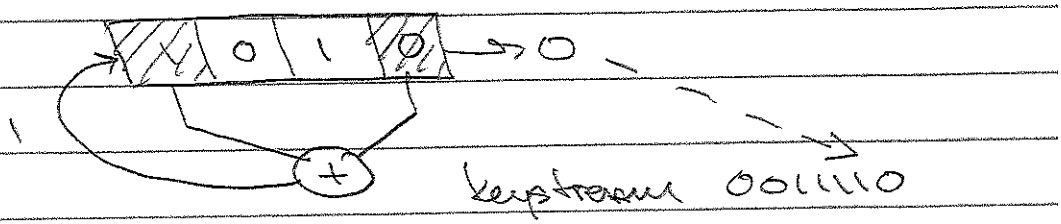


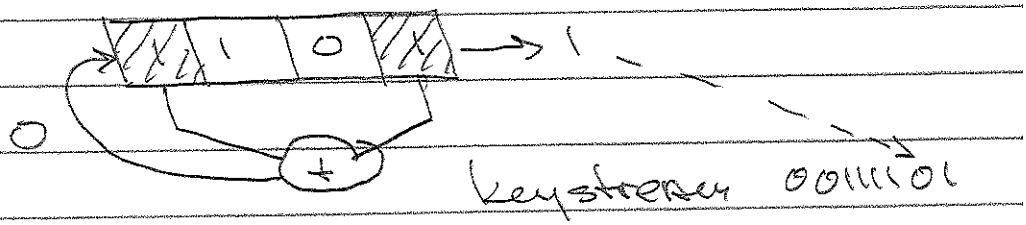


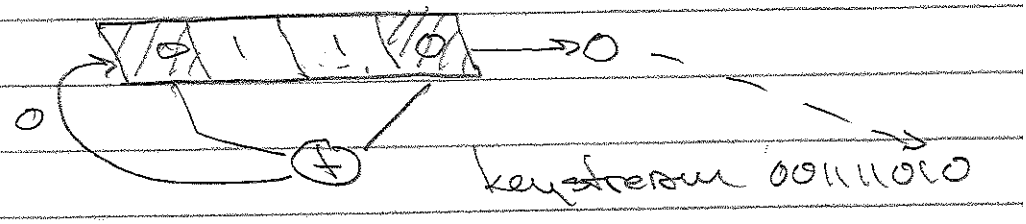

0 1 1
1
keystream 0011

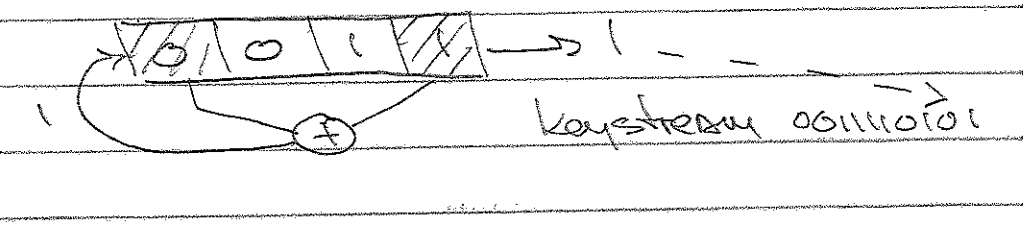

1 0 1
0
keystream 00111

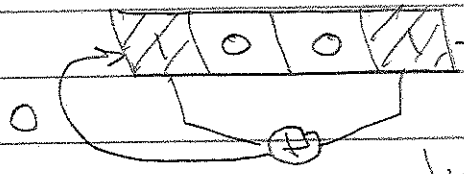

1 1 0
1
keystream 001111


0 1 0
1
keystream 0011110

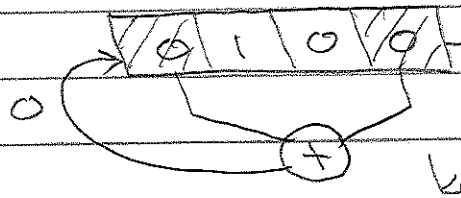

1 0
0
keystream 00111101


0 1 1 0
0
keystream 001111010

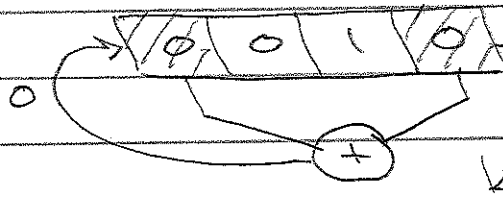

0 0 1
1
keystream 0011110101



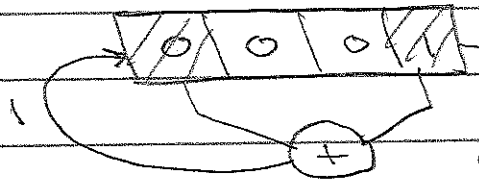
keystream 00111101011



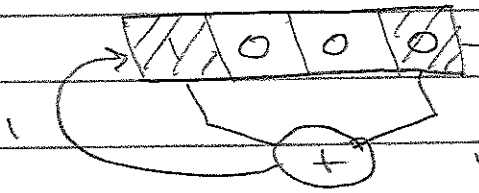
keystream 00111101011 0



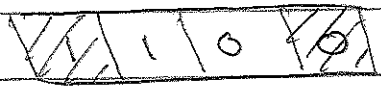
keystream 001111010110 0



keystream 0011110101100 1



keystream 00111101011000 0



repeats

keystream 00111101011000

MAX period

known pt attack

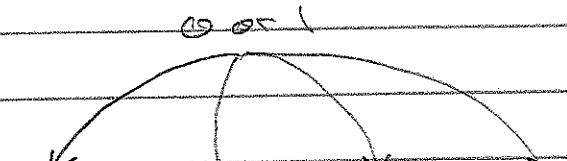
4-bit register

keystream ... 11101011 ...

8 bits

LFSR

linear function



$f(b_4, b_3, b_2, b_1) = a_3 b_4 \oplus a_2 b_3 \oplus a_1 b_2 \oplus a_0 b_1$

1 1 1 0 1 0 1 1

$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$

$f(0,1,1,1) =$ ($b_4\ b_3\ b_2\ b_1$)

$a_2 \oplus a_1 \oplus a_0 = 1$ $\quad b_5$

$a_3 \quad a_1 \oplus a_0 = 0$ $\quad b_6$

etc. $\quad a_2 \quad \oplus a_0 = 1$ $\quad b_7$

$a_3 \quad \oplus a_1 = 1$ $\quad b_8$

solve

$$\begin{cases} a_2 \oplus a_1 \oplus a_0 = 1 \\ a_3 \oplus a_1 \oplus a_0 = 0 \\ a_2 + a_0 = 1 \\ a_3 \oplus a_1 = 1 \end{cases}$$

$a_3 \oplus a_1 \oplus a_0 = 0$

$a_2 \oplus a_1 \oplus a_0 = 1$

$a_2 \oplus a_0 = 1$

$a_3 \oplus a_1 = 1$

$a_3 \oplus a_1 \oplus a_0 = 0$

$a_2 \oplus a_1 \oplus a_0 = 1$

$a_2 \oplus a_0 = 1$

$a_0 = 1$

$a_3 \oplus a_1 \oplus a_0 = 0$

$a_1 = 0$

$a_2 \oplus a_0 = 1$

$a_0 = 1$

$a_3 \oplus a_1 \oplus a_0 = 0$

$a_1 = 0$

$a_2 = 0$

$a_0 = 1$

$a_3 = 1$

$a_1 = 0$

$a_2 = 0$

$a_0 = 1$

$f(b_4, b_3, b_2, b_1) = b_4 \oplus b_1$