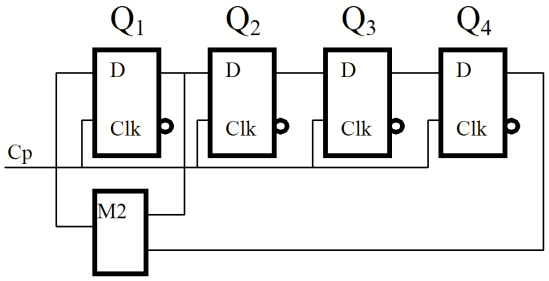
POLITECHNIKA BIAŁOSTOCKA
WYDZIAŁ INFORMATYKI
Bezpieczeństwo sieci komputerowych

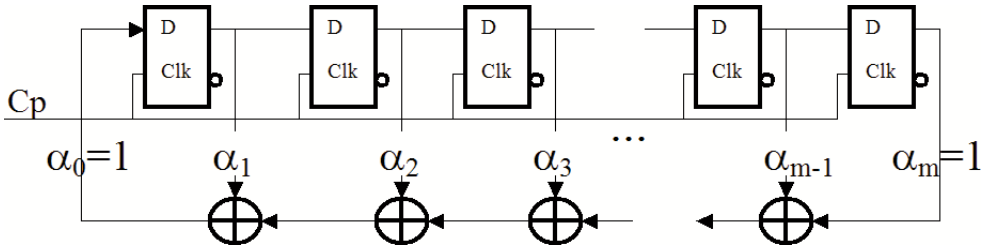
PRACOWNIA SPECJALISTYCZNA 4
MGR INŻ. MACIEJ BRZOZOWSKI

TEMAT: GENERATORY LICZB PSEUDOLOSOWYCH. SZYFRY STRUMIENIOWE.

Przykład 1. Linear Feedback Shift Register (LFSR)

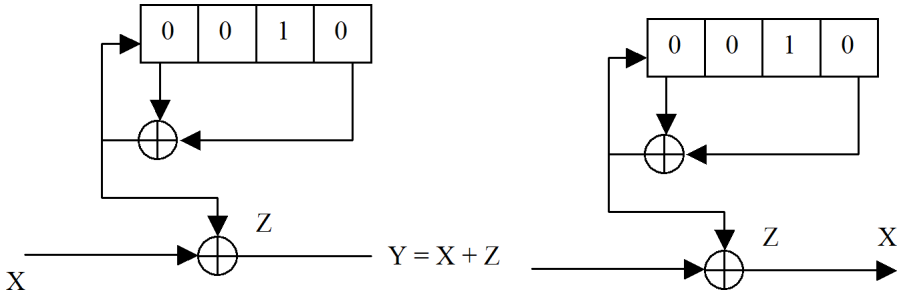


Rysunek 1: Generator LFSR wielomianu $\phi_{(x)} = 1 + x + x^4$



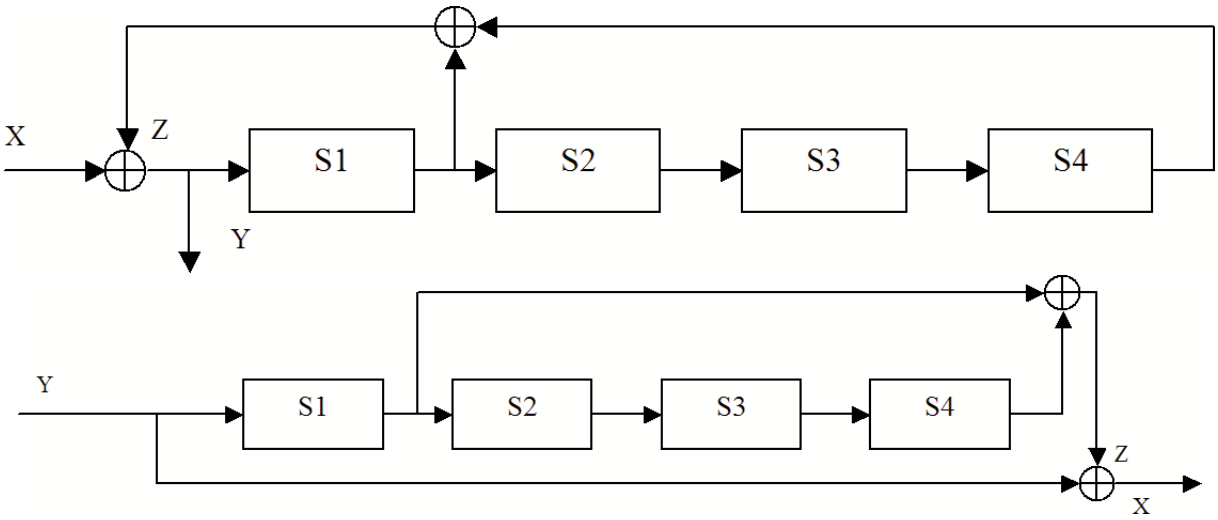
Rysunek 2: Generator LFSR wielomianu $\phi_{(x)} = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$ gdzie $a_i = \{0, 1\}$

Przykład 2. Synchronous Stream Cipher



Rysunek 3: Synchronous Stream Cipher

Przykład 3. Ciphertext Autokey



Rysunek 4: Ciphertext Autokey

Zadania:

1. Zaimplementuj generator liczb pseudolosowych bazujący na LFSR o zadanym stopniu wielomianu.
2. Zaimplementuj kryptosystem bazujący na schemacie *Synchronous Stream Cipher* dla podanego wielomianu i ziarna.
3. Zaimplementuj kryptosystem bazujący na schemacie *Ciphertext Autokey* dla podanego wielomianu i ziarna.