**Лабораторна робота №4**

**Потоковий шифр на основі генератора BBS.**

**Моделювання роботи n розрядного лінійного регістра зсуву зі зворотним зв'язком.**

Лабораторна робота містить два завдання. Перше завдання не має варіантів, друге завдання – вибираємо варіант відповідно до порядкового номера студента у списку групи.

**Потоковий шифр на основі генератора BBS**

1. Створити програму, яка реалізовує потоковий шифр на основі генератора BBS.
2. Згенерувати два великих простих числа p, q, обчислити модуль n та випадкове число x.
3. За допомогою створеної програми зашифрувати та розшифрувати повідомлення.

**Моделювання роботи n розрядного лінійного регістра зсуву зі зворотним зв'язком**

1. Створити функцію генерування ключів шифру за допомогою n-розрядного регістра зсуву зі зворотним зв'язком (значення n залежить від степеня багаточлена, вказаного у варіанті). Послідовність роботи регістра зсуву зі зворотним зв'язком у вигляді таблиці див. (лекція 8 слайд 9)
2. Реалізувати шифрування та розшифрування на заданому ключі відкритого тексту з алфавіту Z2.



