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 текстове 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 Z_2.

№	Скремблер
1	$x^8+x^4+x^3+x^2+1$
2	$x^8+x^5+x^3+x^2+1$
3	x^9+x^4+1
4	x^9+x^3+1
5	$x^{10}+x^3+1$
6	$x^{10}+x^7+1$
7	x^5+x^2+1
8	x^5+x^4+x+1
9	$x^{11}+x^2+1$
10	$x^{11}+x^5+x^2+1$
11	x^7+x+1
12	$x^7+x^5+x^2+1$
13	$x^{12}+x^6+x^4+x+1$
14	$x^{12}+1$
15	$x^8+x^4+x^3+x^2+1$
16	$x^8+x^6+x^2+1$
17	$x^{11}+x^2+1$
18	$x^{11}+x^3+x^2+1$
19	x^6+x+1
20	x^6+x^5+x+1