Лабораторная работа 3. Шифры гаммирования.

В лабораторной работе необходимо:

- зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2. При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования;

- сгенерировать гамму с помощью регистра сдвига с линейной обратной связью (принять полином $x^8 + x^4 + x^3 + x^2 + 1$) и алгоритма Блюм - Блюм - Шуба. При оформлении отчета необходимо привести расчет исходного значения и таблицы генерации гамм для 10 итераций (см. табл. 6.6 и 6.7). Исходное значение определить сложением по модулю 2 всех букв фамилии в соответствии с кодировкой Windows 1251. Например, для фамилии "АБРАМОВ" расчет исходного значения для генераторов гамм будет выглядеть следующим образом.

	1100 0000	А
	1100 0001	Б
	1101 0000	Р
$\oplus$	1100 0000	А
	1100 1100	М
	1100 1110	О
	1100 0010	В
	1101 0001	$= 209_{10}$

Контрольные вопросы

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?

2. Назовите основные характеристики гаммы.

3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.

4. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.