## Лабораторная работа №6

Тема: симметричные криптосистемы.

Цель работы: Разработать криптографическую защиту информации, содержащейся в файле данных, с помощью алгоритма шифрования, указанного в варианте. Для этого:

1. Разработать алгоритмы шифрования и дешифрования блока (потока) открытого текста заданной длины из алфавита Z*n* на заданном ключе с помощью метода, указанного в варианте (Если это позволяет алгоритм, длину блока взять кратной 8 бит).
2. Определить алфавит криптосистемы (открытого текста и шифртекста). Если алфавит не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII. Поставить символам исходного алфавита в соответствие символы из алфавита Z*n* (*n* – основание алфавита).
3. Написать программу генерации случайных ключей шифра, оценить размерность ключевого пространства.
4. Написать програму, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами.
5. Написать програму для реализации алгоритма дешифрования полученного файла шифртекста при известном ключе.
6. Провести тестирование программ

* на коротких тестовых примерах.
* на текстах в несколько страниц

*Варианты:*

1. Шифр Гронсфельда с ключевым словом
2. Алгоритм, реализующий идею «диска Альберти» для русского алфавита
3. Полибианский квадрат для русского алфавита.
4. Шифр Гронсфельда с числовым ключом
5. Шифр Кардано без поворотов.
6. Шифр гаммирования с линейным конгруэнтным генератором ключей
7. Шифр Хилла для 3-грамм
8. Шифрующие таблицы Трисемуса
9. Шифр Вернама.
10. Алгоритм, реализующий идею «диска Альберти» для английского алфавита
11. Шифр гаммирования с генератором ключей на основе датчика случайных чисел
12. Полибианский квадрат для английского алфавита.
13. Шифрующие таблицы с двойной перестановкой по ключевому слову.
14. Шифр Уинстона
15. Шифрующие таблицы с двойной перестановкой по числовому ключу.