Лабораторная работа № 1. Симметричная криптография. Стандарт шифрования ГОСТ 28147-89.

Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи стандарта шифрования ГОСТ 28147-89 в следующих режимах:

1 Простой замены;

2 Гаммирования;

3 Гаммирования с обратной связью;

4 Генерации имитовставок.

Лабораторная работа пишется на выбранном студентом языке программирования (на один язык программирования максимум 10 человек).

Варианты распределяются следующим образом:

Студент	Вариант
1	1
2	2
3	3
4	4
5	1
6	2
7	3
8	4
9	1
10	2
11	3
12	4
13	1
14	2
15	3

Студент	Вариант
16	4
17	1
18	2
19	3
20	4
21	1
22	2
23	3
24	4
25	1
26	2
27	3
28	4
29	1
30	2

Лабораторная работа № 2. Симметричная криптография. СТБ 34.101.31-2011.

Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи алгоритма СТБ 34.101.31-2011 в различных режимах работы:

1 алгоритмы шифрования в режиме простой замены;

2 алгоритмы шифрования в режиме сцепления блоков;

3 алгоритмы шифрования в режиме гаммирования с обратной связью;

4 алгоритмы шифрования в режиме счетчика.

Лабораторная работа пишется на том же языке программирования, что и первая. Варианты распределяются аналогично с первой лабораторной работой (1-1, 2-2, 3-3, 4-4, 5-1, 6-2, 7-3, 8-4, 9-1, …).

Теория:

https://apmi.bsu.by/assets/files/std/belt-spec27.pdf

Лабораторная работа № 3. Асимметричная криптография. Криптосистема Рабина.

Реализовать криптостойкое программное средство шифрования и дешифрования текстовых файлов при помощи Криптосистемы Рабина.

Лабораторная работа пишется на том же языке программирования, что и первая, у всех одно задание (за счёт этого буду спрашивать больше теории).

Лабораторная работа № 4. Асимметричная криптография. Алгоритм Мак-Элиса.

Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи алгоритма Мак-Элиса для криптостойких размеров порождающей матрицы.

Лабораторная работа пишется на том же языке программирования, что и первая, у всех одно задание (за счёт этого буду спрашивать больше теории).