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 шифр замены;

2 шифрование методом гаммирования;

3 гаммирование с обратной связью;

4 генерации имитоприставок.

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. Также необходимо добавить интерфейс командной строки, который позволит выбирать файл для шифрования/дешифрования, задавать ключи и режимы операций и предусмотреть обработку возможных ошибок (неверный формат файла, невалидный ключ, …).

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. Реализовать алгоритм для генерации криптостойких порождающих матриц. Обосновать выбор размера и характеристик матрицы.

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

Лабораторная работа № 5. Хэш-функции.

Реализовать программное средство контроля целостности сообщений с помощью вычисления хэш-функции и алгоритма ГОСТ 34.11 с графическим интерфейсом.

Лабораторная работа пишется на том же языке программирования, что и первая. Необходимо выполнить 2 реализации хэш-функций. Варианты распределяются по чётности/нечётности по номеру в списке, где

1 чётные – ГОСТ 34.11 и MD5;

2 нечётные – ГОСТ 34.11 и SHA-1.

Лабораторная работа № 6. Цифровая подпись.

Реализовать программное средство формирования и проверки ЭЦП на базе алгоритма ГОСТ 34.10. Реализовать алгоритм для генерации пары ключей (открытого и закрытого) для подписи и проверки.

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

Лабораторная работа № 7. Криптография с использованием эллиптических кривых.

Реализовать схему шифрования (дешифрования) для аналога алгоритма Эль-Гамаля на основе эллиптических кривых. Написать функцию для генерации открытого и закрытого ключей с использованием эллиптических кривых. Реализовать алгоритм для генерации параметров эллиптической кривой, включая выбор простого числа и коэффициентов.

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

Лабораторная работа № 8. Стеганографические методы.

Реализовать программное средство, сокрытия (извлечения) текстового сообщения в (из) JPEG изображение(я) на основе метода сокрытия в частотной области изображения следующими способами:

1 дискретного косинусного преобразования (ДКП);

2 быстрого преобразования Фурье (БПФ).

Лабораторная работа пишется на том же языке программирования, что и первая.

Варианты распределяются следующим образом:

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

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