При необходимости могу предоставить лекции.

Рекомендации от преподавателя:

1. Сначала Вам необходимо выполнить три лабораторных работы. Задание общее для всех. Результаты каждой лабораторной работы должны содержать файл программы и файл с результатами работы программы.

4. Номер варианта Вашего индивидуального задания контрольной работы соответствует последней цифре Вашего пароля. Результаты выполненной контрольной работы должны включать текст задания, соответствующий именно Вашему варианту, файл с текстом программы, подробное описание работы программы и результаты работы программы. Отчет с описанием работы программы должен быть в формате текстового редактора Word, размером шрифта 14 пунктов.

Программу необходимо реализовать с помощью любой среды визуального программирования под Windows. Обязательным требованием также является вывод всех промежуточных результатов, таких как матрица смежности, гамильтонов цикл, изоморфный граф, закодированная матрица, зашифрованная матрица, посылаемые вопросы и ответы Алисы и Боба.

**Лабораторная работа №1**

**Тема:** Шифры с открытым ключом (Глава 2)

**Задание:**

1.Написать и отладить набор подпрограмм (функций), реализующих алгоритмы возведения в степень по модулю, вычисление наибольшего общего делителя, вычисление инверсии по модулю.

2. Используя написанные подпрограммы, реализовать систему Диффи-Хеллмана, шифры Шамира, Эль-Гамаля и RSA, в частности:

2.1. Для системы Диффи-Хеллмана с параметрами *p* = 30803, *g* = 2, *XA* = 1000, *XB* = 2000 вычислить открытые ключи и общий секретный ключ.

2.2. Для шифра Шамира с параметрами *p* = 30803, *g* = 2, *cA* = 501, *cB* = 601 и сообщения *m* = 11111 вычислить *dA*, *dB*, *x*1, *x*2, *x*3, *x*4.

2.3. Для шифра Эль-Гамаля с параметрами *p* = 30803, *g* = 2, *c* = 500, *k* = 600 и сообщения *m* = 11111 вычислить зашифрованное сообщение.

2.4. Для шифра RSA с параметрами пользователя *P* = 131, *Q* = 227, *d* = 3 и сообщения *m* = 11111 вычислить зашифрованное сообщение.

**Лабораторная работа №2**

**Тема:**  Шифры с секретным ключом (Глава 4)

**Задание:**

Выполнить программную реализацию шифра по ГОСТ 28147-89.

Написать программу, которая, используя полученную реализацию шифра, зашифровывает сообщение в режимах ECB, CBC, OFB и CTR (сообщение, режим и ключ задаются при запуске программы).

Написать программу, которая расшифровывает ранее зашифрованное сообщение.

**Рекомендации к выполнению:**

Зашифрованное сообщение выводить в бинарный файл. Исходный файл так же имеет смысл рассматривать как бинарный.

**Лабораторная работа №3**

**Тема:**  Цифровая подпись (Глава 5)

**Задание:**

Разработать программы для генерации и проверки подписей по ГОСТ Р34.10-94. Рекомендуемые значения общих открытых параметров *q* = 787, *p* = 31481, *a* = 1928. Остальные параметры пользователей выбрать самостоятельно. Хеш-функцию реализовать на основе блокового шифра по ГОСТ 28147-89.

**Рекомендации к выполнению:**

Сообщение брать из файла. Подпись писать в файл с таким же именем, но другим расширением (например, если сообщение в файле message.doc, то подпись помещается в файл message.doc.sign). Все используемые файлы рассматривать как бинарные (т.е. как потоки произвольных байт).

**Контрольная работа**

Тема: Доказательства с нулевым знанием

Задание:

Выполнить компьютерную реализацию протокола «Задачи о нахождении гамильтонова цикла в графе», используя пример 6.2 (см. ниже).

1) Случайную нумерацию вершин, используемую в алгоритме (изначально в примере она равна 7 4 5 3 1 2 8 6), необходимо изменить по формуле ((a+Z)mod 9), где a – это цифра исходной последовательности случайных номеров вершин.

2) Необходимые в алгоритме параметры схемы RSA вычислить, используя значения P и Q по вариантам:

Для Z=0: P=11 Q=53;

П р и м е р б.2. Возьмем в качестве основного граф G, изображенный на рис. б.1. Его матрица смежности имеет вид



В матрице с помощью показан гамильтонов цикл. Алиса выбирает некоторую случайную нумерацию вершин, скажем, 7, 4, 5, 3, 1, 2, 8, б, и получает изоморфный граф



Для шифрования матрицы будем использовать систему RSA с параметрами *N = 55*, *d = 3*. Вначале закодируем матрицу *Н*. В рамках данного примера просто припишем слева к каждому элементу матрицы выбираемую случайно с равными вероятностями цифру из множества {1, 2, 3, 4, 5}:



Теперь мы шифруем матрицу , возводя каждый ее элемент в куб по модулю 55:



(При внимательном просмотре матрицы *F* может показаться, что использованный нами шифр плохо скрывает исходную матрицу *Н*. Это объясняется тем, что, во-первых, модуль 55 слишком мал и, во-вторых, в матрице много чисел, не взаимно просты с модулем. Для реальных систем RSA, где *N* большое число, такая ситуация практически исключена.)

Боб получает матрицу *F* и задает один из двух вопросов. Если он просит доказать изоморфизм графов, то Алиса просто посылает ему кодированную матрицу и использованную нумерацию 7, 4, 5, 3, 1, 2, 8, б. Боб проверяет соответствие матрицы матрице *F*, т.е.выполнение равенств *503 mod 55 = 40*, *203 mod 55 = 25* и т.д. Из матрицы Боб получает граф *Н* (просто отбросив старшую десятичную цифру). Затем он переставляет вершины графа *G* в соответствии с полученной нумерацией, как это делала Алиса, и убеждается в том, что *Н* и *G* один и тот же граф.

Если Боб просит показать ему гамильтонов цикл, то Алиса посылает ему соответствующий список (закодированных) ребер графа *Н: (1, 5, 21), (5, 7, 41), (7, б, 21), ... , (3, 1, 41)*. Каждый элемент содержит номера вершин и код ребра. Боб проверяет соответствие указанных в списке ребер матрице *F*, например, *213 mod 55 = 21 = F1,5, 413 mod 55 = 06 = F5,7* и т.д. Затем он убеждается, что указанный в списке путь проходит через все вершины графа по одному разу.