**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:** Теоретическая стойкость криптосистем (Глава 3)

**Задание:**

Пусть источник без памяти порождает буквы из алфавита {0, 1, 2, ..., 9} с вероятностями 0.4, 0.2, 0.1, 0.05, 0.05, 0.05, 0.05, 0.04, 0.03, 0.03 соответственно. Пусть используется шифр Цезаря

*e* = (*m* + *k*) mod 10

с ключом *k*, выбираемым равновероятно из этого же алфавита.

Написать программу, которая

1) вычисляет расстояние единственности для этого шифра;

2) для введенного зашифрованного сообщения (например, 3462538) вычисляет апостериорные вероятности использования различных ключей.

.

**Лабораторная работа №3**

**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 №4**

**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).

**Лабораторная работа №5**

**Тема:** Криптографические протоколы (Глава 6)

**Задание:**

Выполнить компьютерную реализацию протокола "Электронные деньги". Все необходимые параметры выбрать самостоятельно.