Лабораторная работа 2 по основам криптографии.

1. Спроектируйте и реализуйте сервис, позволяющий вычислять значения символов Лежандра и Якоби.

2. Спроектируйте интерфейс, предоставляющий описание функционала для вероятностного теста простоты (параметры метода: тестируемое значение, минимальная вероятность простоты в диапазоне [0.5, 1)). С использованием сервиса, реализованного в задании 1, реализуйте интерфейс для следующих вероятностных тестов простоты: Ферма, Соловея-Штрассена, Миллера-Рабина.

3. Спроектируйте и реализуйте сервис, предназначенный для выполнения шифрования и дешифрования данных алгоритмом RSA. Сервис должен содержать объект вложенного сервиса для генерации ключей алгоритма RSA (контракт конструктора вложенного сервиса: используемый тест простоты (задаётся перечислением), минимальная вероятность простоты в диапазоне [0.5, 1), битовая длина сгенерированных простых чисел; параметры делегируются из конструктора сервиса-обёртки). При генерации ключей обеспечьте защиту от атаки Ферма и атаки Винера. При выполнении операций шифрования обеспечьте защиту от атаки Хастада. Новую ключевую пару можно генерировать произвольное количество раз. Продемонстрируйте выполнение шифрования и дешифрования данных алгоритмом RSA посредством реализованного сервиса.

4. Реализуйте сервис, демонстрирующий выполнение атаки Винера на открытый ключ алгоритма RSA. В качестве результата выполнения

необходимо получить коллекцию подходящих дробей для цепной дроби $\frac{e}{N}$ и найденное значение дешифрующей экспоненты.