Алгоритмы факторизации чисел

**Предыстория:** Простое число – натуральное число (1,2,3,4…), которое имеет среди своих делителей (те числа, на которое исходное делится нацело) имеет только два числа - 1 и само себя (важно, что число 1 не является простым, так его делитель одно число – 1). Пример простых чисел 2,3,5,7,11… Несмотря на легкое определение, простые числа оказались сложным объектом для изучения и с ними до сих пор связано много нерешенных задач: бесконечно ли количество простых чисел близнецов? (<https://ru.wikipedia.org/wiki/Числа-близнецы)>; Верно ли, что любое четное число больше 4 можно представить в виде суммы двух простых чисел? (<https://ru.wikipedia.org/wiki/Проблема_Гольдбаха>); Бесконечно ли множество простых чисел палиндромов? (которые читаются одинаково начиная слева и справа, например 101, 10501). И в целом много других нерешенных задач. Но самое классное с точки зрения алгоритмов, что до сих пор нет подхода, который бы за разумное количество времени определял является число простым или нет(разложение числа из 200 знаков занимает 75 лет работы одного 2.2 ГГц Opteron). Эта проблема нашла свое применение в RSA-шифровании с открытым ключом, в качестве которого используется большое просто число (129 знаков и более), а в качестве дешифратора его простые делители. Даже если ключ будет перехвачен, понадобится огромное количество времени, чтобы узнать его простые делители и дешифровать информацию. За данное время транзакция будет уже закончена. В момент выпуска своего шифрования RSA Laboratories опубликовала список из 54 чисел (https://ru.wikipedia.org/wiki/RSA-числа), которые предлагалось разложить на простые множители за вознаграждение (в целях демонстрации надежности подхода). Хоть конкурс и завершился в 2007 году и вычислительные мощности значительно увеличились с того времени, к 2020 году удалось разложить лишь 22 из 54 чисел.

**Цель проекта:** разобраться в статьях умных математиков, реализовать описанные в них алгоритмы, оптимизировать их и попытаться разложить одно из чисел RSA (хотя бы RSA-100). В планах изучение алгоритмов метод квадратичного решета и общий метод решета числового поля (если получится разобраться). Пример описания одного из алгоритмов (http://www.uic.unn.ru/~zny/compalg/Lectures/ca\_10\_FactorizationSieve.pdf)

**Возможное применение:** Разработать локальный мессенджер, который будет шифровать сообщения с помощью кастомного алгоритма (с использованием не очень больших простых чисел) и пытаться эти сообщения дешифровать с помощью разработанных алгоритмов факторизации.

**Примерный план работ:**

1. Разобраться в сути алгоритмов
2. Разработать прототип
3. Оптимизировать прототип
4. Разобраться в шифровании с открытым ключом
5. Реализовать кастомный алгоритм шифрования
6. Разработать мессенджер с использованием кастомного алгоритма шифрования
7. Понять, как перехватывать отправляемые сообщения
8. Сделать «хакер-скрипт», который будет перехватывать сообщения и дешифровать их