Лабораторна робота (Основні алгоритми теорії чисел та криптографії)

Реалізувати основні алгоритми криптографії та теорії чисел:

1) Обчислення функцій Ейлера та Мьобіуса. Знаходження найменшого спільного кратного набору чисел.
2) Розв'язання системи лінійних порівнянь за модулем (китайська теорема про лишки).
3) Обчислення символів Лежандра та Якобі.
4) Один алгоритм факторизації довгих цілих чисел на вибір: ро-алгоритм Полларда або алгоритм квадратичного решета.
5) Один алгоритм знаходження дискретного логарифма на вибір: ро-алгоритм Полларда або алгоритм «великий крок – малий крок».
6) Алгоритм Чіпполи знаходження дискретного квадратного кореня.
7) Один алгоритм перевірки чисел на простоту на вибір: алгоритм Соловея-Штрассена або алгоритм Міллера-Рабіна.
8) Криптосистема RSA або криптосистема Рабіна (на вибір).
9) Криптосистема Ель-Гамаля над еліптичними кривими.

Умови:

- Алгоритми реалізувати в довгій арифметиці.
- Для перевірки тестів на простоту використовувати таблиці довгих простих чисел, наприклад: https://primes.utm.edu/nthprime/index.php#nth
- Параметри для еліптичних кривих вибирати згідно з таблицями: http://www.secg.org/SEC2-Ver-1.0.pdf