Задачи к лабораторным занятиям по дисциплине
«Криптографические методы и средства защиты информации»
VIII семестр 2023/2024 учебного года
специальность 10.05.01 Компьютерная безопасность
А. В. Жаркова

1) Длинная арифметика. Реализовать арифметические операции над длинными числами (реализация алгоритмов согласно Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы):

1) сложение;
2) вычитание;
3) умножение;
4) деление;
5) возведение в степень по модулю m.

Сравнение (по времени выполнения) реализованных операций со встроенными в выбранном языке программирования

Пример входа:	Пример выхода (+):
12 123	135

2) Реализация

I) шифрсистемы RSA (с использованием реализованного теста Миллера – Рабина);

II) шифрсистемы Эль-Гамаля (с использованием реализованного теста Соловея – Штрассена)

с использованием реализованных арифметических операций из задания 1 (шифрование сохранённого в .txt-файле сообщения и расшифрование получившейся криптограммы; подробности на занятии). (Русский алфавит, знаки препинания, цифры).

3) …

...