Задачи к лабораторным занятиям по дисциплине
«Криптографические методы и средства защиты информации»
VIII семестр 2022/2023 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. Э. Искусство программирования):

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

2) С использованием реализованных арифметических операций из задания 1 написать следующую программу.

I) Пусть p и q – простые числа, $p = qs + 1$. Написать программу нахождения элемента $g \in \mathbb{Z}_p^*$ порядка q. В стандарте DSS для поиска g указанного вида используется следующий вероятностный алгоритм:

1) выбрать случайное $a \in \{2,3, \dots p-2\}$;
2) вычислить $g := a^{\frac{p-1}{q}} (mod\ p)$;
3) если $g = 1$, то возвратиться к 1), иначе – вернуть g.

II) Написать программу генерации k-битовых простых чисел p таких, что $p-1$ имеет $\left\lfloor \frac{k}{2} \right\rfloor$-битовый простой делитель q. Алгоритм из стандарта ГОСТ Р 34.10-94, применяемый для генерации простых p указанного вида, основан на следующем утверждении:

число $p = qs + 1$ простое, если q – простое, s – чётное,

$p < (2q + 1)^2$, $2^{qs} \equiv 1(mod\ p)$ и $2^s \not\equiv 1\ (mod\ p)$.

3) Реализация

I) шифрсистемы Эль-Гамаля (с использованием реализованного теста Миллера – Рабина);

II) шифрсистемы RSA (с использованием реализованного теста Соловея – Штрассена)

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

4) …

…