Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

Кафедра «Вычислительная техника»

ОТЧЁТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №2

по дисциплине
Информационная безопасность и защита информации

Асимметричные шифры. RSA/DH

(Вариант 4)

Преподаватель _____ Д.В. Новицкий
подпись, дата — инициалы, фамилия

Студент КИ19-07Б 031619531 _____ С.В. Медведев
номер группы, зачетной книжки — подпись, дата — инициалы, фамилия

Красноярск 2022

Цель работы:

- ознакомиться с основами ассиметричной криптографии;
- ознакомиться с элементами теории чисел, используемых в криптографии с открытым ключом;
- изучить особенности алгоритма с открытым ключом RSA;
- получить навыки разработки криптосистем с открытым ключом с использованием языка программирования высокого уровня;

Задание:

Согласно Вашему персональному варианту разработайте алгоритм шифрования/расшифровывания RSA и протестируйте его. Задание по варианту: число знаков N = 38

Выполнение работы:

Для реализации работы программы языком разработки был выбран Python 3. Исходный код проекта выложен в репозиторий на GitHub: https://github.com/eazyproger/rsa

В программе используется автоматическое тестирование для тестирования работы программы.