

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

ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ
по дисциплине «Информационная безопасность и защита информации»
Асимметричные шифры
Вариант 6

Преподаватель

подпись, дата

А. А. Сидарас

инициалы, фамилия

Студент

КИ19-07Б, 031941597

номер группы, зачётной книжки

подпись, дата

А. А. Горбацевич

инициалы, фамилия

Красноярск 2021

Содержание

1 Цель работы.....	3
2 Задание.....	3
3 Выполнение работы.....	3
3.1 Описание метода шифрования.....	3
Приложение А.....	4

1 Цель работы

Освоить принципы работы асимметричного метода шифрования RSA.

2 Задание

Разработать алгоритм шифрования RSA; реализовать программу использующую данный шифр для шифрования/расшифрования данных; протестировать алгоритм.

3 Выполнение работы

3.1 Реализация метода шифрования на ЯП

Для реализации шифра была выбрана платформа Google Colab, языком разработки выбран Python 3.

Исходный код проекта выложен в репозиторий на GitHub:
<https://github.com/NuarkNoir/UPC/blob/master/4sem/isaip/02/RSA/rsaNk.ipynb>.

3.2 Тестирование

Автоматический тест и тестовые данные находятся в первой ячейке раздела «Тестирование алгоритма шифрования»

<https://github.com/NuarkNoir/UPC/blob/master/4sem/isaip/02/RSA/rsaNk.ipynb>.

Также имеется возможность ручного тестирования, при условии открытия проекта через Google Colab.