**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО**

Факультет автоматизированных и информационных систем

Кафедра «Информатика»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3

# по дисциплине «Основы защиты информации»

на тему: «**Криптографические системы с открытым ключом**»

Выполнил: студент гр. ИП-31

Суховенко Э. С.

Принял: преподаватель

Кудин В.П.

Дата сдачи отчета: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата допуска к защите: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата защиты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Гомель 2022

**Цель работы:** изучить принципы работы криптосистемы с открытым ключом на основе алгоритма RSA.

**Ход работы:**

2.1. Изучить теоретический материал по лабораторной работе.

2.2. Используя заданные в соответствии с вариантом значения p, q и закрытого ключа Kс вычислить открытый ключ Ko при помощи расширенного алгоритма Евклида и выполнить шифрование по алгоритму RSA открытым ключом (Ko) своей фамилии. Для представления букв в числовой форме использовать следующее соответствие: ‘A’ – 2, ‘Б’ – 3, ‘В’ – 4, ..., ‘Ё’ – 8, ..., ‘Я’ – 34.

2.3. Выполнить проверку правильности расшифрования полученных зашифрованных данных при помощи закрытого ключа Kс.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Й | К | Л | М | Н | О | П | Р | С | Т |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Э | Ю | Я |  |  |  |  |  |  |  |
| 32 | 33 | 34 |  |  |  |  |  |  |  |

Шифруемое слово:  
СУХОВЕНКО – 20, 22, 24, 17, 4, 7, 16, 13, 17

15

**Вариант задания:**

12. p=17, q=5, Kс=19.

**Решение:**

1. Вычислим
2. Вычислим
3. Вычислим
4. Вычислим 𝐾

*Ko* = 27.

1. Представим шифруемое сообщение как последовательность целых чисел в диапазоне 2...34

Зашифруем сообщение:

1. 20, 22, 24, 17, 4, 7, 16, 13, 17
2. 15
3. Расшифруем сообщение:

*M (2.1)= = 15*

**Вывод:** были усвоены математические основы криптографии.