**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**»

**Вариант 15**

Выполнил: студент гр. ИП-31

Коваленко А.И.

Принял: преподаватель

Кудин В.П.

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

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

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

Гомель 2023

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

**Задания:**

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):

А) числа М = 15

Б) 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.

**Вариант 15**

15. *p*=7, *q*=17, *Kс*=11.

Вычислим .

Функция Эйлера 𝜑(𝑟)= (p–1)•(q–1)=6\*16=96.

НОД(Kc, 𝜑(𝑟))=1 => взаимнопростые

Ко должен удовлетворять условию (𝐾𝑜∗𝐾𝑐)𝑚𝑜𝑑𝜑(𝑟)=1. То есть, Кo является взаимообратным по модулю 𝜑(𝑟) для Кc.

1. Вычислим 𝐾о

*Ko* = .

Таким образом, ключом шифрования является пара значений (35, 119). Ключом расшифрования является (11, 119)

Зашифруем число М = 15.

С=()𝑚𝑜𝑑 𝑟=

𝑚𝑜𝑑 119=[++]

=𝑚𝑜𝑑119=1,2,4,8,16,32… =

**Конечное вычисление:**

– зашифрованное число М.

Убедимся в правильности полученных зашифрованных данных, расшифруем их при помощи закрытого ключа Кс:

M=()𝑚𝑜𝑑 𝑟=

𝑚𝑜𝑑 119=[11=++]=𝑚𝑜𝑑119=1,2,4,8 =

**Конечное вычисление:**

– зашифрованное число М

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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:

КОВАЛЕНКО – 13 17 4 2 14 7 16 13 17

M = 15

15. *p*=7, *q*=17, *Kс*=11.

𝑟=𝑝𝑞=119.

Функция Эйлера 𝜑(𝑟)=96.

Ко = 35

**Начальный шифр: 13 17 4 2 14 7 16 13 17**

**Конечный шифр: 55 68 30 25 7 105 67 55 68**

|  |  |
| --- | --- |
| Буква | Шифровка и дешифровка |
| К (13) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119= **55** |
| Дешифровка: 𝑚𝑜𝑑 119=13 |
| О(17) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119= **68** |
| Дешифровка: 𝑚𝑜𝑑 119=77 |
| В(4) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119 = **30** |
| Дешифровка: 𝑚𝑜𝑑 119=4 |
| А(2) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119=**25** |
| Дешифровка: 𝑚𝑜𝑑 119=2 |
| Л(14) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119= **7** |
| Дешифровка: 𝑚𝑜𝑑 119=14 |
| Е(7) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119=**105** |
| Дешифровка: 𝑚𝑜𝑑 119=7 |
| Н(16) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119=**67** |
| Дешифровка: 𝑚𝑜𝑑 119=16 |
| К(13) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119= **55** |
| Дешифровка: 𝑚𝑜𝑑 119=13 |
| О(17) | Шифровка: С=()𝑚𝑜𝑑 𝑟=  𝑚𝑜𝑑 119= **68** |
| Дешифровка: 𝑚𝑜𝑑 119=77 |

**Вывод:** изучили принципы работы криптосистемы с открытым ключом на основе алгоритма RSA.