**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**»**

Выполнила: студент гр. ИП-32

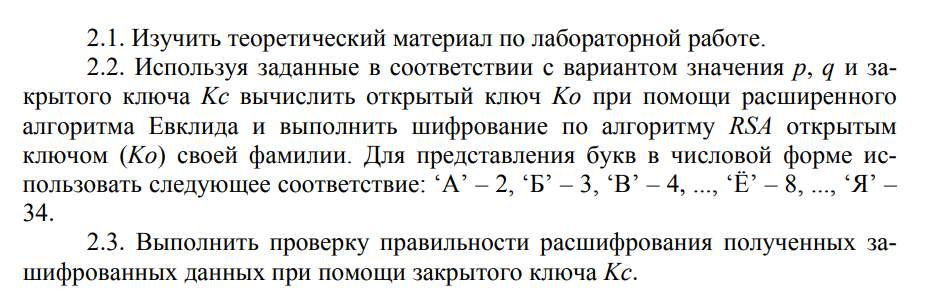
Суховенко Э. С.

Принял: профессор Кудин В.П.

Гомель 2022

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

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ







1. p = 11 q=5;
2. r = p\*q = 11\*5 = 55;
3. ;
4. Кс = 13

Ко = 37

1. Шифруем слово Кирпиченко с помощью открытого ключа Ко = 37

{13,11,19,18, 11,26,7,16,13,17}

С(1) = (1337) mod 55 = 18

С(2) = (1137) mod 55 = 11

С(3) = (1937) mod 55 = 24

С(4) = (1837) mod 55 = 28

С(5) = (1137) mod 55 = 11

С(6) = (2637) mod 55 = 16

С(7) = (737) mod 55 = 17

С(8) = (1637) mod 55 = 36

С(9) = (1337) mod 55 = 18

С(10) = (1737) mod 55 = 52

Получаем{18,11,24,28,11,16,17,36,18,52}

1. Расшифруем слово Кирпиченко с помощью закрытого ключа Кс = 13

{18,11,24,28,11,16,17,36,18,52}

М(1) = (1813) mod 55 = 13

М(2) = (1113) mod 55 = 11

М(3) = (2413) mod 55 = 19

М(4) = (2813) mod 55 = 18

М(5) = (1113) mod 55 = 11

М(6) = (1613) mod 55 = 26

М(7) = (1713) mod 55 = 7

М(8) = (3613) mod 55 = 16

М(9) = (1813) mod 55 = 13

М(10) = (5213) mod 55 = 17

Получаем {13,11,19,18,11,26,7,16,13,17}, что расшифровывается как Кирпиченко

**Вывод:** В ходе выполнения данной лабораторной работы были изучены принципы работы криптосистемы с открытым ключом на основе алгоритма RSA.