МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования   
«Гомельский государственный университет имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Отчёт по теме

**«КРИПТОСИСТЕМА RSA»**

Студент группы МС-22 Яковенко Т.В.

Проверил: ст. преп. Соколов С.И.

Гомель 2022

Задание 1.

Зашифровать свою фамилию и имя, используя следующие пары

простых чисел p и q и открытый ключ e=13

1 Возьмем два простых числа: p =9281, q =9283.

2. Зашифруем системой RSA: « Яковенко Тимофей »

Тогда открытый ключ n=p\*q=86155523

Находим f(n)=(9281-1)\*(9283-1)=86136960

Возьмем c=33121603061512160020101416220611

Разделим по 8 цифр:

c1=33121603

c2=06151216

c3=00201014

c4=16220611

Запишем е в двоичной системе:

e=13=1101

Разделим на n с остатком:

c1%n=38249643

c2%n=59815799

c3%n=37132347

c4%n=17027048

Ответ: (38249643, 59815799, 37132347, 17027048), n=86155523, e=13;

Задание 2. Расшифровать сообщение (криптосистема RSA)

В файле питона

n =1269083, e =13, ш =1101727

с=97

p= 3, q=37

n=111

НОД(3,37)=1

f(n)=(3-1)(37-1) = 72

e=5

НОД(72,5)=1

c^e=82(mod n)

(5,111) –открытый ключ

Передаваемое сообщение (82,5,111)

Задание 3

В файле питона

Вывод

В ходе лабораторной работы ознакомились с криптосистемами RSA.

Научились шифровать и расшифровывать сообщение разными способами.