МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«Гомельский государственный университет

имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Отчет по теме

**«КРИПТОСИСТЕМА RSA»**

Студент группы МС-22 Перникова Ю.С.

Проверил:

Старший преподаватель

кафедры общей физики Соколов С. И.

Гомель, 2023

**Вариант 8**

**Задание 1.** Зашифровать свою фамилию и имя, используя следующие пары простых чисел p и q и открытый ключ e=13.

1. Зашифруем системой RSA: «Перникова Юлия».
2. Возьмем два простых числа: p =9929 и q =9931.
3. Открытый ключ: n=p\*q=98604899
4. Находим ф(n)=(9929-1)(9931-1)=98585040
5. Выберем e=13
6. Возьмем c=1706181510121603010032131033

Разделим по 7 цифр:

с1=1706181

с2=5101216

с3=0301003

с4=2131033

Разделим на n с остатком:

c1%n=55781912

c2%n=16107294

c3%n=3605379

c4%n=58874231

Передаваемые сообщения: (55781912, 13, 98604899), (16107294,13,98604899),

(3605379, 13, 98604899) и (58874231, 13, 98604899).

**Вывод:** в ходе лабораторной работы мы ознакомились с криптосистемами RSA. Научились шифровать сообщение разными способами.