**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 № 2

по дисциплине **«Основы защиты информации»**

на тему: **«**Математические основы криптографии**»**

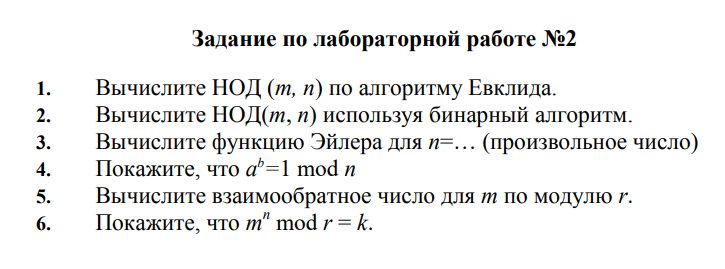
Выполнила: студентка гр. ИП-32

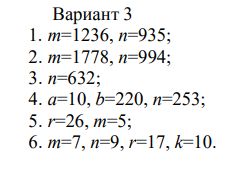
Кирпиченко Д.Д.

Принял: профессор Кудин В.П.

Гомель 2022

Цель работы: Изучить основные математические преобразования, используемые в криптографии.

****



1. Вычислите НОД (m, n) по алгоритму Евклида

m=1239, n=935;

НОД(1239,935)

1239=935\*1+304  
935=304\*3+23

304=23\*13+5  
23=5\*4+3

5=3\*1+2

3=2\*1+1

2=1\*2+0

НОД(1239,935) = 1

1. Вычислите НОД(m, n) используя бинарный алгоритм

m=1778, n=994

НОД(1778, 994)= 2НОД(889, 497)= 2НОД(497, 392)= 2НОД(497, 196)= 2НОД(497, 98)= 2НОД(497, 49)=2 НОД(49, 448)= 2НОД(49, 224)= 2НОД(49, 112)= 2НОД(49, 56)=2 НОД(49, 28)= 2НОД(49, 14)= 2НОД(49, 7)= 2НОД(7, 42)= 2НОД(7, 21)= 2НОД(7, 14)= 2НОД(7, 7)= 2\*7=14

1. Вычислите функцию Эйлера для n=… (произвольное число)

n=632

1. Покажите, что a^b =1 mod n

a=10, b=220, n=253;

НОД(10,253)=1

1. Вычислите взаимообратное число для m по модулю r.

r=26, m=5;

5 \* n = 1 mod 26

5 \* 21 = 1 mod 26

1. Покажите, что m^n mod r = k.

m=7, n=9, r=17, k=10.

9 = 3\*3

1. 7\*7\*7mod17=3
2. 3\*3\*3mod17=10

**Вывод:** В ходе выполнения данной лабораторной работы были изучены основные математические преобразования, используемые в криптографии.