**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**»**

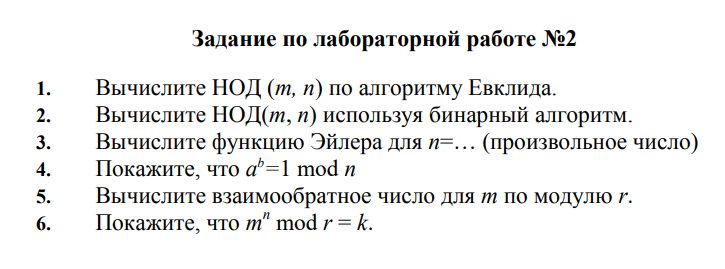
Выполнила: студентка гр. ИП-32

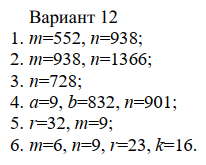
Суховенко Э. С.

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=552, n=938;

НОД(552, 938) = НОД(938, 552)

938=552\*1+386 // gcd(386, 552)  
552=386\*1+166 // gcd(166, 386)

386=166\*2+54 // gcd(54, 166)  
166=54\*3+4 // gcd(4, 54)

54=4\*13+2 // gcd(4, 2)

4 = 2 \* 2 + 0 // gcd(0, 2) = 2

НОД(552, 938) = 2

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

m=938, n=1366

gcd(938, 1366) = 2 \* gcd(469, 683) = 2 \* gcd(683, 469) [1]

gcd(683, 469) = gcd(469, 683 - 469) = gcd(469, 214) [3]

gcd(469, 214) = gcd(469, 107) [2]

gcd(469, 107) = gcd(107, 362) [3]

gcd(107, 362) = gcd(107, 181) = gcd(181, 107) [2]

gcd(181, 107) = gcd(107, 181 – 107) = gcd(107, 74) [3]

gcd(107, 74) = gcd(107, 37) [2]

gcd(107, 37) = gcd(37, 70) [3]

gcd(37, 70) = gcd(37, 35) [2]

gcd(37, 35) = gcd(35, 2) [3]

gcd(35, 2) = gcd(35, 1) = 1 [2]

gcd(938, 1366) = 2

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

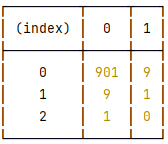
n=728

1. Покажите, что a^b =1 mod n

a=9, b=832, n=901;

Если *n* ≥ 0 – положительное целое число и gcd(*a, n*)=1, где *a* – целое, то  
справедливо:

1.



2.

*=b*

1. Вычислите взаимообратное число для m по модулю r.

r=32, m=9;

– (по теореме Эйлера)

1. Покажите, что m^n mod r = k.

m=6, n=9, r=23, k=16.

9 = 3\*3

1. 6^3 mod 23 = 9
2. 9^3 mod 23 = 16

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