**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**»**

Выполнил: студент гр. ИП-31

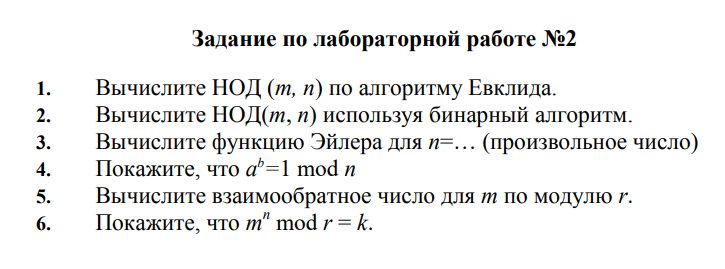
Коваленко А.И.

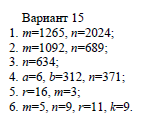
Принял: профессор

Кудин В.П.

Гомель 2023

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

****



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

m=1265, n=2024;

НОД(1265, 2024) = НОД(2024, 1265)

2024=1265\*1+759 //gcd(759, 1265)

1265=759\*1+506//gcd(506, 759)

759=506\*1 +253//gcd(253, 506)

506=253\*2+0//gcd(0, 253) = 253

НОД(1265, 2024) = 253

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

m=1092, n=689

gcd(1092, 689) = gcd(273, 689)

gcd(273, 689) = gcd(689-273, 273) = gcd(416, 273)

gcd(416, 273) = gcd(13, 273)

gcd(13, 273) = gcd(260, 13)

gcd(260, 13) = gcd(65, 13)

gcd(65, 13) = gcd(52, 13)

gcd(52, 13) = gcd(13, 13) = 13

gcd(1092, 689) = 13

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

n=

1. Покажите, что

a=6, b=312, n=371;

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=16, m=3;

– (по теореме Эйлера)

Проверка

1. Покажите, что

m=5, n=9, r=11, k=9.

9 = 3\*3

1. 5^3 mod 11 = 4
2. 10^3 mod 11 = 9

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