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.

Задание по лабораторной работе №2

1. Вычислите НОД (m, n) по алгоритму Евклида.
2. Вычислите НОД(m, n) используя бинарный алгоритм.
3. Вычислите функцию Эйлера для n=… (произвольное число)
4. Покажите, что a^b=1 mod n
5. Вычислите взаимообратное число для m по модулю r.
6. Покажите, что m^n mod $r = k$.

Вариант 15

1. m=1265, n=2024;
2. m=1092, n=689;
3. n=634;
4. a=6, b=312, n=371;
5. r=16, m=3;
6. m=5, n=9, r=11, k=9.

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

2) 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

3) Вычислите функцию Эйлера для n=… (произвольное число)
n=634

$$634 = 2 * 317$$

$$\varphi(634) = 634 * \left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{317}\right) = 316$$

4) Покажите, что $a^b = 1\ mod\ n$
a=6, b=312, n=371;

$$6^{312} = 1\ mod\ 371$$

Если $n \geq 0$ – положительное целое число и gcd(a, n)=1, где a – целое, то справедливо:

$$a^{\varphi(n)} = 1\ mod\ n$$

1. $$gcd(a,n) = gcd(6,371) = 1$$
2. $$371 = 7 * 53$$

$$\varphi(n) = 371 * \left(1 - \frac{1}{7}\right) * \left(1 - \frac{1}{53}\right) = 312$$

$\varphi(n) = \varphi(371) = 312 = b$

5) Вычислите взаимообратное число для m по модулю r.
r=16, m=3;

$$n * m = 1\ mod\ r$$
$$n^{\varphi(n)} = 1\ mod\ r$$
$$=>\ 1 = n^{\varphi(n)}\ mod\ r$$ – (по теореме Эйлера)
$$=> n * m = n^{\varphi(n)}\ mod\ r$$
$$=> m = n^{\varphi(n)-1}\ mod\ r$$

$$3 * n = 1\ mod\ 16$$

$$\varphi(16) = 16 * \left(1 - \frac{1}{2}\right) = 8$$

$$m = 3^{\varphi(16)-1}\ mod\ 16 = 3^{8-1}\ mod\ 16 = 3^7\ mod\ 16 = 11$$

$$3 * 11 = 1\ mod\ 16$$

Проверка

$$3 * 11\ mod\ 16 = 1$$

6) Покажите, что $m^n \ mod\, r \ = \ k$.

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

$$5^9 \ mod\ 11 = 9$$

9 = 3*3

$$(5^3)^3 mod\ 11 = 9$$

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.