Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникации им. проф. М.А. Бонч-Бруевича»

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии»

Лабораторная работа № 12

РЕШЕНИЕ ЗАДАЧ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ

Выполнил: ст. г. ИКТЗ-83

Громов А.А.

Проверил: Яковлев В. А.

Санкт-Петербург
2021

Цель лабораторной работы:

- Приобретение навыков выполнения вычислений дискретной математики

Выполнение работы:

Задание №1

Найти наибольший общий делитель.
Четные номера. Найти НОД (8888,2404)

$$\mathbf{8888 = 3 * 2404 + 1676}$$
$$\mathbf{2404 = 1 * 1676 + 728}$$
$$\mathbf{1676 = 2 * 728 + 220}$$
$$\mathbf{728 = 3 * 220 + 68}$$
$$\mathbf{220 = 3 * 68 + 16}$$
$$\mathbf{68 = 4 * 16 + 4}$$
$$\mathbf{16 = 4 * 4 + 0}$$

Ответ: НОД (8888,2404) = 4

Задание №2

Используя алгоритм быстрого возведения в степень, вычислить:
Четные номера. $\mathbf{3^{104}(mod\ 7)}$.

$$\mathbf{104 = 64 + 32 + 8 = 110100}$$
$$\mathbf{3^1 = 3(mod\ 7); 3^2 = 2(mod\ 7);\ 3^4 = 4\ (mod\ 7); 3^8 = 2\ (mod\ 7);\ 3^{16} = 4\ (mod\ 7);\ 3^{32} = 2\ (mod\ 7); 3^{64} = 4\ (mod\ 7);}$$
$$\mathbf{Y = 4 * 2 * 2\ (mod\ 7) = 2}$$

Ответ: $\mathbf{3^{104}(mod\ 7) = 2}$

Задание №3

Найти обратный элемент к числу *a* по *mod b*,
где *a* соответствует числу в таблице 1, порядковый номер которого совпадает с Вашим номером по журналу, *b* с номером большим на 10 порядковый номер числа *a*.

Таблица1

23	29	31	37	41	43	47	53	59	61
67	71	73	79	83	89	97	101	103	107
109	113	127	131	137	139	149	151	157	163
167	173	179	181	191	193	197	199	211	223

$a = 37; b = 79$

1) Находим НОД:

$79 = 2 * 37 + 5$

$37 = 7 * 5 + 2$

$5 = 2 * 2 + 1$

$2 = 2*1 + 0$

НОД (79,37) = 1

2) $1 = (z1 * 37 + z2 * 79)\ mod\ 79 = z1 * 37\ mod\ 79$

$1 = 5 - 2 * 2$

$2 = 37 - 7 * 5$

$5 = 79 - 2 * 37$

$$\mathbf{1 = 5 - 2 * 2 = 79 - 2 * 37 - 2 * \left(37 - 7 * (79 - 2 * 37)\right)}$$
$$\mathbf{= 79 - 2 * 37 - 2 * (37 - 7 * 79 + 14 * 37)}$$
$$\mathbf{= 79 - 2 * 37 - 2 * (15 * 37 - 7 * 79)}$$
$$\mathbf{= 79 - 2 * 37 - 30 * 37 + 14 * 79 = 15 * 19 - 32 * 37}$$

$\boldsymbol{z1 = -32;\ z2 = 15}$

3) $\boldsymbol{a^{-1} = -32 = 47}$

4) Проверка $\mathbf{47 * 37(mod\ 79) = 1739(mod\ 79) = 1}$

Ответ: $\boldsymbol{a^{-1} = 47}$

Задание №4

Используя тест Ферма, проверить является ли число p простым.

Таблица 2

179	183	191	193	197	199	213	223	227	229
233	239	247	251	257	263	269	271	277	281
283	299	307	311	311	317	331	337	347	349

$P = 193; b = 2$

$2^{192} = (2^{16})^{12}\ mod\ 193 = \left(65536(mod\ 193)\right)^{12}(mod 193) = 1$

$P = 193; b = 3$

$3^{192} = (3^{16})^{12}\ mod\ 193 = \left(43046721(mod\ 193)\right)^{12}(mod 193) = 1$

Вероятность ошибки, т. е. вероятность принять составное число за простое составляет 0.25.

Ответ: число 193 – простое

Выводы:

В ходе данной лабораторной работы, мы закрепили навыки вычисления наибольшего общего делителя, быстрого возведения в степень по модулю, вычисления обратного элемента к числу по модулю, а также проверки простого числа используя тест Ферма.