Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Валдайцев А. Д.

ФИТ 2 курс 5 группа

Преподаватель: Берников В. О.

Минск 2022

**Практическое занятие №8**

**Тема «****Криптографическая защита информации»**

**Цель:** получение основных сведений из курса теории чисел**.**

**Индивидуальные задания**

1.Найти канонические разложения чисел *а* и *b*.

2. Найти НОД  пользуясь: a) алгоритмом Евклида, б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удовлетворяющие соотношению Безу: *au* + *bv* = НОД .

6. Найти остаток от деления данного числа на простое.

**Вариант 3**

1-3. *а* = 660422941, *b* = 36481301.

6. Найти остаток от деления  на 19.

**Задание 1.** Найти канонические разложения чисел *а* = 660422941, *b* = 36481301.

**Решение.**

|  |  |
| --- | --- |
| 660422941 | 101  6538841 | 101  64741 | 101  641 | 641  1 | | 36481301 | 101  361201 | 601  601 | 601  1 | |

660422941 = 101 ∙ 101 ∙ 101 ∙ 641 = 1013 ∙ 641;

36481301 = 101 ∙ 601 ∙ 601 = 101 ∙ 6012.

**Задание 2.** Найти НОД (660422941*,* 36481301) пользуясь: а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** а) Применим алгоритм Евклида.

660422941 = 36481301 ∙ 18 + 3759523;

36481301 = 3759523 ∙ 9 + 2645594;

2645594 = 1113929 ∙ 2 + 417736;

1113929 = 417736 ∙ 2 + 278457;

417736 = 278457 ∙ 1 + 139279;

278457 = 139279 ∙ 1 + 139178;

139279 = 139178 ∙ 1 + 101;

139178 = 101 ∙ 1378 – остаток равен нулю; значит, НОД равен предыдущему остатку от деления.

НОД (660422941; 36481301) = 101.

б) Применим разложение чисел на простые множители, полученное в предыдущем задании:

660422941 = 101 ∙ 101 ∙ 101 ∙ 641 = 1013 ∙ 641;

36481301 = 101 ∙ 601 ∙ 601 = 101 ∙ 6012.

Наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел:

НОД (660422941; 36481301) = 101.

**Задание 3.** С помощью расширенного алгоритма Евклида найти целые числа *u*,*v*, удовлетворяющие соотношению Безу:  для целых чисел *а* = 660422941, *b* = 36481301.

**Решение.** Сначала необходимо с помощью алгоритма Евклида найти НОД (660422941; 36481301). Используем значение, полученное в предыдущем задании с помощью алгоритма Евклида:

НОД (660422941; 36481301) = 101.

Теперь построим соотношение Безу для данных *a* и *b:*

*au* + *bv* = НОД ;

660422941∙ *u* + 36481301 ∙ *v* = 101.

101 = 139279 + 139178 ∙ (-1) = 139279 + (278457 + 139279 ∙ (-1)) ∙ (-1) = 139279 ∙ 2 + 278457 ∙ (-1) = … = 660422941 ∙ (-262) + 36481301 ∙ 4743.

Значит, коэффициенты соотношения Безу:

*u* = -262;

*v* = 4743.

**Задание 4.**

а)Найти остаток от деления  на 19.

**Решение.**

