Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Практическое занятие №8**

Криптографическая защита информации

Выполнил:

Студент 2 курса 7 группы ФИТ

Бобрович Глеб Сергеевич

Проверил:

Барковский Евгений Валерьевич

**Минск 2022 г.**

**Цель работы**: Получение основных сведений из курса теории чисел

**Задание**

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

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

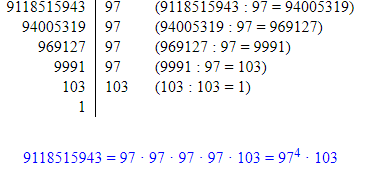
3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удовлетворяющие соотношению Безу: *au* + *bv* = НОД(a, b).

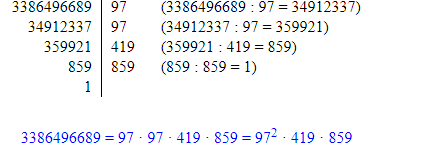
6. Найти остаток от деления данного числа на простое.

***Вариант 5***

a = 9118515943, b = 3386496689

1. **Каноническое разложение чисел a и b**





1. **Найти НОД пользуясь**

**А)** алгоритмом Евклида

9118515943 = 3386496689 ∙ 2 + 2345522565

3386496689 = 2345522565 ∙ 1 + 1040974124

2345522565 = 1040974124 ∙ 2 + 263574317

1040974124 = 263574317 ∙ 3 + 250251173

263574317 = 250251173 ∙ 1 + 13323144

250251173 = 13323144 ∙ 18 + 10434581

13323144 = 10434581 ∙ 1 + 2888563

10434581 = 2888563 ∙ 3 + 1768892

2888563 = 1768892 ∙ 1 + 1119671

1768892 = 1119671 ∙ 1 + 649221

1119671 = 649221 ∙ 1 + 470450

649221 = 470450 ∙ 1 + 178771

470450 = 178771 ∙ 2 + 112908

178771 = 112908 ∙ 1 + 65863

112908 = 65863 ∙ 1 + 47045

65863 = 47045 ∙ 1 + 18818

47045 = 18818 ∙ 2 + 9409

18818 = 9409 ∙ 2

Остаток от деления = 0, следовательно, НОД = 9409

**Б)** Разложением на простые множители

9118515943 = 97 · 97 · 97 · 97 · 103

3386496689 = 97 · 97 · 419 · 859

Общий множитель чисел: 94 \* 97

НОД = 9409

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

По алгоритму Евклида НОД равен 9409.

9118515943 = 3386496689 ∙ 2 + 2345522565 поэтому 2345522565 = 9118515943 + 3386496689 \* (-2)

3386496689 = 2345522565 ∙ 1 + 1040974124 поэтому 1040974124 = 3386496689 + 2345522565 \* (-1)

2345522565 = 1040974124 ∙ 2 + 263574317 поэтому 263574317 = 2345522565 + 1040974124 \* (-2)

1040974124 = 263574317 ∙ 3 + 250251173 поэтому 250251173 = 1040974124 + 263574317 ∙ (-3)

263574317 = 250251173 ∙ 1 + 13323144 поэтому 13323144 = 263574317 + 250251173 ∙ (-1)

250251173 = 13323144 ∙ 18 + 10434581 поэтому 10434581 = 250251173 + 13323144 ∙ (-18)

13323144 = 10434581 ∙ 1 + 2888563 поэтому 2888563 = 13323144 + 10434581 ∙ (-1)

10434581 = 2888563 ∙ 3 + 1768892 поэтому 1768892 = 10434581 + 2888563 ∙ (-3)

2888563 = 1768892 ∙ 1 + 1119671 поэтому 1119671 = 2888563 + 1768892 ∙ (-1)

1768892 = 1119671 ∙ 1 + 649221 поэтому 649221 = 1768892 + 1119671 ∙ (-1)

1119671 = 649221 ∙ 1 + 470450 поэтому 470450 = 1119671 + 649221 ∙ (-1)

649221 = 470450 ∙ 1 + 178771 поэтому 178771 = 649221 + 470450 ∙ (-1)

470450 = 178771 ∙ 2 + 112908 поэтому 112908 = 470450 + 178771 ∙ (-2)

178771 = 112908 ∙ 1 + 65863 поэтому 65863 = 178771 + 112908 ∙ (-1)

112908 = 65863 ∙ 1 + 47045 поэтому 47045 = 112908 + 65863 ∙ (-1)

65863 = 47045 ∙ 1 + 18818 поэтому 18818 = 65863 + 47045 ∙ (-1)

47045 = 18818 ∙ 2 + 9409 поэтому 9409 = 47045 + 18818 ∙ (-2)

18818 = 9409 ∙ 2

Получим 9409 = (151238) \* 9118515943 + 3386496689 \* (-407225)

U = 151238

V = -407225

1. **Найти остаток от деления**

на 23

1999 делится на 23 с остатком 21.

1999^2 делится на 23 с остатком 4.

1999^3 делится на 23 с остатком 15.

1999^4 делится на 23 с остатком 16.

1999^5 делится на 23 с остатком 14.

1999^6 делится на 23 с остатком 18.

1999^7 делится на 23 с остатком 10.

1999^8 делится на 23 с остатком 3.

1999^9 делится на 23 с остатком 17.

1999^10 делится на 23 с остатком 12.

1999^11 делится на 23 с остатком 22.

1999^12 делится на 23 с остатком 2.

1999^13 делится на 23 с остатком 19.

1999^14 делится на 23 с остатком 8.

1999^15 делится на 23 с остатком 7.

1999^16 делится на 23 с остатком 9.

1999^17 делится на 23 с остатком 5.

1999^18 делится на 23 с остатком 13.

1999^19 делится на 23 с остатком 20.

1999^20 делится на 23 с остатком 6.

1999^21 делится на 23 с остатком 11.

1999^22 делится на 23 с остатком 1.

1999^23 делится на 23 с остатком 21.

1999^24 делится на 23 с остатком 4.

1999^25 делится на 23 с остатком 15.

1999^26 делится на 23 с остатком 16.

(mod 23) = 15

**Вывод:** в ходе практической работы я получил основные сведения из курса теории чисел.