

**Цель работы:**

- Изучить основы криптографической защиты информации
- Применить данные методы на практике

**Задание №1. С помощью алгоритма Евклида найти НОД чисел:**

1. НОД (130, 15)
2. НОД (374, 32)
3. НОД (5741, 76)
4. НОД (846, 42)
5. НОД (5783, 3420)

1. НОД (130, 15) = 5
2. НОД (374, 32) = 2
3. НОД (5741, 76) = 1
4. НОД (846, 42) = 6
5. НОД (5783, 3420) = 1

**Задание №2. С помощью расширенного Алгоритма Евклида найти НОД (a, b) и значения s и t:**

1. a = 57, b = 14
2. a = 328, b = 36
3. a = 1179, b = 27
4. a = 502, b = 52
5. a = 791, b = 13

1. **a = 57, b = 14:** НОД = 1, s = -1, t = 4  $\Rightarrow (57 * (-1) + 14 * 4 = 1)$
2. **a = 328, b = 36:** НОД = 4, s = -1, t = 9  $\Rightarrow (328 * (-1) + 36 * 9 = 4)$
3. **a = 1179, b = 27:** НОД = 9, s = 1, t = -44  $\Rightarrow (1179 * 1 + 27 * (-44) = 9)$
4. **a = 502, b = 52:** НОД = 2, s = -5, t = 48  $\Rightarrow (502 * (-5) + 52 * 48 = 2)$
5. **a = 791, b = 13:** НОД = 1, s = -5, t = 304  $\Rightarrow (791 * (-5) + 13 * 304 = 1)$

**Задание 3. Найдите частное и общие решения следующих линейных диофантовых уравнений:**

1.  $25x + 10y = 15$
2.  $19x + 13y = 20$
3.  $14x + 21y = 77$
4.  $40x + 16y = 885$

1.  **$25x + 10y = 15$** 
  - Частное решение: x = 1, y = -1
  - Общее решение:  $x = 1 + 2k, y = 1 - 5k, k \in \mathbb{Z}$
2.  **$19x + 13y = 20$** 
  - Частное решение: x = 7, y = -10
  - Общее решение:  $x = 7 + 13k, y = -10 - 19k, k \in \mathbb{Z}$
3.  **$14x + 21y = 77$** 
  - Частное решение: x = 1, y = 3
  - Общее решение:  $x = 1 + 3k, y = 3 - 2k, k \in \mathbb{Z}$
4.  **$40x + 16y = 88$** 
  - Частное решение: x = 1, y = 3

- Общее решение:  $x = 1 + 2k$ ,  $y = 3 - 5k$ ,  $k \in \mathbb{Z}$

**Задание 4. Определите, сколько из следующих целых чисел пройдут испытание Ферма на простоту чисел: 100, 110, 130, 150, 200, 250, 271, 341, 561. Используйте основание 2.**

Прошли испытание: 27

Не прошли: 100, 110, 130, 150, 200, 250, 341, 561

**Задание 5. Найдите результаты следующих операций:**

1.  $22 \bmod 7$
2.  $140 \bmod 10$
3.  $-78 \bmod 13$
4.  $0 \bmod 15$

1.  $22 \bmod 7 = 1$
2.  $140 \bmod 10 = 0$
3.  $-78 \bmod 13 = 0$
4.  $0 \bmod 15 = 0$

**Вывод:** в результате работы были изучены основы криптографической защиты информации.