**Практическое занятие 1**

***Основы модулярной арифметики, проверка простоты и факторизация чисел***

***Цель работы:*** освоение и программная реализация принципов, методов и алгоритмов решения вспомогательных задач криптографии.

**Задание 1.1.** Найти наибольший делитель двух чисел методом Евклида

**Индивидуальное задание**

| Вариант | *a* | *b* |
|---|---|---|
| 1 | 32911 | 38189 |
| 2 | 38189 | 60127 |
| 3 | 60127 | 46619 |
| 4 | 46619 | 41113 |
| 5 | 41113 | 43711 |
| 6 | 43711 | 55439 |
| 7 | 65147 | 41131 |
| 8 | 41131 | 55799 |
| 9 | 55799 | 65141 |
| 10 | 65141 | 36209 |
| 11 | 36209 | 54419 |
| 12 | 54419 | 59221 |
| 13 | 59221 | 33829 |
| 14 | 33829 | 41611 |
| 15 | 41381 | 48079 |

**Задание 1.2.** Найти результат преобразования

- методом, основанным на теореме Эйлера;
- методом цепочек

**Индивидуальное задание**

| Вариант | задание | Вариант | задание |
|---|---|---|---|
| 1 | $17^{31}$mod7 | 9 | $17^{121}$ mod 7 |
| 2 | $3^{311}$ mod 7 | 10 | $3^{121}$mod7 |
| 3 | $17^{213}$mod7 | 11 | $7^{17}$ mod 5 |
| 4 | $2^{61}$mod5 | 12 | $3^{255}$ mod7 |
| 5 | $2^{111}$mod5 | 13 | $5^{215}$mod7 |
| 6 | $3^{61}$mod7 | 14 | $2^{63}$ mod7 |
| 7 | $5^{63}$mod7 | 15 | $5^{21}$mod7 |
| 8 | $5^{213}$mod7 | | |

**Задание 1.3.** Найти обратное значение числа по модулю:

- при помощи определения кратности k («по определению»)
- с использованием функции Эйлера.

**Индивидуальное задание**

| Вариант | задание | Вариант | задание |
|---|---|---|---|
| 1 | $7^{-1}$(mod 19) | 9 | $7^{-1}$(mod l7) |
| 2 | $19^{-1}$(mod 5) | 10 | $5^{-1}$(mod 13) |
| 3 | $17^{-1}$(mod 5) | 11 | $19^{-1}$(mod 7) |
| 4 | $7^{-1}$(mod 17) | 12 | $17^{-1}$(mod 7) |
| 5 | $9^{-1}$(mod 23) | 13 | $7^{-1}$(mod 5) |
| 6 | $7^{-1}$(mod 23) | 14 | $5^{-1}$(mod 7) |
| 7 | $7^{-1}$(mod l3) | 15 | $5^{-1}$(mod 11) |
| 8 | $79^{-1}$(mod 17) | | |