
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Домашнее задание 2

ЗАДАНИЕ

1. Решить сравнение $125x \equiv 3 \pmod{512}$.
2. Решить систему сравнений
$$\begin{cases} x \equiv 2 \pmod{12}, \\ x \equiv 5 \pmod{13}, \\ x \equiv 3 \pmod{7}. \end{cases}$$
3. Вычислить символ Лежандра $\left(\frac{426}{557}\right)$ с помощью его свойств и с использованием квадратичного закона взаимности.
4. Решить сравнение $x^2 \equiv 128 \pmod{311}$.
5. Выполнить целочисленную факторизацию числа 17136 посредством р-алгоритма Полларда.
6. Найти $\log_{71} 156$ в группе \mathbb{Z}_{251}^* , если известно, что $\mathbb{Z}_{251}^* = \langle 71 \rangle$.

ОЦЕНИВАНИЕ

Домашнее задание считается зачтенным в случае успешного выполнения не менее чем четырех заданий из шести.
