Российский государственный педагогический университет им. А. И. Герцена.
Институт информационных технологий и технологического образования
Информатика и вычислительная техника Технологии разработки программного обеспечения

Защита Информации

Отчёт по лабораторной работе №2

Работу выполнил:
Маковеев Никита Владимирович
Группа:
090301/2.2
Преподаватель:
М. В. Швецкий

Санкт-Петербург
2025

Задание 1. Номера 1,2

Номер 1.

(a) $p_1 = 5, p_2 = 11, a = 3, m = 12$

$$r_a = 5 \cdot 11 = 55$$
$$\varphi(55) = 40$$
$$m_1 = 12^3 \mod 55 \to m_1 = 23$$
$$\alpha = 3^{-1} \mod 40 \to \alpha = 27$$
$$m_2 = 23^{27} \mod 55 \to m_2 = 12$$

(b) $p_1 = 5, p_2 = 13, a = 5, m = 20$

$$r_a = 5 \cdot 13 = 65$$
$$\varphi(65) = 48$$
$$m_1 = 20^5 \mod 65 \to m_1 = 50$$
$$\alpha = 5^{-1} \mod 48 \to \alpha = 29$$
$$m_2 = 50^{29} \mod 65 \to m_2 = 12$$

(c) $p_1 = 7, p_2 = 11, a = 7, m = 17$

$$r_a = 7 \cdot 11 = 77$$
$$\varphi(77) = 60$$
$$m_1 = 17^7 \mod 60 \to m_1 = 53$$
$$\alpha = 7^{-1} \mod 60 \to \alpha = 43$$
$$m_2 = 53^{43} \mod 60 \to m_2 = 17$$

(d) $p_1 = 7, p_2 = 13, a = 5, m = 30$

(e) $p_1 = 3, p_2 = 11, a = 3, m = 15$

$$r_a = 3 \cdot 11 = 33$$
$$\varphi(33) = 20$$
$$m_1 = 15^3 \mod 33 \to m_1 = 9$$
$$\alpha = 3^{-1} \mod 20 \to \alpha = 7$$
$$m_2 = 9^7 \mod 33 \to m_2 = 15$$

Номер 2.

$$m = p_1 \cdot p_2 \to e \cdot d \equiv 1 \mod \varphi(m) \to \alpha \cdot 3 + \beta \cdot \varphi(m) = 1$$
$$\to d \equiv \frac{1 - \beta \cdot \varphi(m)}{3} \mod \varphi(m), \beta \in \mathbb{Z} \to d = \frac{1 - \beta \cdot \varphi(m)}{3} + k \cdot \varphi(m)$$
$$1 < d < \varphi(m) \to] \ k = 0 \to -1 < \beta < -3 \to \beta = -2$$

Что и требовалось доказать.

Задание 2.

$$r_a = 187 \quad \alpha = 3 \quad m = 100$$

$$r_a = 11 \cdot 17 \to \varphi(r_a) = 160$$

$$a \cdot \alpha \equiv 1 \mod 160 \to a = 107 \to m_2 = m^a \mod r_a \to m_2 = 100^{107} \mod 187$$

$$m_2 = 111$$