

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

# 1. Задание 1. Номера 1,2

## 1.1. Номер 1.

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

$$r_a = 5 \cdot 11 = 55$$

$$\varphi(55) = 40$$

$$m_1 = 12^3 \mod 55 \rightarrow m_1 = 23$$

$$\alpha = 3^{-1} \mod 40 \rightarrow \alpha = 27$$

$$m_2 = 23^{27} \mod 55 \rightarrow m_2 = 12$$

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

$$r_a = 5 \cdot 13 = 65$$

$$\varphi(65) = 48$$

$$m_1 = 20^5 \mod 65 \rightarrow m_1 = 50$$

$$\alpha = 5^{-1} \mod 48 \rightarrow \alpha = 29$$

$$m_2 = 50^{29} \mod 65 \rightarrow m_2 = 12$$

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

$$r_a = 7 \cdot 11 = 77$$

$$\varphi(77) = 60$$

$$m_1 = 17^7 \mod 60 \rightarrow m_1 = 53$$

$$\alpha = 7^{-1} \mod 60 \rightarrow \alpha = 43$$

$$m_2 = 53^{43} \mod 60 \rightarrow m_2 = 17$$

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

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

$$r_a = 3 \cdot 11 = 33$$

$$\varphi(33) = 20$$

$$m_1 = 15^3 \mod 33 \rightarrow m_1 = 9$$

$$\alpha = 3^{-1} \mod 20 \rightarrow \alpha = 7$$

$$m_2 = 9^7 \mod 33 \rightarrow m_2 = 15$$