

Задача 5.

$$p = 59$$

$$g = 3$$

$$X_A = 8$$

$$X_B = 43$$

$$y = g^x \pmod{p} \text{ - открытый ключ}$$

$$y_A = 3^8 \pmod{59} = 12$$

$$y_B = 3^{43} \pmod{59} = 16$$

$$Z_{AB} = y_B^{X_A} \pmod{p} = 16^8 \pmod{59} = 51$$

$$\text{Ответ: } y_A = 12; y_B = 16; Z_{AB} = 51$$