RSA Operations

Marcio Woitek

Problem 1

Answer: 4

When the consider the integers k in the range $1 \leq k \leq 12$, there are only 4 integers that are relatively prime to 12: 1, 5, 7, 11. Hence:

$$\varphi(12) = 4. \tag{1}$$

Problem 2

Answer: 40

$$\begin{aligned} \varphi(n) &= \varphi(pq) && (2)\\ &= (p-1)(q-1) && (3)\\ &= (5-1)(11-1) && (4)\\ &= 40 && (5) \end{aligned}$$

Problem 3

Answer: 14

Assuming the message is encrypted using the public key, the ciphertext is given by

$$C = M^e \bmod n. \tag{6}$$

By substituting the known values, we get

$$C = 9^3 \bmod 55. \tag{7}$$

First, we use that $9^3 = 729$. Next, we write this power as $729 = 13 \cdot 55 + 14$. Hence:

$$C = 14. \tag{8}$$

Problem 4

Answer: 60

$$\begin{aligned} \varphi(n) &= \varphi(pq) && (9)\\ &= (p-1)(q-1) && (10)\\ &= (7-1)(11-1) && (11)\\ &= 60 && (12) \end{aligned}$$

Problem 5

Answer: 57

Assuming the message is encrypted using the public key, the ciphertext is given by

$$C = M^e \bmod n. \tag{13}$$

By substituting the known values, we get

$$C = 8^{17} \bmod 77. \tag{14}$$

First, we use that $8^{17} = 2251799813685248$. Next, we write this power as

$$2251799813685248 = 29244153424483 \cdot 77 + 57.$$

Hence:

$$C = 57. \tag{15}$$