Quiz on RSA

Marcio Woitek

Problem 1

Answer: 20

$$\varphi(33) = \varphi(3 \cdot 11) = (3-1)(11-1) = 20. \tag{1}$$

Problem 2

Answer: $p-1$

Problem 3

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:

$$\varphi(12) = 4. \tag{2}$$

Problem 4

Answer: 1

First notice that $77 = 7 \cdot 11$. Since 7 and 11 are prime numbers, the value of the totient function for 77 is

$$\varphi(77) = (7-1)(11-1) = 60. \tag{3}$$

This result allows us to write

$$10^{60} \bmod 77 = 10^{\varphi(77)} \bmod 77.$$

Next, we use the fact that $10 = 2 \cdot 5$. This expression makes it clear that 10 and 77 don't have prime factors in common. In other words, these numbers are relatively prime. Then we can apply Euler's totient theorem, which yields

$$10^{60} \bmod 77 = 1. \tag{4}$$

Problem 5

Answer: 1

To determine the last digit of a^4, we need to compute $a^4 \bmod 10$. To compute this value, first notice that

$$\varphi(10) = \varphi(2 \cdot 5) = (2-1)(5-1) = 4. \tag{5}$$

We'll also use the fact that a and 10 are relatively prime. This has to be true, since by hypothesis a is not divisible by 2 or 5. This means 2 and 5 are not prime factors of a. But they are the only prime factors of 10. Then a and 10 don't have prime factors in common, i.e., they're relatively prime.
With the aid of Euler's theorem, we obtain the following for the last digit of a^4:

$$a^4 \bmod 10 = a^{\varphi(10)} \bmod 10 = 1. \tag{6}$$

Problem 6

- ▷ $\varphi(n)$: $\varphi(n) = \varphi(33) = 20$ [see Problem 1]
- ▷ $e^{\varphi(n)} \bmod n$: e and n are relatively prime, which means this value equals 1 (by Euler's theorem).
- ▷ $\mathrm{GCD}(e, \varphi(n))$: $\mathrm{GCD}(e, \varphi(n)) = \mathrm{GCD}(7, 20) = 1$
- ▷ (d, k) such that $de - k\varphi(n) = 1$: We need to solve the equation $7d - 20k = 1$. We could do that using the extended Euclidean algorithm. But it's easy to guess a solution: $(d, k) = (3, 1)$.
- ▷ Public Key: $(e, n) = (7, 33)$
- ▷ Private Key: $(d, n) = (3, 33)$

Problem 7

- ▷ The prime factors of n.
- ▷ The Euler totient function $\varphi(n)$.