RSA Algorithm

Marcio Woitek

Problem 1

- ▷ d
- ▷ p
- ▷ q
- ▷ The Euler totient function of n, $\varphi(n)$

Problem 2

- ▷ After choosing d, the extended Euclidean algorithm can be used to derive e.
- ▷ After choosing e, the extended Euclidean algorithm can be used to derive d.
- ▷ For the public-private keys of RSA, e and d, given any plaintext m, m raised to the power of $e \cdot d$ $\left(m^{e \cdot d}\right)$ is equal to m.

Problem 3

- ▷ 9
- ▷ 17
- ▷ 21

Problem 4

Answer: 5

We can determine the original plaintext m with the aid of the following equation:

$$m = \frac{m'}{r}. \tag{1}$$

We were given the value of m': $m' = 15$. So we need to find r. To do so, we use the fact that the chosen ciphertext can be written as

$$c' = cr^e \bmod n = 14r^7 \bmod 33 = 14 \cdot 2187 \bmod 33, \tag{2}$$

where we've used the other information given in the problem statement. For the last equality to hold, we must have

$$r^7 = 2187 \Rightarrow r = 3. \tag{3}$$

Hence:

$$m = \frac{15}{3} = 5. \tag{4}$$