Answers to Exercise 1

1. What makes a one-way function computationally feasible?
   - ☐ Key
   - ☐ Cipher
   - ☐ **Trapdoor**
   - ☐ Inversion
2. In asymmetric encryption, the public key is used for
   - ☐ Decrypting a message
   - ☐ Encryption and decryption
   - ☐ **Encrypting a message**
   - ☐ None of the mentioned
3. Which of the following are asymmetric encryption schemes?
   - ☐ DES
   - ☐ **RSA**
   - ☐ AES
   - ☐ **ECC**
   - ☐ ROT13
4. Which of the following are properties of public-key encryption schemes?
   - ☐ They are usually faster than symmetric encryption schemes
   - ☐ Participants need to agree on a pre-shared secret
   - ☐ **A key is a pair of a public and a secret key**
   - ☐ **They are used as part of SSL/TLS (and, thus, https)**

Answers to Exercise 2

One-way property states that it is computationally intractable to compute the pre-image of a digest $h^{-1}\,(\mathrm{y}) = x$.

Collision (second-preimage) resistance implies that it is computationally infeasible to find a second input that has the same output hash.

Answers to Exercise 3

1. With $x|y$, we denote that x divides y with remainder 0. To show $\gcd(a,b) = \gcd(b, a \bmod b)$, we need to show that $\gcd(a,b) \mid \gcd(b, a \bmod b)$ and $\gcd(b, a\ mod\ b) \mid \gcd(a,b)$:
   - $\gcd(a,b) \mid \gcd(b, a \bmod b)$:

     Let $d = \gcd(a,b)$, thus $d \mid a$ and $d \mid b$. Moreover, we know $a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor . b$
     Thus, $a \bmod b$ is a linear combination of a and b. Hence, $d \mid (a \bmod b)$. From this, we can conclude that $d \mid \gcd(b, a \bmod b)$, which is equivalent to $\gcd(a,b) \mid \gcd(b, a \bmod b)$.

   - $\gcd(b, a\ mod\ b) \mid \gcd(a,b)$ can be shown similarly

   Note: In an exam, an informal argument (including examples) would be sufficient.

2. A definition in pseudocode is:

```
euclid(a,b) =
      if b = 0
            return a
      else
            return euclid(b, a mod b)
```

3. A definition in pseudo code is:

```
ext_euclid(a,b) =
      if b = 0
            return (a, 1, 0)
      else
            (d', x', y') := ext_euclid(b, a mod b)
            return (d', y', x' - (a div b) * y')
```

4. We have `ext_euclid(33, 40) = (1, 17, -14)`, hence
   $d = 17$ and $1 = 33.17 + 40.(-14) = 561 - 560$
   We can compute `ext_euclid(33, 40) = (1, 17, -14)` by executing the extended Euclidean algorithms using “paper & pencil”:

```
ext_euclid(33,40)=(d', x', y') := ext_euclid(40, 33 mod 40)
      ext_euclid(40, 33)=(d', x', y') := ext_euclid(33, 40 mod 33)
            ext_euclid(33,7)=(d', x', y') := ext_euclid(7, 33 mod 7)
                  ext_euclid(7,5)=(d', x', y') := ext_euclid(5, 7 mod 5)
                        ext_euclid(5,2)=(d', x', y') := ext_euclid(2, 5 mod 2)
                              ext_euclid(2,1)=(d', x', y') := ext_euclid(1, 2 mod 1)
                                    ext_euclid(1,0) = (1,1,0) // base case
                                    return (1,0,1)
                              return (1,0,1)
                        return (1, 1, -2)
                  return (1, -2, 3)
            return (1, 3, -14)
      return (1, -14, 17)
return (1, 17, -14)
```

Answer to Exercise 4

We first need to compute $n = pq$ and $\Phi = (p-1)(q-1)$:

$$n = p.q = 11.5 = 55$$

$$\Phi = (p-1)(q-1) = (11-1).(5-1) = 10.4 = 40$$

Next, we need to select an e, $1 < e < \Phi$ and e relatively prime to Φ. We choose $e = 33$ ($1 < 33 < 48$ and 33 is relatively prime to 40, i.e., $\gcd(40{,}33) = 1$).

Now, we need to compute the unique integer d, $1 < d < \Phi$ where $ed \bmod \Phi$. From the last exercise, we know already $d = 17$.

Hence, Bob's public key is (55, 33) and his private key is 17.

Answers to Exercise 5

1. Firstly, we encode the message "geheim":

   7, 5, 8, 5, 9, 13

   Secondly, for each encoded letter c, we compute $c = m^{33} \bmod 55$ (i.e., encryption using the public key of Alice):

   2, 15, 28, 15, 14, 8

2. First, we decrypt the message by computing for each letter c of the ciphertext via $m = c^5 \bmod 39$ (i.e., decryption using the private key of Bob):

   19, 5, 3, 18, 5, 20

   Second, we decode the message:

   secret

3. It is worth to note that the cipher text can be identical to the plaintext without any precautions. Usually, we want to avoid this behaviour.