## 9.3 The RSA Cryptosystem

The RSA cryptosystem is a very popular public-key cryptosystem developed in 1977 by the mathematicians Rivest, Shamir, and Adleman. The name of the system is also derived from the first letters of their names. Although the system is already considered old, it is still widely used in modern IT systems.

The basic principle of the RSA cryptosystem is based on the properties of public key cryptosystems: each participant in the system has a private and a public key. Messages are encrypted with the recipient’s public key and can only be decrypted again with the recipient’s corresponding private key.

We will explain the functionality of the RSA system using an example. But before we do so, we need to look at some brief definitions and properties that are necessary for underDefinition: Euler’s φ Functionφ : ℕ → ℕ∈ ℕ 1 ≤ a ≤ n∧gcd a, nφ = 1 standing the RSA algorithm.

Let n ∈ ℕ. We define the function φ n : = a by

We call the function φ the Euler’s totient function or Euler’s function.

The Euler’s φ function (also Euler’s Phi function) thus outputs for a given number n the number of numbers which are greater than or equal to 1 and less than or equal to n and gcd(a,n) = 1gcd(5, 6) = 1. φ gcd(6, 6) = 6gcd(1, 6) = 1 gcd(2, 6) = 2 gcd(3, 7) = 1gcd(3, 6) = 3 |{1, 2, 3, 4, 5,gcd(4,gcd(4,gcd(4,