

# Topics in Algebra: Cryptography - Blatt 2

<http://www.mat.univie.ac.at/~gagt/crypto2019>

Goulnara Arzhantseva  
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell  
martin.finn-sell@univie.ac.at

## 1 Test questions from the lecture to refresh:

**Question 1.** What is the complexity of the RSA parameter generation?

**Question 2.** Let  $f$  be a one-way function. Is  $f \circ f$  necessarily a one-way function?

**Question 3.** What is the worst case / average case complexities of trial division?

**Question 4.** Design an algorithm for computing the square root of an integer. What about its complexity? What about its modular variant and its complexity?

**Question 5.** Which of the following statements are true?

1. If the RSA cryptosystem is breakable, then large numbers can be factored;
2. Breaking the ECC cryptosystem is equivalent to solving the discrete logarithm problem;
3. There is no message expansion in the ECC cryptosystem.

**Question 6.** Why in practice public-key cryptosystems have longer key lengths than symmetric cryptosystems?

## 2 Exercises

**Question 7.** Solve the discrete logarithm problem in  $(\mathbb{Z}/n\mathbb{Z}, +)$ , where  $n \in \mathbb{N}$ . What is the complexity?

**Question 8.** A plaintext  $x$  is said to be *fixed* if  $e_{\mathcal{K}}(x) = x$ . Show that, for  $\mathcal{K} = \text{RSA}$ , the number of possible fixed  $x \in \mathbb{Z}_n^{\times}$  is equal to:

$$\gcd(b-1, p-1)\gcd(b-1, q-1).$$

**Question 9.** Find and describe the steps of Shanks algorithm, then compute  $\log_5 20$  in  $\mathbb{Z}_{47}^\times$ .

**Question 10.** Interpret the function  $h : \mathbb{Z} \rightarrow \mathbb{Z}_n$ , where  $h(x) = x \bmod n$  as a function on binary strings. Is this function a reasonable one way or hash function?

**Question 11.** Show that the function  $y^2 = x^3 + 2x - 2$  is an elliptic curve for some field.

### 3 Optional computer exercises

An exercise here is not mathematically harder than the above, but the numbers are too large and they are best solved by computer:

**Question 12.** Find, describe and implement the steps of Shanks algorithm, and use it to compute  $\log_{106} 12357$  in  $\mathbb{Z}_{24691}^\times$ .

**Question 13.** Let  $E$  be the elliptic curve  $y^2 = x^3 + x + 28$  defined over  $\mathbb{Z}_{71}$ .

- a) Determine the number of points in  $E$ ;
- b) Show that  $E$  is not a cyclic group;
- c) What is the maximal order of an element in  $E$ ? Exhibit an element with that order in  $E$ .