

---

Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

## Exercise 13

Friday, July 21, 2017

### Problem 1.

(*computing square roots modulo  $p$* ) The following scheme is used to compute square roots modulo a prime number  $p$ .

---

**Algorithm 1** Computing square roots modulo a prime number  $p$ .

---

**Input:** An odd prime number  $p$  and a quadratic residue  $a$  modulo  $p$

**Output:** Two square roots  $(r, -r)$  of  $a$  modulo  $p$

- 1) Choose a random  $b \in \mathbb{Z}_p$  until  $v = b^2 - 4a$  is a quadratic non-residue modulo  $p$ .
- 2) Let  $f(x)$  denote the polynomial  $x^2 - bx + a$  with coefficients in  $\mathbb{Z}_p$ .
- 3) Compute  $r = x^{\frac{p+1}{2}} \bmod f(x)$  (Use without proof:  $r$  is an integer)

**return**  $(r, -r)$

---

- a) Let  $p = 11$  and  $a = 5$ . Compute the square roots of  $a$  using Algorithm 1 above. Instead of choosing  $b$  at random, begin with  $b = 5$ . If  $b$  is invalid, increment  $b$  by one.

**Hint:** To compute  $r$  in step 3), perform the polynomial division.

Consider the Rabin cryptosystem. The prime numbers are given by  $p = 11$  and  $q = 23$ . It is known that the plaintext message  $m$  ends with 0100 in its binary representation.

- b) Decrypt the ciphertext  $c = 225$ .
- c) Naive Nelson announces that the plaintext message  $m$  ends with 1111 in its binary representation. Why is this agreement a bad choice for the given ciphertext  $c$ ?

**Problem 2.** (*Rabin cryptosystem*) Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key  $n = 4757 = 67 \cdot 71$ . All integers in the set  $\{1, \dots, n - 1\}$  are represented as a bit sequence of 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram  $c = 1935$ . Decipher this cryptogram.

**Problem 3.** (*coin flipping*) Consider the coin flipping protocol. Let  $p > 2$  be prime.

- a) Show that if  $x \equiv -x \pmod{p}$ , then  $x \equiv 0 \pmod{p}$ .
- b) Suppose Alice cheats when flipping coins over the telephone by choosing  $p = q$ . Show that Bob almost always loses if he trusts Alice.
- c) Alice chooses  $n = p^2$  as the secret key, but Bob suspects that Alice has cheated. Can Bob discover her attempt to cheat? Can Bob use Alice' cheating as an advantage for himself?