# Review Exercise in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2015-03-04

**Problem 1.** *(A variant of the Rabin cryptosystem)* A prime number $p \equiv 5 \mod 8$, a quadratic residue $a$ modulo $p$ and the following algorithm are given.

**Algorithm 1** SQR: Square roots with $p \equiv 5 \mod 8$

**Input:** Prime number $p$ with $p \equiv 5 \mod 8$ and quadratic residue $a$ modulo $p$

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

$d \leftarrow a^{\frac{p-1}{4}} \mod p$
**if** $(d = 1)$ **then**
  $r \leftarrow a^{\frac{p+3}{8}} \mod p$
**end if**
**if** $(d = p - 1)$ **then**
  $r \leftarrow 2a(4a)^{\frac{p-5}{8}} \mod p$
**end if**
**return** $(r, -r)$

**a)** Show that the variable $d$ in algorithm SQR can only take the values 1 or $p - 1$.

**b)** Suppose that $2^{\frac{p-1}{2}} \equiv -1 \mod p$ holds. Prove that algorithm SQR computes both square roots of $a$ modulo $p$.

A variant of the Rabin cryptosystem uses algorithm SQR and is accordingly defined for prime numbers $p, q \equiv 5 \mod 8$ with $n = p \cdot q$.
The prime numbers $p = 53$, $q = 37$, and the ciphertext $c = 1342 = m^2 \mod n$ are given. By agreement the message $m$ ends on 101 in its binary representation.

**c)** Compute the square roots of 17 modulo 53 and 10 modulo 37.

**d)** Decipher the message $m$. You may use $7 \cdot 53 - 10 \cdot 37 = 1$ for your computation.

**Problem 2.** *(Coin Tossing protocols via telephone)* This problem deals with several protocols for realizing a coin toss via telephone. The following symmetric cryptosystem is used for realizing coin tossing over the telephone. The protocol actions are as follows:

- $A$ and $B$ agree upon a common key $k$.
- $A$ chooses a number $x$, encrypt it as $y = E_k(x)$, and sends $y$ to $B$.

- $B$ guesses, if $x$ is even or odd, and sends his guess to $A$.
- $A$ sends $x$ to $B$.

If $B$ has guessed correctly, $B$ wins, otherwise $A$ wins.

**a)** Which player can always win? Substantiate your answer.

In the following a cryptographic hash function is employed.

**b)** State the four basic requirements on cryptographic hash functions.

**c)** Give a protocol for realizing a coin toss which utilizes a cryptographic hash function.

Finally, a protocol for tossing a coin over the telephone based on the factorization problem shall be derived. The protocol starts with:

- $A$ chooses prime numbers $p, q$ with $p, q \mod 4 = 1$ or $p, q \mod 4 = 3$.

**d)** Complete the protocol.

**Problem 3.** *(Pollard Rho Factoring Method)* Consider the following function:

$$E : Y^2 = X^3 + 2X + 6.$$

**a)** Does $E$ describe an elliptic curve in the field $\mathbb{F}_7$? Give a reason.

**b)** Determine all points and their inverses in the $\mathbb{F}_7$-rational group.

**c)** What is the order of the group?

It is difficult to obtain the discrete logarithm $a$ of $Q$ to the base $P$ for two points $P, Q$ on an elliptic curve $E$. A possible approach is the application of the Pollard $\rho$-factoring method. The idea behind this method is to find numbers $c, d, c', d' \in \mathbb{Z}$ for two given points $P, Q$ on the elliptic curve with $\gcd(d - d', \operatorname{ord}(P)) = 1$ such that the following equation holds:

$$cP + dQ = c'P + d'Q. \tag{1}$$

**d)** Compute the discrete logarithm $a$ of $Q$ to the base $P$ by means of (1).

An oracle provides the values $c = 2$, $d = 4$, $c' = -1$, $d' = -3$, $P = (4, 1)$, $Q = (1, 3)$, $4Q = (3, 5)$, and $-3Q = (5, 6)$. Assume that $P$ is a generator.

**e)** Show that equation (1) is fulfilled for these values and compute the discrete logarithm $a$ of $Q = (1, 3)$ to the base $P = (4, 1)$.