# Cryptography I

## Exam, 28.2.2017

### Duration: 3h

**Allowed equipment:** Writing equipment and a calculator not capable of graphical or symbolic calculations.
**Answer all questions.**

1. (2p) a) What is the definition of a cryptosystem?

   (2p) b) Define the Discrete Logarithm Problem (DLP). Name a cryptosystem whose security is based on DLP.

   (2p) c) How many generators does $\mathbb{Z}_{37}^*$ have? Give one of them.

2. (3p) a) Present the VIGENÉRE CIPHER.

   (3p) b) Describe a cryptotext-only attack on the system.

3. (3p) a) Present the RSA cryptosystem.

   (3p) b) Find the factors of $n$, when $n = 2059$ and $782^2 = 1 \pmod{2059}$.

4. (3p) a) Show that 1729 is not a prime using Solovay–Strassen primality test.

   (3p) b) Show that 1729 is not a prime using Miller–Rabin primality test.

   To calculate the **Jacobi symbols**, see the end of the exam paper.

5. (6p) Present the El Gamal digital signature algorithm. Select a public and private key when $p = 61$ and $g = 2$. Sign and verify the message $m = 14$.

The **Jacobi symbol** can be calculated using the following identities. Here $n$ is an odd integer, $n > 1$.

- $m_1 = m_2 \pmod{n} \Rightarrow \left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$;
- $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$;
- $\left(\frac{1}{n}\right) = 1$; $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$; $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$; and
- for $m$ and $n$ odd: $\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}\left(\frac{n}{m}\right)$