**Norwegian University of Science and Technology**
**Department of Mathematical Sciences**



Contact during the exam:
Kristian Gjøsteen 73 55 02 42

# EXAM IN TMA4160 CRYPTOGRAPHY

English
Wednesday, December 16, 2009, with corrections.
Time: 0900-1300
Any printed or hand-written material is allowed during the exam.
An approved, simple calculator is allowed.

**All problems have equal weight. Show your work.**

**Problem 1** We shall work in the group $\mathbb{F}_{83}^*$. Let $g = 2$.

**a)** Find the order of $g$.

**b)** Compute $\log_g 17$ using the Baby-step Giant-step method (Shanks' algorithm).

**c)** Given

$$\begin{aligned} g^{35} &= 5 \cdot 7, \\ g^{80} &= 3 \cdot 7, \text{and} \\ g^{17} &= 3 \cdot 5, \end{aligned}$$

find $\log_g 3$, $\log_g 5$ and $\log_g 7$.

**d)** Use the results from the previous task and the fact that $17g^{14} = 63$ to find $\log_g 17$.

**Problem 2** Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over $\mathbb{F}_{83}$.

**a)** Show that $P = (29, 10)$ is a point on the curve and compute $2P$ and $3P$. What is the order of $P$?

**b)** The point $Q = (73, 53)$ has order 9. Use this together with the result from the previous task to determine the number of points on the curve. Is the group $E(\mathbb{F}_{83})$ cyclic?

**Problem 3** Let $n$ be the product of two primes $p$ and $q$, where $(p-1)/2$ and $(q-1)/2$ are also prime and odd.

**a)** Show that the Jacobi symbol $\left(\frac{-1}{n}\right)$ equals 1, but that $-1$ is not a square $\mathbb{Z}_n^*$.

**b)** Let $J = \{x \in \mathbb{Z}_n^* \mid \left(\frac{x}{n}\right) = 1\}$ and $Q = \{x^2 \mid x \in \mathbb{Z}_n^*\}$. Show that $J$ is a subgroup of $\mathbb{Z}_n^*$, that $Q$ is a non-trivial subgroup of $J$, and that the factor group $J/Q$ has order 2.

**c)** Show that for any $x \in J \setminus Q$ we have that $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$.

Based on these results, we can construct a public key cryptosystem with message space $\{-1, 1\}$ as follows:

- Key generation is to find two primes $p$ and $q$ such that $(p-1)/2$ and $(q-1)/2$ are also prime. The encryption key is $n = pq$.
- To encrypt $m \in \{-1, 1\}$ with the encryption key $n$, choose a random $r \in \mathbb{Z}_n^*$ and compute the ciphertext as $c = r^2 m$.

**d)** Suggest a decryption algorithm (and explain what the decryption key is) and show that it works.