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



Contact during exam:
Øystein Thuen (735 50255)

# TMA4160 - CRYPTOGRAPHY

English
Monday December 1st, 2008
Time: 09:00 – 13:00
Permitted aids (Code B): All written and printed materials. Specified, simple calculator (SR-270X or HP30S)
Grades: December 22, 2008.

**Problem 1** Let $n = 5063$ be an integer.

**a)** Compute the Jacobi symbol $\left(\frac{14}{n}\right)$.

**b)** Given that $14^{\left(\frac{n-1}{2}\right)} \equiv 902 \bmod n$, explain why $n$ is a composite number.

**c)** Compute $986^2 \bmod n$ and use this to factor $n$.

**Problem 2** $p = 683$ is a prime. We have $p - 1 = 2 \cdot 11 \cdot 31$. Compute $4^{11112} \bmod p$.

**Problem 3** For an integer $m \geq 2$, consider the following cryptosystem, called $m$-prime RSA. Let $\{p_1, \ldots, p_m\}$ be a set of $m$ distint primes such that the product $n = \prod_{i=1}^{m} p_i$ is 2048-bit. The Euler phi-function of $n$ is $\phi(n) = \prod_{i=1}^{m}(p_i - 1)$. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ and define the keyspace to be

$$\mathcal{K} = \{(n, e, d) : ed \equiv 1 \bmod \phi(n)\}.$$

Let $K = (n, e, d)$ be a key. For a plaintext $x \in \mathbb{Z}_n$, define encryption

$$e_K(x) = x^e \bmod n.$$

For a ciphertext $y \in \mathbb{Z}_n$, define decryption

$$d_K(y) = y^d \bmod n.$$

The public key is $(n, e)$ and the corresponding private key is $(n, d)$.

**a)** Let $x$ be a plaintext. Show that first encrypting and then decrypting using the corresponding private key, will return x. In other words, show that $d_K(e_K(x)) \equiv x(\mathrm{mod} n)$ for any key $K$ and plaintext $x$.

**b)** It is known that increasing the number of primes $m$ will speed up decryption. Explain why choosing a large $m$ will reduce the security of the system.

**Problem 4** Bob is using Schnorr Signature Scheme to sign his messages. His public key is $(p = 47, q = 23, \alpha = 2, \beta = 7)$. You suspect Bob used the same random number $k$ when signing two different messages. The two signatures are $(\gamma_1, \delta_1) = (15, 15)$ and $(\gamma_2, \delta_2) = (9, 12)$. Use the two signatures to find Bob's private key. Prove that Bob used the same random number for both signatures.

**Problem 5** Bob is using the ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$. He decided to use his favorite prime number

$$p = 2^{1947} \cdot 5 + 1.$$

Since the bit lenght of $p$ is almost 2000, Bob is sure that he will be safe from any adversary. Explain why Bob should reconsider his choice of parameter.

**Problem 6** Let $E$ be an elliptic curve over $\mathbb{Z}_{17}$ given by

$$E : y^2 = x^3 + 3x + 1.$$

$Q = (15, 2)$ is a point on $E$.

**a)** Show that $2Q = (0, 16)$ and that $3Q = (0, 1)$.

**b)** Does $Q$ generate all points of $E$?