Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Contact during exam:
Kristian Gjøsteen (735) 50242

TMA4160 - Kryptografi

English
Saturday December 2, 2006
Time: 09:00 – 13:00
Grades: January 2, 2007

Permitted aids: All printed and written. All types of calculators.

Oppgave 1

a) Find all solutions of

$$\begin{aligned} x &\equiv 1 \pmod{21} \\ x &\equiv 8 \pmod{35}. \end{aligned}$$

For which values of a does the following set have a solution?

$$\begin{aligned} x &\equiv 1 \pmod{21} \\ x &\equiv a \pmod{35} \end{aligned}$$

Oppgave 2

Given $\beta^{10}\alpha^4 \equiv \beta^3\alpha^{61} \pmod{167}$, where α is a generator for $\mathbb{Z}_{167}^*$. Find $\log_\alpha \beta$.

Oppgave 3 Each student at NTNU will receive their own pair of keys for RSA.

- Public key: n and e, where $n = pq$ with p og q prime, and e is such that $\gcd(e, \phi(n)) = 1$.
- Private key: d.

Four methods have been proposed to generate keys efficiently. Explain why none of the methods should be used.

a) All use the same n, where p and q are kept secret, and all have different e.

b) Everyone share the same p, but have different values of q.

c) For each user, let p be arbitrary, and let $q = \text{nextprime}(\text{stn} * 2^{500})$, where stn is a student number consisting of six digits. We assume that everyone can keep their student number hidden to others. Here nextprime(x) is an algorithm that returns the smallest prime $\geq x$.

d) For each user, let p be arbitrary, and let $q = \text{nextprime}(p + 1)$.

Oppgave 4 The following is a suggestion for an identification protocol. Alice has a public key $n = pq$, where p and q are secret (large primes). Alice authenticates to Bob by sending Bob a number x which is a quadratic residue modulo n, and Alice returns y such that $y^2 = x \pmod{n}$. (We can assume that $p \equiv 3 \equiv q \pmod{4}$, such that Alice can compute square roots).

Suppose that you are Bob, explain how you can use this protocol to find Alice's secret p and q.

Oppgave 5 Consider the elliptic curve E given by

$$y^2 = x^3 - 7x + 6 \text{ over } \mathbb{Z}_{107}.$$

a) Find $(-3, 0) \oplus (-1, 36)$ (the sum on the elliptic curve).

b) Show that E has an element of order ≥ 40.

c) Show that E is not a cyclic group.