Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam: Sverre Smalø
(Phone: 735 91750)

Exam in TMA4160 Cryptography

Tuesday 18th of December 2007
Time: 09.00 - 13:00
Permitted aids: (Code B) All printed and hand written aids allowed, simple plain calculator HP30S allowed.

Grades: 18. January 2008

Problem 1 Solve the system of congruences:

$$\begin{aligned} 2^{1334}x + 2y &\equiv 5 \pmod{21} \\ 10^{2669}x + 10y &\equiv 6 \pmod{21} \\ 7x + 4y &\equiv 6 \pmod{15} \\ 11x + 13y &\equiv 10 \pmod{15} \end{aligned}$$

Problem 2 Consider the field F given by $F = \mathbb{Z}_2[X]/(f)$ where $f = X^8+X^4+X^3+X+1$. An affine cipher was designed with $P = C = F$ and with the encryption function E given by $E(t) = a \cdot t + b$ where $a = X^5 + X + 1$ and $b = X + 1$. Find the decryption function D.

Problem 3 For a prime $p \geq 7$, and a generator g in $\mathbb{Z}_p^*$, the elements a and b in $\mathbb{Z}_p^*$ satisfy the following relations:

$$\begin{aligned} 5ab^2 &\equiv g^2 (\operatorname{mod} p) \\ 25a^2b^5 &\equiv g^6 (\operatorname{mod} p) \\ 125a^4b^6 &\equiv g^{11} (\operatorname{mod} p) \end{aligned}$$

Find $\log_g a$ and $\log_g b$.

Problem 4 The ElGamal cryptosystem over $\mathbb{Z}_{71}^*$ with key $(71, \alpha, a, \beta)$ was used to exchange messages between A and B. One day A sent the same message m to B twice, and the sending was $(16, 11)$ and $(64, 9)$. Find m.

Problem 5 Let E be the elliptic curve over $\mathbb{Z}_{71}$ given by the equation $y^2 = x^3 - 8x$. The points $(0, 0)$ and $(1, 8)$ are points on E. Find their sum, i.e. find $(0, 0) \oplus (1, 8)$.

Problem 6 In a bank there are 4 trusted senior employees. The bank has a vault equipped with 6 locks. The bank owner wants that any group of three of the trusted seniors should be able to open the vault, but no group consisting of two of them should be able to open the vault. Find a way of distributing keys to the senior employees so these two requirements are satisfied.