Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Contact during exam:
Aslak Bakke Buan 73 55 02 89/73 59 35 20

EXAM IN TMA4160 CRYPTOGRAPHY

English
Thursday December 8, 2005
Time: 0900-1300

Permitted aids:
any calculator
all printed or written aids

The grades are posted January 7.

All answers should be explained.

Problem 1

2 is a generator for $\mathbb{Z}_{179}^*$. Is $2^{1977769}$ also a generator?

Problem 2

How many solutions does $x^3 \equiv 3 \mod (357035)$ have?

Problem 3

Find all solutions of the set

$x \equiv 2^{191889} \mod 119$
$x \equiv 2^{119} \mod 19$

Problem 4

A public key cryptosystem was used to encrypt x, and you have the corresponding ciphertext y. The owner of the private key is willing to decrypt exactly one ciphertext y' that you can choose and send to him, as long as $y' \neq y$. How can you use this to find x, if

a) RSA is used?

b) ElGamal is used?

Problem 5

Let $GF(16)$ be the finite field with 16 elements constructed using the polynomial $p(x) = x^4 + x + 1$ in $\mathbb{Z}_2[x]$.

a) Show that the (residue class of the) polynomial x is a generator for the multiplicative group of non-zero elements of $GF(16)$.

b) Consider the symmetric cryptosystem with plaintext and ciphertext elements in $GF(16)$, and where encryption is given by multiplying with $x^2 + 1$ modulo $p(x)$. Find the decryption function.

Problem 6

We consider a $(2, 6)$ Shamir secret sharing scheme over $\mathbb{Z}_{11}$. Four players A,B,C,D cooperate to find the secret, but one of them is cheating (so the share he claims to have might not be an actual share). They claim that their shares are
A:(1,2) B:(2,5) C:(3,10) D:(4,3)
Who is cheating and what is the secret?

Problem 7

Show that any elliptic curve over $\mathbb{Z}_{83}$ has an element of order > 30.