Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
AlexeiRudakov 73 59 16 95

EXAM IN COURSE TMA4160 Kryptografi

English
Thuesday December 14, 2004
Time 9–13

Permitted aids (code A):

Grades: Januar 13, 2005.

Remember: numbers 3001, 5003, 7001, 10007 are prime.

Problem 1

Consider the field $F = \frac{\mathbb{Z}_2[x]}{(f)}$ where $f = x^8 + x^4 + x^3 + x + 1$.

An affine cipher was designed with $\mathcal{P} = \mathcal{C} = F$ and an encryption function

$$s = E(t) = a \cdot t + b$$
$$a = [x^5 + x^3 + x^2 + 1] \in F,$$
$$b = [x^4 + x^3 + 1] \in F.$$

Find the coefficients $u, v \in F$ of the decryption function

$t = D(s) = u \cdot s + v$

Problem 2

Find all integers x, such that

$$\begin{cases} x \equiv 2^{356} & (mod\ 71), \\ 2x \equiv 3^{318483} & (mod\ 31). \end{cases}$$

Problem 3

For a prime p, we have $a, b \in \mathbb{Z}_p^*$, and g is a generator of $\mathbb{Z}_p^*$. In calculations for the Index Calculus method it was found that modulo p:

$$\begin{cases} 2a^3\, b^2 \equiv -g^2, \\ 4a^2\, b^5 \equiv +g^6, \\ 8a^8\, b^8 \equiv -g^3. \end{cases}$$

Find $log_g\, a$, $log_g\, b$.

Problem 4

The ElGamal cryptosystem over $\mathbb{Z}_p^*$ was used to exchange messages between A and B. It so happend that A sent the same message $m \in \mathbb{Z}_p^*$ to B twice and the sendings were:

$(27, 56)$, $(81, 19)$.

It is known that $p = 3001$, find m.

Problem 5

Let $p = 71$ and E is an elliptic curve over $\mathbb{Z}_p$ given by the equation

$y^2 = x^3 + 9x$

Let $A = (0, 0), B = (1, 9)$ points of E.

Find $C = A \bigoplus B$

Problem 6

We want to make RSA system with $n = 21010001$ and the encryption function

$y = x^{433}$ $\underline{mod}$ n.

Find the decryption function. (Check if $q = 3001$ divides n).

Problem 7

Let $n = 21010001$ and denote for $a \in \mathbb{Z}_n^*$

$$N(a) = \#\{x \in \mathbb{Z}_n^* : x^3 = a\}$$

Provided that a is destributed uniformly randomly over $\mathbb{Z}_n^*$ find the probabilities

$$p_i = Pr[N(a) = i] \text{ for } i = 1, ..., 10.$$

(Check if $q = 3001$ divides n.)

Problem 8

Let $p = 10007$, $q = 5003$. Propose a method to check "quickly" for $a \in \mathbb{Z}_p^*$ if $ord a = q$ or not. Determine if $ord\ 213 = q$, $ord\ 87 = q$ by your method (without raising the number to q.th power).