Norwegian University
of Science and Technology
Department of Mathematical Sciences

Faglig kontakt under eksamen:
Kristian Gjøsteen, tlf. 73 59 35 20

EKSAMEN I SIF5023 KRYPTOGRAFI

onsdag 18. desember 2002
Kl. 9-14

Sensur: uke 2

Hjelpemidler: A

Problem 1
We make RSA with $n = 31.41 = 1271$, and $y = e(x) = x^{23} \underline{\mathrm{mod}}\ n$ is the encryption function. Write the decryption function. Find the decryption exponent.

Problem 2
The field F

$$F = \mathbb{Z}_2[x]/(x^3 + x + 1) = \{a_0 + a_1\alpha + a_2\alpha^2\}$$

where $a_i \in \mathbb{Z}_2,\ \alpha^3 + \alpha + 1 = 0$, is used as the plaintext and ciphertext domain. The encryption function is given by the formula

$$z = e(y) = (\alpha^2 + 1)y + \alpha.$$

Find $(\alpha^2 + 1)^{-1}$ in F. Write explicitely the decryption function $y = d(z)$.

Problem 3
Find integers x such that

$$\begin{aligned} x &\equiv 2^{37686} \mod 155, \\ x &\equiv 3^{1456} \mod 65. \end{aligned}$$

What such x, if any, satisfy $0 \leq x < 1000$?

Problem 4
It is known that

$$\begin{aligned} a^3b^{10}c^3 + a^2b^{13}c^8 &\equiv 0 \mod 101 \\ a^2b^7c^{10} - a^4b^{12}c^{11} &\equiv 0 \mod 101 \end{aligned}$$

101 is a prime and c is a generator of the multiplicative group. Find logarithms: $\log_c a, \log_c b$.

Problem 5
Given a prime $p = 112233445543$ determine if there exists x, such that

$$x^2 \equiv 22 \mod p$$

(without finding the solution itself). Explain, mention the relevant theorems.

Problem 6
The same message (a 4-digits credit card password) was sent twice from A go B using the same El Gamal setup with $p = 10007$. The El Gamal cipher-texts happened to be

$$(7; 30) \quad , \quad (49; 139).$$

Find the message. Explain!

Hint: $7 \cdot 7 = 49$.

Problem 7
How many roots has the polynomial

$$f(x) = x^{134} + x^{127} + x^7 + 1$$

in $\mathbb{F}_{2^n}$, where $n = 1463$? Explain.

(Remember, the groups is cyclic and $127 + 7 = 134$.)

Problem 8
Count the number of points on the curve

$$y^2 = (x+1)^3$$

over $\mathbb{Z}_p$, $p = 1619$. Explain how you got your answer.