Norges teknisk–naturvitenskapelige universitet
Institutt for dette og hint

Faglig kontakt under eksamen:
Alexei Rudakov, tlf. 73 59 16 95

EKSAMEN I TMA4160 KRYPTOGRAFI

Torsdag 4. desember 2003
Kl. 9-14

Sensur: 4. januar 2004

Hjelpemidler: A

Write carefully, mark the answers, refer to theorems you use, show the logical steps of you solution. Each task is evaluated as a whole, there can be subquestions marked by a, b, c, but they are not separate tasks.

Oppgave 1

It is known that g is a generator for $\mathbb{Z}_p^*$ where $p = 107$ is prime. Given that

$$\begin{cases} a^2 b^{87} + b^{35} c^5 \equiv 0 \\ a^3 b^{18} - b^{23} c^7 \equiv 0 \end{cases} \pmod{107}$$

find discrete logarithms $\log_b a$, $\log_b c$.

Oppgave 2

It is known that $p = 11330087$, is a Sophie Germain prime (or $p = 2q + 1$, where q is prime).

a) Determine if $g_1 = 5$ is a generator for $\mathbb{Z}_p^*$.

b) Determine if $g_2 = 11$ is a generator for $\mathbb{Z}_p^*$.

Explain your reasons.

c) Evaluate probability that a randomly chosen a, $1 < a < (p - 1)$, is a generator for $\mathbb{Z}_p^*$ (up to an error magnitude 0.001).

Oppgave 3
Let $n = p \cdot q$, where $p = 2^{16} + 1$, $q = 2^{127} - 1$ are known to be prime.

a) Write down <u>the definition</u> of the order of an element h of a group G.

b) Explain what is the group we are to think of, when one speaks about " the order of 2 mod n".

c) Find this "order of 2 mod n" for n given above. Explain your reasoning.

Oppgave 4
The RSA encryption/decryption $n = pq$, $y = E(x) = x^e \underline{\text{mod}}\ n$, $z = D(y) = y^d \underline{\text{mod}}\ n$, was used with $p = 3307$, $q = 4409$, $e = 139$. An "expert" said that to find d it is sufficient to solve the system:

$$\begin{cases} d \equiv -5 \pmod{24}, \\ d \equiv 111 \pmod{551}. \end{cases}$$

a) What is your opinion, is the statement of the "expert" correct or wrong?
Provide arguments to prove your position.

b) Find d, chose the value as small as possible.

Oppgave 5
You can use the fact that over $\mathbb{Z}_2$ irreducible polynomials of degree 2 and 3 are:
$x^2 + x + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1.$

a) Determine if $f(x) = x^6 + x^4 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$ or not.

b) Determine if $g(x) = x^6 + x^5 + x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$ or not.

Oppgave 6
An encryption system, stream cipher, was made with the encryption rule $y_i = x_i + c_i$, where the plaintext $\overline{x} = (x_0, x_1, ..., x_n) \in \mathbb{Z}_2^n$, and $\tau = (c_0, c_1, ..., c_N) \in \mathbb{Z}_2^n$ is the key sequence generated by LFSR with the connection polynomial $p(x)$, and this polynomial $p(x)$ is equal to the irreducible one among the polynomials $f(x), g(x)$ of Task 5 above.
It can be calculated that $gcd(f(x), x^{21} - 1) \neq 1$, $gcd(g(x), x^{21} - 1) \neq 1$.
The following plaitext/ciphertext pairs are known:
$(x_{65}, y_{65}) = (0, 0)$, $(x_{84}, y_{84}) = (1, 0)$, $(x_{109}, y_{109}) = (0, 1)$
$(x_{66}, y_{66}) = (0, 1)$, $(x_{85}, y_{85}) = (1, 1)$, $(x_{110}, y_{110}) = (10, 0)$
Break the system: write the recurrence relation and the initial part $c_0, ..., c_5$ of the key sequence.