Final exam in

MATHEMATICAL CRYPTOLOGY

Inst. för Informationsteknologi
Lunds Tekniska Högskola
Dept. of Information Technology
Lund University

March 7, 2005, 9–13

- You are allowed to use a calculator.
- Each solution should be written on a *separate sheet of paper*.
- You must *clearly* show the line of reasoning.
- If any data is lacking, make reasonable assumptions.

Good luck!

Problem 1 Answer each of the following questions using 1- 50 words.

1.1) If N is a product of two primes and the element x has a square root, then how many square roots has it?

1.2) Describe the meaning of a Feistel cipher.

1.3) Describe why ECB mode of operation of a block cipher is not always a good choice.

1.4) What is Kerberos and how does it work (very briefly)?

1.5) Describe the relation between the three problems FACTORING, SQRROOT, RSA problem.

1.6) Describe the baby-step/giant-step method of solving the discrete log problem.

1.7) Explain commitment scheme and give an example of such.

1.8) When does Wiener's attack on RSA work?

1.9) Explain perfect security, semantic security and polynomial security.

1.10) Explain the relation between random oracles and hash functions in the random oracle model.

(20 points)

Problem 2

Consider the elliptic curve $Y^2 = X^3 + X + 3$ defined over $\mathbb{F}_7$. One point on the curve is $P = (4, 6)$. Calculate $[2]P, [3]P, \ldots$ and determine the order of the element P.

Hint: For the curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (char K not 2 or 3), and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, we have $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$. Also if $x_1 \neq x_2$ we set $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$. If $x_1 = x_2$ and $P_2 \neq -P_1$ we set $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $\mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$. Now $P_1 + P_2 = P_3 = (x_3, y_3)$ is given by $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -(\lambda + a_1)x_3 - \mu - a_3$.

(6 points)

Problem 3

Assume that we try to strengthen a block cipher by using it twice with two different n-bit keys k_1, k_2 (in total $2n$ bits),

$$c = E_{k_1}(E_{k_2}(m)).$$

Describe a chosen plaintext attack which requires $O(2^n)$ memory and $O(2^n)$ encryptions/decryptions using E.

(6 points)

Problem 4

Show that if one knows the secret RSA decryption exponent d corresponding to the public key (N, e), then one can efficiently factor N through a Las Vegas algorithm.

(6 points)

Problem 5

In El Gamal encryption, the private key x is an element of a group G. The public key is given by $h = g^x$, where g is a fixed known element.

In encryption of message m, one generates a random ephemeral key k, sets $c_1 = g^k$ and $c_2 = m \cdot h^k$ and output the ciphertext $c = c_1, c_2)$. Describe the decryption process and prove that it always returns the encrypted message m.

(6 points)

Problem 6

Describe a zero-knowledge proof of knowledge of the secret discrete logarithm x of public y with respect to $g \in G$. Give arguments for completeness, soundness and zero-knowledge.

(6 points)