Final exam in

MATHEMATICAL CRYPTOLOGY

August 17, 2006, 14–19

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

- 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 briefly the different operations used in AES (Rijndael).

1.3) Describe CBC mode of operation of a block cipher.

1.4) What is meaning of "nonce" used in many (key distribution) protocols?

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

1.6) Describe Pollard's Rho algorithm for solving the discrete log problem.

1.7) Explain the birthday paradox and its relation to hash functions.

1.8) Give one example of circumstances when a lattice based attack on RSA can work?

1.9) Explain when an encryption scheme is non-malleable.

1.10) Give the definition of an NP complete decision problem.

(20 points)

Problem 2

Consider the elliptic curve $Y^2 = X^3 + 4X + 4$ defined over $\mathbb{F}_7$ and the associated group. Determine the set of points on the curve and determine the order of each element.

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

Consider triple DES but with two keys k_1, k_2 instead of three,

$$c = DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(m))).$$

Describe a chosen plaintext attack which requires roughly 2^{56} memory and roughly 2^{56} encryptions/decryptions using single DES.

(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 ElGamal 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 $c = (_1, c_2)$. Describe the decryption process and prove that it always returns the encrypted message m.

Also prove that assuming that DHP is hard, ElGamal is secure under chosen plaintext attacks (security means it is hard for the adversary, given the ciphertext, to recover the whole of the plaintext). (6 points)

Problem 6

Let $B(m)$ be defined as $B(m) = 0$ if $m < N/2$, otherwise $B(m) = 1$. Show that $B(m)$ is a hard predicate for the RSA problem (defined as $c = m^e \pmod N$).

(6 points)