Final exam in

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

CRYPTOGRAPHY

December 15, 2004, 8–13

- 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

Alice wants to encrypt some English text. She decides that she wants extra protection by encrypting the text first by one cipher and then by a second cipher. If E_K denotes the encryption by the first cipher and $E_{K'}$ denotes the encryption by the second cipher, the encryption process would be as follows.

A sequence of message symbols $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertext symbols $C_1, C_2, \ldots, C_n$ by

$$C_i = E_{K'}(E_K(M_i)), \quad \forall i, 1 \leq i \leq n.$$

a) Determine the unicity distance if the first cipher is a simple substitution cipher and the second cipher is the identity map ($E_{K'}(M_i) = M_i$).

b) Determine the unicity distance if the first cipher is a simple substitution cipher and the second cipher is a Caesar cipher.

Hint: Two keys are different if they represent different mappings from plaintext symbol to ciphertext symbol.

c) If we want to make the unicity distance for the system above even larger than in **a)** and **b)**, suggest what we could do.

(10 points)

Problem 2

b) Find the shortest linear feedback shift register that generates the sequence

$$s = [0, 0, 0, 1, 1]^\infty$$

over $\mathbb{F}_2$.

a) Find the shortest linear feedback shift register that generates the sequence

$$s = (1, 0, 1, 2\alpha, 2\alpha, \alpha + 1, 2)$$

over $\mathbb{F}_{3^2}$, generated by $p(x) = x^2 + x + 2$ and $p(\alpha) = 0$.

(10 points)

Problem 3

a) A Shamir threshold scheme for $n = 5$ participants with threshold $k = 3$ using the public values $x_i = i$ is assumed. All values are assumed to be in $\mathbb{F}_{101}$. Participants 1, 2, and 3 hold the private shares $y_1 = 40$, $y_2 = 50$, and $y_3 = 60$. Help them to reconstruct the secret.

b) In an authentication system the message M and the key K are given as,

$$M = (m_1, m_2), \quad K = (k_1, k_2),$$

where

$$m_1, m_2, k_1, k_2 \in \mathbb{F}_3.$$

The ciphertext C is a 3-tuple generated by

$$C = (m_1, m_2, t),$$

where

$$t = k_1 + m_1 k_1 + m_2 k_2.$$

Find the value of P_I and P_S. Recall that P_S is defined as

$$P_S = \sum P(C) \max_{C' \neq C} P(C' \text{ valid} | C \text{ observed}).$$

(10 points)

Problem 4

Factor the RSA number $n = 44384521$ using the basic form of the Quadratic Sieve algorithm you learned in the first project. The square of the following numbers are B-smooth for some very small B,

$$1883840, 6521874, 13519124, 16006155.$$

Note that factoring n by trial division is not allowed.

(10 points)

Problem 5

Consider the polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^5$.

a) Show that $p(x)$ is irreducible ("primpolynom") over $\mathbb{F}_2$.

b) Determine whether $p(x)$ is primitive ("primitivt polynom") over $\mathbb{F}_2$ or not.

c) Determine the cycle set (“cykelkarakteristiken”) for $p(x)$ defined over $\mathbb{F}_3$.

(10 points)