Final exam in

CRYPTOGRAPHY

December 17, 2003, 8–13

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

We wish to encrypt a memoryless source with alphabet $\mathcal{M} = \{0, 1, 2\}$ and $P(M = 0) = 1/2$, $P(M = 1) = 1/4$, $P(M = 2) = 1/4$. Let the key $K = (K_0, K_1, \ldots, K_l)$, $K_i \in \mathbb{F}_3$, be chosen uniformly from the set of l-tuples. 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

$$C_i = M_i + K_{i \bmod l} \pmod 3, \quad \forall i, 1 \leq i \leq n.$$

a) Determine the unicity distance ("entydighetslängd") when $l = 64$.

b) Find all values of l than give perfect secrecy when $n = 3$.

(10 points)

Problem 2

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

$$s = (1, 0, 4, 3, 0, 3)$$

over $\mathbb{F}_5$.

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

$$s = [1, 0, 4, 3, 0, 3]^{\infty}$$

over $\mathbb{F}_5$.

(10 points)

Problem 3

a) 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

$$t = k_1 + m_1 k_2 + m_2 k_2^2.$$

Find the value of P_I and P_S.
Hint: A polynomial $p(x)$ of degree l has at most l roots.

b) 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 $\mathbb{F}_{97}$. Participant 1, 2, and 3 hold the private shares $y_1 = 44$, $y_2 = 73$, and $y_3 = 28$. Help them to reconstruct the secret.

(10 points)

Problem 4

a) Factor the RSA number $n = 3844384501$ using the knowledge that

$$3117761185^2 \equiv 1 \pmod{3844384501}.$$

b) Prove that the number 31803221 is not a prime number using the hint

$$2^{31803212} \equiv 27696377 \pmod{31803221}.$$

(10 points)

Problem 5 Let $p(x) = x^2 + x + 2$ be an irreducible polynomial over $\mathbb{F}_3$. The field $\mathbb{F}_{3^2}$ is constructed using $p(x)$ with $p(\alpha) = 0$. Consider the polynomial

$$q(x) = x^3 + (\alpha + 1)x^2 + (\alpha + 1)x + 1,$$

over $\mathbb{F}_{3^2}$. Determine the cycle set ("cykelkarakteristiken") for $q(x)$. (10 points)