Final exam in

CRYPTOGRAPHY

December 17, 2002, 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

We wish to encrypt a memoryless source with alphabet $\mathcal{M} = \{0, 1, 2\}$ and $P(M = 0) = 1/2$, $P(M = 1) = p$, $P(M = 2) = 1/2 - p$, $0 \leq p \leq 1/2$. Let the key $K = (K_0, K_1, K_2)$ be chosen uniformly from the set of binary 3-tuples. A sequence of messages $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertexts $C_1, C_2, \ldots, C_n$ by

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

a) Find all values of p that give a unicity distance ("entydighetslängd") larger than 20.

b) Let $p = 0$. Give a new cipher for this source that has an infinite unicity distance.

(10 points)

Problem 2

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

$$s = (1, 0, 4, 3, 2, 4, 0)$$

over $\mathbb{F}_5$.

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

$$s = [1, 0, 4, 3, 2, 4, 0]^{\infty}$$

over $\mathbb{F}_5$.

(10 points)

Problem 3

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

$$M = (m_1, m_2, m_3), \quad K = (k_1, k_2),$$

where

$$m_1, m_2, m_3, k_1, k_2 \in \mathbb{F}_{13}.$$

The ciphertext C is a 4-tuple generated by

$$C = (m_1, m_2, m_3, t),$$

where

$$t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_2^3.$$

a) Find the value of P_I.

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

(10 points)

Problem 4

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

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

b) Show that $p(x)$ is primitive ("primitivt polynom") over $\mathbb{F}_2$.

c) Show that $p(x)$ is reducible (**not** irreducible) over $\mathbb{F}_{2^5}$.

(10 points)

Problem 5

a) Decrypt the following ciphertext, obtained from a Caesar cipher:

WKHSUHVLGHQWZLOOVHQGWKHPRQHB.

b) Decrypt the following ciphertext, obtained from a Transposition cipher ("Transpositionskrypto"):

OYORTETDNSEORTHPOTSUITHGN.

Hint: This is not columnwise transposition.

(10 points)