Final exam in

CRYPTOGRAPHY

December 15, 1998, 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 $P(M=0) = 1/2$, $P(M=1) = 1/4$, $P(M=2) = 1/4$. Let the key $K = (K_0, K_1, \ldots, K_{l-1})$ be chosen uniformly from the set of binary l-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

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

a) Find the smallest value of l for which the unicity distance ("entydighetslängd") is larger than 200.

b) Construct a new cipher for this source that has infinite unicity distance (but a finite key size).

(10 points)

Problem 2

a) Find the shortest LFSR that generates the finite sequence

$$\mathbf{s} = [1, 0, 0, 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha, \alpha + 1],$$

where $\mathbf{s}$ is defined over $\mathbb{F}_8$ using the irreducible polynomial $p(x) = x^3 + x + 1$ and $p(\alpha) = 0$.

b) Show how to implement the LFSR obtained in **a)** using only binary delay units ("D-element") and XOR-gates. Draw a picture!

(10 points)

Problem 3

In an RSA-system the public encryption function is denoted $E(M)$ and the secret decryption function is denoted $D(C)$, where M is the plaintext and C is the ciphertext.

The RSA-system has public parameters $(n, e) = (31897, 19)$.

a) Find $C = E(M)$ if $M = 20000$.

b) Prove that $D(E(M)) = M$ for the case $\gcd(M, n) = 1$.

c) Prove that $D(E(M)) = M$ for the case $\gcd(M, n) \neq 1$. Hint: Use the Chinese remainder theorem.

(10 points)

Problem 4

a) Suppose that in a Shamir Threshold Scheme we have $p = 167$, $k = 3$ and $n = 7$. The public x-coordinates are $x_i = i$, for $1 \leq i \leq 7$. Suppose that $\mathcal{B} = \{P_1, P_4, P_7\}$ pool their shares, which are 3, 13, and 57, respectively. Help them to calculate the secret K.

b) A system providing authentication protection is constructed as follows: The key consists of two parts, $K = (k_1, k_2)$, where $k_i \in \mathbb{F}_{2^{10}}$, $1 \leq i \leq 2$. The plaintext is the 3-tuple $\mathbf{m} = (m_1, m_2, m_3)$ where $m_i \in \mathbb{F}_{2^{10}}$, $1 \leq i \leq 3$. The 3-tuple is associated with a polynomial $m(x)$ defined by $m(x) = m_1 x + m_2 x^2 + m_3 x^3$. The ciphertext $\mathbf{c}$ is now produced as

$$\mathbf{c} = (m_1, m_2, m_3, m(k_1) + k_2).$$

Determine P_I and P_S.

Hint: For any polynomial $p(x)$ over $\mathbb{F}_q$ of degree k there are at most k different elements $\alpha \in \mathbb{F}_q$ for which $p(\alpha) = 0$.

(10 points)

Problem 5

Let $p_1(z) = z^{-6} + z^{-4} + 1$ and $p_2(z) = z^{-7} + z^{-3} + z^{-2} + z^{-1} + 1$ be two polynomials over $\mathbb{F}_2$. Consider the following statements:

a) The polynomial $p_1(z)$ is irreducible ("primpolynom").

b) The LFSR with feedback polynomial $p_1(z)$ has cycle set $1(1) \bigoplus 9(7)$.

c) The LFSR with feedback polynomial $p_1(z)p_2(z)$ has at least nine cycles of length 7.

d) The shortest LFSR generating the sequence $[00000100010101]^\infty$ has feedback polynomial $p_1(z)$.

e) All irreducible polynomials of degree 7 over $\mathbb{F}_2$ are primitive.

Choose for each of the five statements given above one of the following alternatives:

i) Correct — I am uncertain
ii) Wrong — I am uncertain
iii) Correct — I am certain
iv) Wrong — I am certain.

Correct answer according to i) or ii) gives 1 point.
Correct answer according to iii) or iv) gives 2 points.
Erroneous answer according to i) or ii) gives 0 points.
Erroneous answer according to iii) or iv) gives -2 points.

(Only answers are required!)

(10 points)