Final exam in

CRYPTOGRAPHY

December 12, 2000, 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

An instance of the Hill cipher is defined as follows. Let $m \in \mathbb{F}_{2^3}^2$ and let the set of possible keys $\mathcal{K}$ be

$$\mathcal{K} = \{ \text{ all } 2 \times 2 \text{ invertible matrices over } \mathbb{F}_{2^3} \}.$$

The encryption function is $e_K(m) = mK$. Assume that $\mathbb{F}_{2^3}$ is generated by $\pi(x) = x^3 + x + 1$ and $\pi(\alpha) = 0$.

a) Encrypt the plaintext $m = (\alpha, \alpha^2)$ using the key $K = \begin{pmatrix} \alpha^2 & \alpha + 1 \\ \alpha^2 + 1 & 1 \end{pmatrix}$.

b) Explain why $\mathcal{K}$ cannot contain all 2×2 matrices.

c) Find the unicity distance if a source with redundancy $D = 1$ bit per symbol is encrypted.

(10 points)

Problem 2

It is common in different buildings to require a pin code to open certain doors. Usually, the pin code consists of four digits between 0 and 9. So there are 10000 different pin codes possible. If you do not know better, you might think that it is necessary to push a maximum of 40000 digits, or on average 20000 digits, in order to find the correct pin code and open the door.

But this is of course wrong, which is easily seen if you push the sequence "00001" of length 5. You test both pin codes "0000" and "0001". We see that the best we can do is to test a new pin code every time we push a digit (except the first three). This is exactly a de Bruijn sequence over $\mathbb{Z}_{10}$.

Provide an explicit construction of a de Bruijn sequence over $\mathbb{Z}_{10}$ such that the 10003 first digits of the sequence contains every 4-tuple in $\mathbb{Z}_{10}^4$ exactly once!

You must provide values for all the parts in the construction. Furthermore, you must provide the values of the first ten digits in the sequence.

Hint: The polynomial $p(x) = x^4 + x^3 + 2x^2 + x + 2$ is a primitive polynomial over $\mathbb{F}_5$.

(10 points)

Problem 3

a) In an authentication system the message M and the key K are both 2-tuples,

$$M = (M_1, M_2), \quad K = (K_1, K_2),$$

where

$$M_1, M_2, K_1, K_2 \in \mathbb{F}_2.$$

The ciphertext C is a 3-tuple generated by

$$C = (M_1, M_2, K_1 + M_1K_2 + M_2K_2).$$

Find the value of P_I and P_S.

b) A secret key $K \in \mathbb{Z}_{13}$ is shared in a $(3, 6)$ Shamir threshold scheme. The public values are $x_i = i$, for $i = 1, \ldots, 6$. The participants P_1, P_3, P_5 have been given shares 6, 8, and 12, respectively. Help them to determine the secret key K when they pool their shares.

(10 points)

Problem 4

Let $p_1(z) = z^{-3} + z^{-2} + 1$ and $p_2(z) = z^{-3} + 2z^{-2} + z^{-1} + 1$ be feedback polynomials over $\mathbb{F}_3$ for two LFSRs, respectively. Let $\mathbf{s_1}$ and $\mathbf{s_2}$ denote the two output sequences over $\mathbb{F}_3$ from the LFSRs, when both of them are initialized with $(2, 2, 2)$. Consider the following statements:

a) The polynomial $p_2(z)$ is irreducible ("primpolynom").

b) The LFSR with feedback polynomial $p_2(z)$ has cycle set $1(1) \bigoplus 1(26)$.

c) The period of the sequence $\mathbf{s_1}$ is 8.

d) The linear complexity of the sequence $\mathbf{s_1} + \mathbf{s_2}$ is 6.

e) The cycle set for $p_2(z)^{100}$ will contain exactly one cycle of length 26.

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)

Problem 5

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. Let the public parameters of the RSA-system be denoted by (n, e).

a) Find a valid value for the pair (n, e), such that the factors of n are larger than 4004.

b) Give the corresponding secret parameters $(p, q, d, \phi(n))$.

c) Prove the neccessary property $D(E(M)) = M$ for RSA, when $gcd(M, n) = 1$.

(10 points)