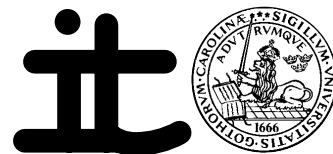


Final exam in

CRYPTOGRAPHY

on December 17, 1994, 14:00 – 19.00



Institutionen för Informationsteori
Lunds Tekniska Högskola
Department of Information Theory
Lund University

Note: During this final exam, you are allowed to use a calculator and the enclosed set of formulas. Each solution should be written on a separate sheet of paper. Show the line of reasoning clearly, and use the methods presented in the course. If any data is lacking, make reasonable presumptions.

Good luck!

Problem 1

We wish to authenticate a message M using a key $\underline{K} = (\alpha_0, \alpha_1)$, where $M, \alpha_i \in GF(3)$. The cryptotext $\underline{C} = (c_0, c_1)$, $c_i \in GF(3)$, is constructed by

$$\underline{C} = (M, \alpha_0 + M\alpha_1).$$

- a) Find P_I for the authentication system, and
- b) find P_S .

(10 points)

Problem 2

The public parameters of an (unsecure) RSA-system are $n = 7081$ and $e = 5113$. Break the system and find the plaintext when the ciphertext $C = 957$.

Hint: $70 < p < 80$.

(10 points)

Problem 3

Find the shortest linear feedback shift register that generates the sequence

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

over $GF(5)$. (Maximum 5 points are given if Massey's algorithm is used.)

(10 points)

Problem 4

Find the cycle set [periodmängden] of

$$C(z) = z^{-7} + 2z^{-6} + z^{-1} + 2$$

over $GF(3)$.

(10 points)

Problem 5

Let a message \underline{M} consist of a sequence of independent binary symbols of plaintext M_1, M_2, \dots, M_l with $P(M_i = 0) = p$ and let the key K , that is chosen once for each message \underline{M} , be a binary variable with $H(K) = 1$. Encrypt using

$$C_i = M_i + K, \quad i = 1, 2, \dots, l,$$

where C_i is binary, and consider the following statements:

- a) If $p = 0.11$ the unicity distance [entydighetslängden] is equal to 4.
- b) If $p = 0.5$ the cryptosystem has perfect secrecy.
- c) If $p = 0.5$ the unicity distance is ∞ .
- d) $H(\underline{M} \mid \underline{C}) \rightarrow 0$ when $l \rightarrow \infty$ for all $p \neq 0.5$.
- e) $H(K \mid \underline{C}) \rightarrow 0$ when $l \rightarrow \infty$ for all $p \neq 0.5$.

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.

(A negative sum counts as zero points!)

(10 points)
