Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

December 16, 2008, 14–19

- 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

Consider the following statements about the polynomial $p(x) = x^3 + x + 1$.

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

b) The polynomial $p(x)$ is irreducible over $\mathbb{F}_3$.

c) The polynomial $p(x)$ is irreducible over $\mathbb{F}_{2^3}$.

d) The polynomial $p(x)$ is a primitive polynomial over $\mathbb{F}_2$.

e) The polynomial $p(x)$ over $\mathbb{F}_2$ has period 3.

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 2

Factor the RSA number $n = 44384521$ using the basic form of the Quadratic Sieve algorithm you learned in the first project. The square of the following numbers are B-smooth for some very small B,

$$1883840, 6521874, 13519124, 16006155.$$

Note that factoring n by trial division is not allowed.

(10 points)

Problem 3

a) Construct a device with a 3 bit memory that produces a full-length sequence over $\mathbb{F}_2$ with period 8. Draw a picture and give the sequence using a starting state of your choice.

b) Determine the length of the shortest linear feedback shift register that generates the periodic sequence in **a)**.

(10 points)

Problem 4

A source producing independent ternary symbols m_i, $i = 0, 1, 2, \ldots$ from the alphabet $\mathbb{F}_3$ is encrypted by a Vigenére cipher to a ciphertext as follows,

$$c_i = m_i + k_{i \bmod t} \mod 3, \quad i = 0, 1, 2, \ldots$$

It is known that the period t of the Vigenére cipher is either 3, 4, or 5. It is also known that plaintext symbols from the source are drawn from the distribution $P(m_i = 0) = 2/3$, $P(m_i = 1) = 1/4$, and $P(m_i = 2) = 1/12$.

Use the idea of ciphertext autocorrelation from the theory of index of coincidence to find the correct period. Then find the (most probable) plaintext and the key. The ciphertext is given as

$$\mathbf{c} = 1201022201\ 2110012022\ 1110122220\ 1210001211\ 2021010112\ 0120020202.$$

(10 points)

Problem 5

a) Compute the unicity distance for the Vigenére cipher and the source in Problem 4, if the period (length of the keyword) would have been 6 and all keywords would have been selected from a uniform distribution.

b) For the same Vigenére cipher but with period 2, the key $\mathbf{k}$ has been shared among 4 participants in a Shamir Threshold scheme defined over $\mathbb{F}_{3^2}$ using $\pi(x) = x^2 + x + 2$ and $\pi(\alpha) = 0$. The threshold is $k = 3$.

Participants 1, 2 and 3 have public values $x_1 = 1$, $x_2 = 2$ and $x_3 = \alpha$. Their secret shares are $y_1 = \alpha$, $y_2 = 0$, and $y_3 = 1$. Help them to find the key $\mathbf{k} \in \mathbb{F}_{3^2}$.

(10 points)