Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

January 14, 2016, 08–13

- 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 two polynomials $P_1(x) = x^3 + 1$ and $P_2(x) = x^2 + 1$.

a) The polynomial $P_1(x)$ is irreducible ("primpolynom") over $\mathbb{F}_2$.

b) The polynomial $P_1(x)$ is irreducible over $\mathbb{F}_3$.

c) The polynomial $P_2(x)$ is irreducible over $\mathbb{F}_{3^2}$.

d) The polynomial $P_2(x)$ over $\mathbb{F}_3$ has period 2.

e) If $P_1(x)$ defined over $\mathbb{F}_3$ is used as a connection polynomial for an LFSR, then the cycle set contains a cycle of length 6.

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

We wish to encrypt a source with alphabet $\mathbb{Z}_4$ having the very special property that $M_{i+1} = M_i$ for $i = 0, 2, 4, \ldots$, i.e., all message symbols with odd index is a copy of the previous message symbol. For i even we have $P(M = i) = 1/4$, $i \in \mathbb{Z}_4$.

The key $\mathbf{K} = (K_0, K_1, \ldots, K_{l-1})$ is chosen uniformly from the set of l-tuples ($K_i \in \mathbb{Z}_4$). A sequence of message symbols $\mathbf{M} = (M_0, M_1, \ldots, M_{n-1})$ is encrypted to a sequence of ciphertext symbols $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ by

$$C_i = M_i + K_{i \bmod l} \mod 4, \quad 0 \leq i \leq n-1.$$

a) When $l = 64$, compute the unicity distance N_0 according to the formula.

(4 points)

b) Determine, for any l, exactly how many ciphertext symbols (n) we need to observe in order to uniquely determine the key.

(4 points)

c) For this particular source, can you propose a new encryption scheme using l key symbols from $\mathbb{Z}_4$ such that we have perfect secrecy and still $l < n$ when $n > 1$?

(2 points)

Problem 3

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

$$s = [1, 1, 0]^\infty + [1, 0]^\infty$$

over $\mathbb{F}_2$. Use the D-transform and not the BM algorithm.

(4 points)

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

$$s = (1, \alpha, \alpha^2, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + 1, \alpha^3 + \alpha^2, 1)$$

over $\mathbb{F}_{2^4}$, generated by $p(x) = x^4 + x + 1$ and $p(\alpha) = 0$.

(6 points)

Problem 4

Factor the RSA number $n = 21769199$ using the basic form of the Quadratic Sieve algorithm you learned in the first project. The square of most of the following numbers are B-smooth for some very small B,

$$6038438, 10816226, 13211263, 4653427, 21591962, 10795981.$$

Note that factoring n by trial division is not allowed.

(10 points)

Problem 5

We will investigate some problems with different ways of doing authentication.

a) In an authentication code we can only send a single message, then we need to change the key. Assume that Alice makes a mistake and sends two messages using the same key.

The code maps a source message (s_1, s_2), $s_1, s_2 \in \mathbb{F}_{101}$ into an authenticated channel message M. They are using an authentication code, where the key (encoding rule) E is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_{101}$. The transmitted message is $M = (s_1, s_2, t)$, where $t = e_1 + s_1 e_2 + s_2 e_2^2$. Eve observes the two messages $M = (0, 0, 10)$ and $M' = (1, 0, 12)$. Find another message that maximizes her chances of getting this other message accepted instead of M'.

(4 points)

b) CBC-MAC is a technique for constructing a MAC from a block cipher. The message is $(m_0, m_1, \ldots m_{l-1})$, where each m_i is a b-bit block. We compute $c_i = E_K(m_i + c_{i-1})$, for $i = 0, 1, \ldots, l-1$ and $c_{-1} = 0$. Here $E_K()$ is the block cipher. The MAC is the last computed output, i.e., $\text{MAC} = c_{l-1}$ and we transmit $(m_0, m_1, \ldots m_{l-1}, \text{MAC})$.

This construction is regarded secure if all messages have the same length, but insecure if we allow messages of different length. Show how to break this construction (how an observed message can be substituted for another message) in the latter case (l may be different for different messages). Draw a picture of the construction.

(4 points)

c) Yet another way of constructing MACs is by using hash functions. A secure way is the HMAC construction, whereas simpler constructions may be insecure.

Show why the simple $MAC_k(\mathbf{m}) = h(k||\mathbf{m})$ is not a good construction, assuming a Merkle-Damgård hash function construction and variable length messages. Here $\mathbf{m}$ is the message, $||$ denotes string concatenation, and k is the key and h is the hash function.

(2 points)