Final exam in

CRYPTOGRAPHY

Dept. of Electrical and Information Technology
Lund University

December 14, 2009, 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

Alice wants to encrypt some English text. She decides to encrypt the text with a simple substitution cipher, denoted E_K. The encryption process would be as follows. A sequence of letters $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertext symbols $C_1, C_2, \ldots, C_n$ by

$$C_i = E_K(M_i), \quad \forall i, 1 \leq i \leq n.$$

a) Write down one possible key for a simple substitution cipher.

b) Determine the unicity distance.

c) Determine the plaintext if the ciphertext is

QSPA PDLP QDBC PEFC QSPG BFPH IPLP JKMP FQBQ SPGE FDEN NPCE FCH .

Hints: Two words present in the plaintext are GIVEN and CALLED. Some repeating blocks are also underlined.

(10 points)

Problem 2

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

$$s = [1, 1, 0, 1, 2, 2, 0, 2]^{\infty}$$

over $\mathbb{F}_3$.

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

$$s = (1, 1, 1, 0, \alpha, \alpha^2 + 1, \alpha^3 + \alpha^2)$$

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

(10 points)

Problem 3

Consider the following statements about the polynomial $p(x) = x^4 + x^2 + 1$.

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 $\mathbb{F}_{2^{30}}$.

d) The polynomial $p(x)$ is a product of four different polynomials of degree one over $\mathbb{F}_7$.

e) The polynomial $p(x)$ over $\mathbb{F}_2$ has period 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 4

a) Find an irreducible polynomial $p(x)$ over $\mathbb{F}_{17}[x]$ that can be used to construct the finite field with 17^2 elements.

b) Consider a Shamir Threshold scheme with 5 participants and $k = 2$ for the secret $K \in \mathbb{F}_{17^2}$.

Participants 1 and 2 have public values $x_1 = \alpha + 1$, $x_2 = 2\alpha + 2$, where $p(\alpha) = 0$ and $p(x)$ is your polynomial in a). Their secret shares are $y_1 = 3\alpha + 14$, $y_2 = 1$. Help them to find the secret key K.

(10 points)

Problem 5

a) Factor the RSA number $n = 3844384501$ using the knowledge that

$$31124754^2 \equiv 4095^2 \pmod{3844384501}.$$

b) Prove that for RSA, with encryption $E(M) = M^e \pmod{n}$ and decryption $D(C) = C^d \pmod{n}$, we have necessary relation

$$D(E(M)) = M, \forall M \in \mathbb{Z}_n.$$

(10 points)