Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

December 16, 2011, 8–13

- 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 polynomial $P(D) = D^4 + D^2 + 1$.

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

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

c) The polynomial $P(D)$ is irreducible over $\mathbb{F}_{2^{31}}$.

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

e) The polynomial $P(D)$ 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 2

Factor the RSA number $n = 44370047$ using what you learned about the basic Quadratic Sieve algorithm in the first project. Use the information you get from squaring (modulo the RSA number) the following numbers, which are B-smooth for some small B,

$$33965, 2145407, 19416874, 15213395.$$

Note that factoring n by trial division is not allowed.

(10 points)

Problem 3

a) Consider a Shamir threshold scheme for $n = 30$ participants with threshold $k = 3$ using the public values $x_i = i$. All values are assumed to be in $\mathbb{F}_{37}$. Assume that it is known to participant 2, holding the private share $y_2 = 13$, that the secret is $K = 1$. He also knows that the private share of participant 3 is $y_3 = 3$.

Help participant 2 to determine the private share of participant 29.

b) In an authentication system, Alice would like to send the source state S given as $S = (s_1, s_2)$, where $s_i \in \mathbb{F}_{101}$, $i = 1, 2$.

In a good authentication code, the key (encoding rule) E could be given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_{101}$. The transmitted message M is then a 3-tuple generated as $M = (s_1, s_2, t)$, where

$$t = e_1 + s_1 e_2 + s_2 e_2^2.$$

However, Alice and Bob have tried to reduce the key size and is using a key of the form $E = (e_1)$, $e_1 \in \mathbb{F}_{101}$ and is generating the tag t as

$$t = e_1 + s_1 e_1 + s_2 e_1^2.$$

Help Eve to do one of the best possible substitution attacks, when observing the message

$$M = (1, 0, 13).$$

(10 points)

Problem 4

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

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

in $\mathbb{F}_3$.

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

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

in $\mathbb{F}_{2^4}$, generated by $p(x) = x^4 + x^3 + x^2 + x + 1$ and $p(\alpha) = 0$.

c) Find a shortest linear feedback shift register in $\mathbb{F}_{47}$ that generates a sequence containing all nonzero elements in $\mathbb{F}_{47}$.

(10 points)

Problem 5

In an RSA-system the public encryption function is $C = M^e \bmod n$ and the secret decryption function is $M = C^d \bmod n$, where M is the plaintext and C is the ciphertext. Let the public parameters of the RSA-system be $n = 4967299$ and $e = 5$.

a) Show how you can compute p and q knowing that $\phi(n) = 4961736$.

b) Find the secret decryption exponent d using the knowledge of the prime factors [if you did not solve a), use that $p = 1117$].

c) Compute the ciphertext if the plaintext is $M = 4967298$.

d) Assume that we append a *digital signature* S to message M, using RSA, by

$$S = M^d \bmod n.$$

Assume that Alice signed and sent two messages (M_1, S_1) and (M_2, S_2). Show how Eve can obtain a signature on a new message (not $0, 1, -1$) that Alice did not sign. Also, explain how to improve the security of this signature scheme.

(10 points)