Final exam in

CRYPTOGRAPHY

Dept. of Electrical and Information Technology
Lund University

January 15, 2015, 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

We wish to encrypt a memoryless source with alphabet $\mathbb{Z}_3$ and $P(M=0)=1/2$, $P(M=1)=P(M=2)=1/4$. The key $\mathbf{K}=(K_0,K_1,\ldots,K_{l-1})$ is chosen uniformly from the set of ternary l-tuples ($K_i \in \mathbb{Z}_3$). 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

$$C_i = M_i + K_{i \bmod l} \mod 3, \quad 0 \le i \le n-1.$$

Consider the following statements:

a) When $l=64$ the unicity distance N_0 is in the interval $700 < N_0 < 800$.

b) $H(\mathbf{K}|\mathbf{C}) = H(\mathbf{M}|\mathbf{C})$ when $l=n$.

c) When $l=n$ the system has perfect secrecy.

d) When l is fixed, it is possible to have perfect secrecy for any n if the source sequence is compressed to zero redundancy ($D=0$) before encryption.

e) Let $l=2$ and $n=200000$. In *odd* positions, $\mathbf{C}$ contains 25041 zeros, 50129 ones, and 24830 occurrences of the symbol 2. The most probable value for K_1 is $K_1=1$.

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

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

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

over $\mathbb{F}_2$.

(4 points)

b) 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 $p(\alpha) = 0$.

(6 points)

Problem 3

It is common in different buildings to require a pin code to open certain doors. In our case, the pin code consists of four integer symbols between 0 and 5. So there are 6^4 different pin codes possible. You would like to test all pin code combinations by pushing symbols according to a sequence of minimum length.

Provide an explicit construction of such a (de Bruijn) sequence over $\mathbb{Z}_6$ with the property that the $6^4 + 3$ first digits of the sequence contains every 4-tuple in $\mathbb{Z}_6^4$ exactly once!

You must provide an explicit description for all the parts in your construction and draw a picture! Furthermore, give the values of the first ten symbols in your sequence.

Hint: One of the polynomials $x^4 + x^3 + c$, $c \in \mathbb{F}_3$ is a primitive polynomial over $\mathbb{F}_3$.

(10 points)

Problem 4

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 participant 2 holds the private share y_2, participant 3 holds the private share y_3, and participant 27 holds the private share y_{27}. Show that $K = f_{\text{lin}}(y_2, y_3, y_{27})$, where f_{lin} is a linear function, and derive its value.

(5 points)

b) In an authentication system, Alice would like to send a source message (s_1, s_2), $s_1, s_2 \in \mathbb{F}_{101}$ to Bob in 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 message $M = (0, 0, 10)$. Find another message that maximizes her chances of getting this other message accepted instead of M.

(5 points)

Problem 5

In an RSA cryptosystem 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 denoted (n, e), where $n = pq$.

a) Show a few steps of a probabilistic primality test that asserts that $p = 1009$ is a (probable) prime.

(2 points)

b) Then pick the prime $q = 113$ and form the RSA public keys $(n = 114017, e = 5)$. Give the secret parameters d and $\phi(n)$ in the RSA cryptosystem.

(2 points)

c) Show the steps of calculating the ciphertext $C = M^5 \bmod n$ when encrypting the plaintext $M = 123$ **WITHOUT** using a calculator. (You may use your calculator to verify your result)

(2 points)

d) Try to find arguments proving that if Eve knows d in an RSA system with public keys (n, e), then she most likely can compute p and q.

(4 points)