Final exam in

CRYPTOGRAPHY

Inst för Informationsteknologi
Lunds Tekniska Högskola
Dept of Information Technology
Lund University

on December 16, 1996, 14:00 – 19.00

Note: During this final exam, you are allowed to use a calculator and the enclosed set of formulas. Each solution should be written on a separate sheet of paper. Show the line of reasoning clearly, and use the methods presented in the course. If any data is lacking, make reasonable presumptions.

Good luck!

Problem 1

a) We wish to encrypt a memoryless source with alphabet $\mathcal{M} = \mathbb{Z}_{17}$, $P(M = 0) = 1/2$, and $P(M = i) = 1/32$, $1 \leq i \leq 16$ for $M \in \mathcal{M}$. Let the key K be chosen uniformly from $\mathbb{Z}_{17}$. A sequence of messages $M_1, M_2, \ldots$ taken from $\mathcal{M}$ is encrypted to a sequence of ciphertexts $C_1, C_2, \ldots$ by

$$C_i = M_i + K \pmod{17}, \quad i \geq 1.$$

Determine the unicity distance (”entydighetslängden”).

b) Five users share the above key $K \in \mathbb{Z}_{17}$ in a secret sharing scheme using Shamir's (k, n)-threshold scheme, where $k = 3$. Find the value of K if the share for user 1 is 7, the share for user 2 is 11, the share for user 3 is 0, and the public information for user i is $x_i = i$.

(10 points)

Problem 2

Let $p_1(x) = x^4 + x^2 + 1$ and $p_2(x) = x^7 + x^3 + x^2 + x + 1$ be two polynomials over $\mathbb{F}_2$. Consider the following statements:

a) The polynomial $p_1(x)$ is irreducible ("primpolynom").

b) The LFSR with feedback polynomial $p_1(x)$ has at least one cycle of length 2.

c) The LFSR with feedback polynomial $p_1(x)p_2(x)$ has at least one cycle of length 3.

d) The shortest LFSR generating the sequence $[000101]^\infty$ has feedback polynomial $p_1(x)$.

e) The polynomial $p_2(x)$ is primitive.

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 3

A sequence of plaintext symbols $M_1, M_2, \ldots$ is encrypted to a sequence of ciphertext symbols $C_1, C_2, \ldots$ by

$$C_i = M_i + K_i, \quad i \geq 1,$$

where $M_i, C_i, K_i \in \mathbb{F}_{5^2}$. The field $\mathbb{F}_{5^2}$ is generated by the primitive polynomial $p(x) = x^2 + 4x + 2$ over $\mathbb{F}_5$. Furthermore, it is known that the key sequence $K_1, K_2, \ldots$ is generated by a LFSR over $\mathbb{F}_{5^2}$ with a length less than 4.

The plaintext symbols are english letters, and they are associated with $\mathbb{F}_{5^2}$ in the following way: A = 0, B = 1, C = α, D = α^2, ..., H = α^6, I = J = α^7, K = α^8, ..., Z = α^{23}.

You have observed the ciphertext `RTZDDDVAZUSSE`, a message in english. You have also been informed that the first five letters in the plaintext are `YOUZS`.

Find a LFSR that generate the key sequence $K_1, K_2, \ldots$.

(10 points)

Problem 4

An RSA cryptosystem has open parameters n, e and trapdoor parameters $d, p, q, \phi(n)$, where p, q are primes and $ed = 1 \pmod{\phi(n)}$. The encryption function is denoted $E_K()$ and the decryption function is denoted $D_K()$.

a) Show that $D_K(E_K(M)) = M$, when M is not divisible by p or q.

b) In fact, $D_K(E_K(M)) = M$ even if M is divisible by p or q. Verify this for the particular example $n = 187$, $e = 3$, and $M = 22$.

c) Determine how many numbers in $\{0, 1, \ldots, \phi(n) - 1\}$ that are possible values for e if $p = 2p_1 + 1$ and $q = 2q_1 + 1$, where p_1 and q_1 are primes.

d) The security of RSA is based on the intractability of factoring n. Show that calculating $\phi(n)$ has the same complexity as factoring n, i.e., show that if we can calculate $\phi(n)$ then we can factor n and vice versa.

(10 points)

Problem 5

On the next page you find a description of "Toy-DES", a DES-like block cipher.

a) Encrypt the plaintext 00000000 with key 00000001 using "Toy-DES".

b) Explain how the decryption process should be done in "Toy-DES" and show formally that it works.

c) You have observed the plaintext/ciphertext pairs given below, encrypted by "Toy-DES" with unkown key. Calculate one input x-or and the corresponding output x-or for the S-box. Then explain in words how this gives you some information about the key K.

plaintext	ciphertext
00000000	00111010
00010000	10110000

(10 points)

Description of "Toy-DES": "Toy-DES" has an 8-bit input x_0, an 8-bit output, and an 8-bit key K, where the last bit is a parity bit (odd parity). The block cipher has 3 rounds as follows.

1. The plaintext x_0 is divided in two parts, $x_0 = L_0R_0$, where L_0 is the first 4 (leftmost) bits and R_0 is the 4 last (rightmost) bits.
2. A certain function with start value x_0 is iterated 3 times. If $x_i = L_iR_i$, we compute L_iR_i according to the following iteration:
$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{aligned}$$
where $\oplus$ denotes bitwise addition of the two bitstrings.
3. Finally, the ciphertext is (R_3L_3). Note the reversed order of L_3 and R_3.

We now describe the function f. If we write $f(R_x, K_x)$, then R_x is of length 4 and K_x is of length 6. The function $f(R_x, K_x)$ returns a bitstring of length 4, which is obtained by executing the following steps:

1. R_x is expanded to a bitstring of length 6 using a fixed expansion function E.
2. Compute $B = E(R_x) \oplus K_x$.
3. The next step uses an *S-box* S, which is a fixed 4×16 array whose entries are from the integers $0 - 15$. Given a 6-bit string $B = b_1b_2b_3b_4b_5b_6$, we compute $S(B)$ as follows. The two bits b_1b_6 determine the binary representation of a row r of S, $0 \leq r \leq 3$, and the four bits $b_2b_3b_4b_5$ determine the binary representation of a column c of S, $0 \leq c \leq 15$. Then $S(B)$ is defined to be the entry in row r and column c, written in a binary representation as a 4-bit string. In this fashion, we compute $C = S(B)$.
4. The bitstring C obtained from the previous step is defined to be $f(R_x, K_x)$.

The expansion function E is specified by the following table:

$$\mathrm{E} = \begin{bmatrix} 1 & 2 & 3 & 4 & 1 & 2 \end{bmatrix}$$

The S-box is as follows:

$$S = \begin{bmatrix} 14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\ 15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{bmatrix}$$

The partial keys K_i are obtained from K by selecting the following bits:

$$K_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}, \quad K_2 = \begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix}, \quad K_3 = \begin{bmatrix} 3 & 4 & 5 & 6 & 7 & 1 \end{bmatrix}$$

Note: Compared with original DES, the IP and P permutations have been removed.