Final exam in

CRYPTOGRAPHY

December 13, 2006, 8–13

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

- 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

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

over $\mathbb{F}_3$.

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

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

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

(10 points)

Problem 3

a) A Shamir threshold scheme for $n = 6$ participants with threshold $k = 3$ using the public values $x_i = i$ is assumed. All values are assumed to be in $\mathbb{F}_{101}$. Participants 1, 4, and 6 hold the private shares $y_1 = 34$, $y_4 = 45$, and $y_6 = 56$. Help them to reconstruct the secret.

b) In an authentication system, Alice would like to send the source state S given as $S = (s_1, s_2)$, where $s_1, s_2 \in \mathbb{F}_5$. The key (encoding rule) E is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_5$. The transmitted message M is a 3-tuple generated as $M = (s_1, s_2, t)$, where

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

Find the value of P_I and P_S.

Hint: Recall that P_S is defined as

$$P_S = \max_{M', MM' \neq M} P(M' \text{ valid} | M \text{ observed}).$$

(10 points)

Problem 4

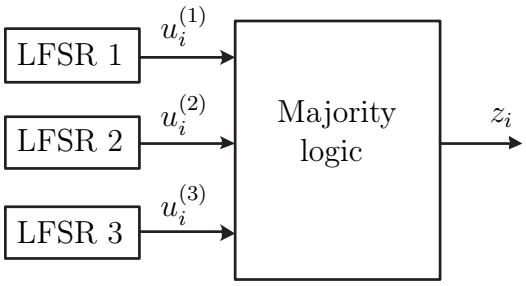

Figure 1: The keystream generator.

Alice encrypts her plaintext using a simple stream cipher, built as in the figure above. The keystream symbol is determined from the output of the LFSRs in the following way. If two or three output symbols from the LFSRs are one, the keystream symbol will be one, otherwise it will be zero. The secret key K is the initial state of the three LFSRs. Hence, we can write the key as a 3-tuple, $K = (K_1, K_2, K_3)$, where K_i is the initial state of the i^{th} LFSR. The connection polynomials for the different LFSRs are $C_1(D) = 1 + D + D^4$, $C_2(D) = 1 + D + D^3$ and $C_3(D) = 1 + D + D^2$.

Determine the key (initial states) when it is known that the keystream output is

$$\mathbf{z} = 0011\ 1110\ 1011\ 0110\ 1111\ 1001\ 0110\ 0101\ 1011$$

(10 points)

Problem 5

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

$$2416766684^2 \equiv 39^2 \pmod{3844384501}.$$

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)