Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

December 12, 2007, 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

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

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

over $\mathbb{F}_2$.

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

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

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

(10 points)

Problem 2

a) A Shamir threshold scheme for $n = 7$ 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, 3, and 7 hold the private shares $y_1 = 1$, $y_3 = 10$, and $y_7 = 100$. Help them to reconstruct the secret.

b) In an authentication system, Alice would like to send the source state S given as $S = (s_1, s_2, s_3)$, where $s_i \in \mathbb{F}_3$, $i = 1, 2, 3$. The key (encoding rule) E is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_3$. The transmitted message M is a 4-tuple generated as $M = (s_1, s_2, s_3, t)$, where

$$t = e_1 + s_1 e_2 + s_2 e_2^2 + s_3 e_2^3.$$

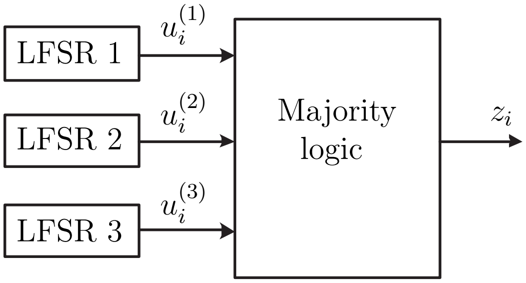
Find the values of P_I and P_S.

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 3



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 4

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

$$989148867^2 \equiv 78^2 \pmod{3844384501}.$$

b) For RSA, with encryption $E(M) = M^e \bmod n$ and decryption $D(C) = C^d \bmod n$, let $e = 7$ and $n = 24820049 = 5507 \cdot 4507$. Calculate the secret decryption exponent d and decrypt $C = 13345349$.

(10 points)

Problem 5

Alice wants to encrypt a string of bits. She decides to encrypt using an LFSR as a generator in a stream cipher. However, she knows that just using an LFSR is a bad choice, so she makes a modification. *She only uses every third bit of the LFSR sequence.*

The encryption process would then be as follows. A sequence of bits $\mathbf{m} = m_1, m_2, \ldots, m_n$ is encrypted to a sequence of ciphertext symbols $\mathbf{c} = c_1, c_2, \ldots, c_n$ by

$$c_i = m_i + s'_i, \quad \forall i, 1 \leq i \leq n,$$

where $\mathbf{s}' = s'_1, s'_2, \ldots$ is obtained from the binary LFSR sequence $\mathbf{s} = s_1, s_2, \ldots$ by $s'_i = s_{3i}$, $i = 1, 2, \ldots$. Finally, $\mathbf{s}$ is generated by a length 5 LFSR with connection polynomial $C(D) = 1 + D^2 + D^5$.

Eve observed the ciphertext $\mathbf{c} = 0, 1, 1, 1, 1, 1, 0, 1, 0, 1$. Also, she knows that the plaintext starts as $1, 1, 1, 1, 1, \ldots$, i.e.,

$$\mathbf{m} = 1, 1, 1, 1, 1, m_6, m_7, m_8, m_9, m_{10}.$$

Find the remaining plaintext bits.

(10 points)