Final exam in

CRYPTOGRAPHY

December 14, 2005, 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 sequence of independent *decimal digits* and send to Bob. Let E_K denote the encryption function operating on decimal digits. A sequence of decimal digits $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertext symbols $C_1, C_2, \ldots, C_n$, $C_i \in \mathbb{Z}_{10}$ by

$$C_i = E_K(M_i), \quad \forall i, 1 \leq i \leq n.$$

a) Determine which of the following mappings that are possible encryption functions: $E_K(M) = M$, $E_K(M) = K$, $E_K(M) = M + K$, $E_K(M) = M \cdot K$, $E_K(M) = M^{K+1}$, if $M, K \in \mathbb{Z}_{10}$.

b) Determine the unicity distance if the cipher is a simple substitution cipher and $P(M = 0) = P(M = 1) = 4 \cdot P(M = 2)$, together with $P(M = 2) = P(M = 3) = \cdots = P(M = 8) = P(M = 9)$.

(10 points)

Problem 2

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

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

over $\mathbb{F}_3$.

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

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

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

(10 points)

Problem 3

a) A Shamir threshold scheme for $n = 5$ participants with threshold $k = 3$ using the public values $x_i = i$ is assumed. All values are assumed to be in $\mathbb{F}_{17}$. Participants 1, 2, and 3 hold the private shares $y_1 = 4$, $y_2 = 5$, and $y_3 = 6$. Help them to reconstruct the secret K.

b) Prove the Lagrange interpolation formula given among the formulas in the appendix and then argue that the reconstruction of the secret K in an (n, k)-threshold scheme can be done by the following expression,

$$K = \sum_{i=1}^{k} y_i \prod_{1 \le j \le k, j \ne i} \frac{x_j}{x_j - x_i}.$$

(10 points)

Problem 4

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 $n = 24820049$ and $e = 5$.

a) Find the secret decryption exponent d using the knowledge that one of the prime factors is $p = 4507$.

b) Decrypt the ciphertext $C = 100000$.

c) Assume that we would like to append a *digital signature* to a message M. Explain how this is done using RSA as a digital signature scheme.

d) Explain how a *hash function* is used together with a digital signature scheme as in **c)**. What are the properties of a collision-free hash function?

(10 points)

Problem 5

Consider the polynomial $p(x) = 1 + x^4 + x^5$ defined over $\mathbb{F}_3$.

a) Determine the cycle set ("cykelkarakteristiken") for $p(x)$.

b) Alice makes a bad choice and uses a LFSR with connection polynomial $p(x)$ as generator in a stream cipher. Bob intercepts the ciphertext $\mathbf{C} = (0, 0, 0, 0, 0, 0, 2, 0, 2, 0, 2)$. Bob also knows that the plaintext is $M_i = 0$ when i is even, i.e., $i = 0, 2, 4, 6, 8, 10$. Help Bob to find the key, equivalent to the initial state of the LFSR.

(10 points)