Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

December 15, 2010, 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

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 (allow unique decryption): $E_K(M) = M$, $E_K(M) = K$, $E_K(M) = M + K$, $E_K(M) = M \cdot K$, $E_K(M) = M^{K+1}$, $E_K(M) = (M + K)^2$, if $M, K \in \mathbb{Z}_{10}$.

b) Determine the unicity distance if the cipher would be a Caesar cipher, where

$$P(M = 0) = P(M = 1) = \cdots = P(M = 5) = 1/8,$$

and

$$P(M = 6) = P(M = 7) = \cdots = P(M = 9).$$

(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 $S = (s_1, s_2)$, where $s_i \in \mathbb{F}_3$, $i = 1, 2$. 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

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

Find the value of 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

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

$$s = (0, 1, 2, 0, 1, 2, 0, 2)$$

over $\mathbb{F}_3$.

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

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

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

(10 points)

Problem 4

a) Find an irreducible polynomial $p(x)$ over $\mathbb{F}_{11}[x]$ that can be used to construct the finite field with 11^3 elements.

b) Construct a device with minimal memory that produces a sequence over $\mathbb{F}_{11}$ with period 11^3. Explain the device in detail, draw a picture and give the first 5 symbols of the sequence using a starting state of your choice.

(10 points)

Problem 5

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 why 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)