Final exam in

CRYPTOGRAPHY

Dept. of Electrical and Information Technology Lund University

December 21, 2012, 14–19

- 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 is going to construct a stream cipher that uses LFSRs and Bob gave her two polynomials from $\mathbb{F}_3[D]$,

$$C_1(D) = D^3 + 1, \quad C_2(D) = D^3 + 2D + 1,$$

to use as connection polynomials for length 3 LFSRs. Consider the following statements.

a) The polynomial $C_1(D)$ is irreducible ("primpolynom") over $\mathbb{F}_3$.

b) The polynomial $C_2(D)$ is irreducible over $\mathbb{F}_3$.

c) The sequences over $\mathbb{F}_3$ produced by connection polynomial $C_1(D)$ has a cycle set including three cycles of length 8.

d) Let $s_t, t \geq 0$ denote the sequence over $\mathbb{F}_3$ produced by connection polynomial $C_2(D)$ and a nonzero starting state. Then $|\{(s_t, s_{t+1}, s_{t+2}) \in \mathbb{F}_3^3 : t \geq 0\}| = 27$.

e) The linear complexity of the sequence $[1, 2]^\infty$ over $\mathbb{F}_3$ is 2.

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 2

An instance of the classic Hill cipher is defined as follows. Let $m \in \mathbb{F}_{2^3}^2$ and let the set of possible keys $\mathcal{K}$ be

$$\mathcal{K} = \{\text{ all } 2 \times 2 \text{ invertible matrices over } \mathbb{F}_{2^3}\}.$$

The encryption function is $e_K(m) = mK$. Assume that $\mathbb{F}_{2^3}$ is generated by $\pi(x) = x^3 + x + 1$ and $\pi(\alpha) = 0$.

a) Encrypt the plaintext $m = (1 + \alpha, \alpha^2)$ using the key $K = \begin{pmatrix} \alpha^2 & \alpha + 1 \\ \alpha^2 + 1 & 1 \end{pmatrix}$.

b) Explain why $\mathcal{K}$ cannot contain all 2×2 matrices.

c) A source outputs all *nonzero* symbols in $\mathbb{F}_{2^3}$ with equal probability. Find the unicity distance if the source is encrypted using the Hill cipher above.

d) Suggest a cipher that achieves infinite unicity distance for the source.

(10 points)

Problem 3

a) Consider a Shamir threshold scheme for $n = 30$ participants with threshold $k = 3$ using the public values $x_i = i$. All values are assumed to be in $\mathbb{F}_{37}$. Assume that participant 2 holds the private share $y_2 = 13$, participant 3 holds the private share $y_3 = 3$, and participant 27 holds the private share $y_{27} = 11$. Help the three participants to restore the shared secret K.

b) In an authentication system, Alice would like to send a source message $S \in \mathbb{F}_{101}$ to Bob.

They use an authentication code, where the key (encoding rule) E is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_{101}$. The transmitted message M is then $M = (S, t)$, where

$$t = e_1 + Se_2.$$

Prove that $P_S = \frac{1}{101}$.

(10 points)

Problem 4

It is known that Alice has two images I_1 and I_2 and will send one of them encrypted to Bob. She uses a block cipher of block length 32 bits and a key of size 80 bits. Assume that image I_1 starts with two zero blocks, followed by blocks with known randomly generated values, $I_1 = (0, 0, x_2, x_3, \ldots)$, $x_i \in \mathbb{F}_2^{32}$. Similarly, I_2 starts with the two blocks $0, 1$, followed by blocks with known randomly generated values, $I_2 = (0, 1, y_2, y_3, \ldots)$, $y_i \in \mathbb{F}_2^{32}$. Both images are of the same length, which is 2^{17} blocks.

a) Explain why ECB mode (Electronic codebook mode) is not a good choice for Alice in this case.

b) Explain a better way to do the encryption by explaining CBC mode as the mode of operation for encryption. Explain also how decryption is done.

c) Eve observes a transmitted ciphertext encrypted as in **b)** using a good block cipher. Show an attack where she can determine which image was sent as plaintext. The attack should succeed with probability > 0.5 and should run in seconds (ruling out exhaustive key search). [If you did not solve **b)**, you can instead use counter mode]

(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 denoted (n, e), where $n = pq$.

a) Find a valid value for the pair (n, e) such that each prime is larger than 1000.

b) Give the corresponding secret parameters $(p, q, d, \phi(n))$.

c) Decrypt the ciphertext $C = 2$ in your system.

d) Assume that we append a *digital signature* S to a message M, using RSA, by

$$S = M^d \bmod n.$$

Assume that Alice signed and sent a message (M, S). Show how this signed message can be used to construct other signed messages (not $0, 1, -1$) that Alice did not sign. How do we modify this scheme to overcome the problem?

(10 points)