# Final exam in

# CRYPTOGRAPHY

**Dept. of Electrical and Information Technology**
**Lund University**

## December 19, 2013, 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 has two polynomials from $\mathbb{F}_3[D]$,

$$C_1(D) = D^4 + D^2 + 1, \quad C_2(D) = 2D^2 + 2D + 1,$$

to use as connection polynomials for two LFSRs over $\mathbb{F}_3$ generating sequences denoted $\mathbf{s_1}$ and $\mathbf{s_2}$, respectively. 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)** If $\mathbf{s_2}$ is nonzero, it has period 8.

**d)** The cycle set for the connection polynomial $C_1(D)$ includes three different cycles of length 1.

**e)** The linear complexity of the sequence $\mathbf{s_1} + \mathbf{s_2}$ is always smaller than or equal to 6.

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 $m \in \mathbb{F}_{2^4}^2$ and let the set of possible keys $\mathcal{K}$ be

$$\mathcal{K} = \{ \text{ all } 2 \times 2 \text{ invertible matrices over } \mathbb{F}_{2^4} \}.$$

The encryption function is $e_K(m) = mK$. Assume that $\mathbb{F}_{2^4}$ is generated by $\pi(x) = x^4 + x + 1$ and $\pi(\alpha) = 0$.

**a)** Encrypt the plaintext $m = (1 + \alpha, \alpha^2)$ using the key $K = \begin{pmatrix} \alpha^3 & \alpha^2 + 1 \\ \alpha^2 + 1 & 1 \end{pmatrix}$.

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

**c)** A (uniform) source outputs binary symbols that are mapped directly to the elements $\{0, 1\}$ in $\mathbb{F}_{2^4}$ (i.e. only two of the 16 elements in $\mathbb{F}_{2^4}$ have nonzero probability). Find the unicity distance if such a source is encrypted using the Hill cipher above.

**d)** Does the Hill cipher achieve perfect secrecy, if we encrypt only a single plaintext vector $m$?

(10 points)

---

## Problem 3

Factor the RSA number $n = 44384521$ using the basic form of the Quadratic Sieve algorithm you learned in the first project. The square of the following numbers are $B$-smooth for some very small $B$,

$$1883840, 6521874, 13519124, 16006155.$$

Note that factoring $n$ by trial division is not allowed.

(10 points)

## Problem 4

**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 $y_2 = 15$, participant 3 holds the private share $y_3 = 25$, and participant 27 holds the private share $y_{27} = 17$. Help the three participants to restore the shared secret $K$.

**b)** In an authentication system, Alice would like to send **two** source messages $s_1, s_2 \in \mathbb{F}_{101}$ to Bob in two separately authenticated messages.

They come up with the less good idea of using 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 first transmitted message $M_1$ is then $M_1 = (s_1, t_1)$, where

$$t_1 = e_1 + s_1 e_2.$$

For the second message, they use $M_2 = (s_2, t_2)$, where

$$t_2 = e_1 + s_2 e_2^2.$$

Eve observes first the message $M_1 = (2, 45)$ and then she observes $M_2 = (3, 3)$. Find a message that maximizes her chances of getting another message accepted instead of $M_2$.

(10 points)

## Problem 5

In an RSA cryptosystem 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 prime $p > 1000$ and show a few steps of a probabilistic primality test that asserts that $p$ is a (probable) prime.

**b)** Then pick the prime $q = 113$ and give the RSA public keys $(n, e)$. Give the secret parameters $d$ and $\phi(n)$ in the RSA cryptosystem.

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

**d)** Prove that if Eve knows $\phi(n)$ in an RSA system with public keys $(n, e)$, then she can compute $p$ and $q$.

(10 points)