# Final exam in

# CRYPTOGRAPHY

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

## January 4, 2018, 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

Consider the following statements about the two polynomials $P_1(x) = x^3 + x^2 + x + 1$ and $P_2(x) = x^3 + x + 1$.

**a)** The polynomial $P_1(x)$ is irreducible ("primpolynom") over $\mathbb{F}_2$.

**b)** The polynomial $P_1(x)$ is irreducible over $\mathbb{F}_3$.

**c)** The polynomial $P_1(x)$ defined over $\mathbb{F}_2$ has period 5.

**d)** The polynomial $P_2(x)$ over $\mathbb{F}_2$ is a primitive polynomial.

**e)** The cycle set for an LFSR with connection polynomial $C(D) = P_1(D)P_2(D)$ in $\mathbb{F}_2$ contains at least one cycle of length 14.

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

We wish to encrypt a source with alphabet $\mathbb{Z}_5$ generating independent symbols with $P(M_i = 0) = P(M_i = 1) = P(M_i = 2) = 1/4$ and $P(M_i = 3) = P(M_i = 4) = 1/8$, $i = 0, 1, \ldots$.

The key $\mathbf{K} = (K_0, K_1)$ is chosen uniformly from the set of 2-tuples ($K_i \in \mathbb{Z}_5$). A sequence of message symbols $\mathbf{M} = (M_0, M_1, \ldots, M_{n-1})$ is encrypted to a sequence of ciphertext symbols $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ by

$$C_i = M_i + K_{i \bmod 2} \mod 5, \quad 0 \leq i \leq n-1.$$

**a)** Compute the unicity distance $N_0$ according to the formula. (5 points)

**b)** For which lengths $n$ do we have perfect secrecy? (1 point)

**c)** Eve observes a ciphertext of length 400 and counts the frequency of different symbols. She gets the following count:

| Symbol | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Number of occurences: | 52 | 73 | 101 | 98 | 76 |

What can you conclude about the key $\mathbf{K}$ from this? (3 points)

**d)** Suggest a better way of counting symbols for Eve, that will find the key if the ciphertext length is only slightly more than $N_0$.

(1 point)

## Problem 3

**a)** Consider a Shamir threshold scheme for $n = 10$ participants with threshold $k = 4$ using the public values $x_i = i$. All values are assumed to be in $\mathbb{F}_{19}$. Assume that participant 2 holds the private share $y_2 = 3$, participant 3 holds the private share $y_3 = 10$, participant 4 holds the private share $y_4 = 6$ and participant 7 holds the private share $y_7 = 6$. Help the four participants to reconstruct the shared secret $K$.

(5 points)

**b)** In an authentication system, Alice would like to send a source message $(s_1, s_2, s_3)$, $s_1, s_2, s_3 \in \mathbb{F}_{37}$ to Bob in an authenticated channel message $M$.

They are using an authentication code, where the key (encoding rule) $E$ is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{F}_{37}$. The transmitted message is $M = (s_1, s_2, s_3, t)$, where $t = e_1 + s_1 e_2 + s_2 e_2^2 + s_3 e_2^3$. Eve observes the message $M = (0, 0, 0, 9)$. Find another message that maximizes her chances of getting this other message accepted instead of $M$.

(5 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. Assume that image $I_1$ starts with four zero 8-bit blocks, followed by blocks with known randomly generated values, $I_1 = (0, 0, 0, 0, x_4, x_5, \ldots)$, $x_i \in \mathbb{F}_2^8$. Similarly, $I_2$ starts with the four blocks $0, 1, 0, 1$, followed by blocks with known randomly generated values, $I_2 = (0, 1, 0, 1, y_4, y_5, \ldots)$, $y_i \in \mathbb{F}_2^8$. (Here 1 means a block with a single one in rightmost position (00000001))

**a)** Alice first uses a good block cipher $E_K(x)$ of block length 8 bits, key length 128 bits, and the ECB mode of operation (Electronic CodeBook). The generated ciphertext starts as

$$10110101, 10010010, \ldots$$

Help Eve to decide which plaintext was sent by Alice. (2 points)

**b)** (cont' from a)) In an attempt to make a better encryption solution, Alice instead uses CBC mode (Cipher Block Chaining), where the ciphertext is generated as $c_i = E_K(x + c_{i-1})$ (assuming $c_{-1} = 0$). Give a rough estimate on the expected number of ciphertext blocks that Eve needs to observe before she will know which image that was transmitted, without trying to find the key or using high complexity procedures. (4 points)

**c)** Alice decides to use instead an LFSR-based stream cipher for encryption, operating on symbols from $\mathbb{F}_{2^8}$. Unfortunately, the linear complexity for the chosen stream cipher is too low ($\leq 1$), i.e., the stream cipher is equivalent to an LFSR over $\mathbb{F}_{2^8}$ of length one. Knowing this, show an attack where Eve determines which image was sent as plaintext. The observed ciphertext is

$$00000001, 10000000, 10011010 \ldots$$

An irreducible polynomial is $\pi(x) = x^8 + x^4 + x^3 + x + 1$, $\pi(x) = 0$ will generate $\mathbb{F}_{2^8}$, and the vector space $\mathbb{F}_2^8$ is mapped to $\mathbb{F}_{2^8}$ in the usual way.

(4 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)** Compute one step of a (Fermat) probabilistic primality test that asserts that $p = 1021$ is a (probable) prime.

(2 points)

**b)** Then pick the prime $q = 127$ and form the RSA public keys $(n = 129667, e)$. Find a suitable choice for $e$ and give the secret parameters $d$ and $\phi(n)$ in the RSA cryptosystem.

(3 points)

**c)** Show the steps of calculating the ciphertext $C = M^e \bmod n$ when encrypting the plaintext $M = 19753$ in your constructed RSA system. Use square-and-multiply or some similar efficient method.

(2 points)

**d)** Eve has tried to factor the number $n = 129667$ by applying the quadratic sieve factoring algorithm. After performing the two main and time consuming steps she has reached the expression

$$574^2 = 447^2 \bmod n.$$

Show Eve how the factors of $n$ are determined from the above relation. (3 points)