# Final exam in
# CRYPTOGRAPHY

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

## January 11, 2017, 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 $P_1(x) = x^3 + x + 1$ and $P_2(x) = x^5 + x + 1$.

**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 $P_1(x)$ is irreducible over $\mathbb{F}_{2^2}$.

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

**e)** There exists a finite field with 33 elements and it can be constructed by using $P_2(x)$ to construct $\mathbb{F}_{2^5}$ and then extending by adding a zero element.

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 $\mathbb{Z}_5$ having $P(M_i = 0) = 1/2$, $P(M_i = 1) = 1/4$ and $P(M_i = 2) = P(M_i = 3) = 1/8$, $i = 0, 1, \ldots$. So $P(M_i = 4) = 0$.

The key $\mathbf{K} = (K_0, K_1, \ldots, K_{l-1})$ is chosen uniformly from the set of $l$-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

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

**a)** When $l = 32$, compute the unicity distance $N_0$ according to the formula.

(5 points)

**b)** Roughly, how many ciphertext symbols ($n$) do Eve need to observe in order to uniquely determine the key if she is performing an exhaustive key search in a *ciphertext-only* attack? (2 point)

**c)** Roughly, how many ciphertext symbols ($n$) do Eve need to observe in order to uniquely determine the key if she is performing an exhaustive key search in a *known-plaintext* attack?

(1 point)

**d)** For this particular source, can you propose a new encryption scheme such that we have $N_0 = \infty$? (2 points)

## Problem 3

It is known that Alice has two images $I_1$ and $I_2$ and will send one of them encrypted to Bob. She first uses a block cipher of block length 16 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, $I_1 = (0, 0, x_2, x_3, \ldots)$, $x_i \in \mathbb{F}_2^{16}$. Similarly, $I_2$ starts with the two blocks $0, 1$, followed by blocks with known randomly generated values, $I_2 = (0, 1, y_2, y_3, \ldots)$, $y_i \in \mathbb{F}_2^{16}$. (Here 1 means a block with 16 ones)

**a)** Explain why ECB mode (Electronic codebook mode) is not a good choice for Alice in this case. (2 points)

**b)** Explain a better way to do the encryption by explaining countermode as the mode of operation for encryption. Explain also how decryption is done. (1 points)

**c)** Alice decides to use instead an LFSR based stream cipher for encryption, operating on single bits. Unfortunately, the linear complexity for the chosen stream cipher is too low ($\leq 8$). Show an attack where Eve determines which image was sent as plaintext. The observed ciphertext is

$$1000100000001000, 01111111\ldots$$

(7 points)

## Problem 4

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)** Show a few steps of a probabilistic primality test that asserts that $p = 2017$ is a (probable) prime.

(2 points)

**b)** Then pick the prime $q = 113$ and form the RSA public keys $(n = 227921, e = 25)$. Give the secret parameters $d$ and $\phi(n)$ in the RSA cryptosystem.

(2 points)

**c)** Show the steps of calculating the ciphertext $C = M^{25} \bmod n$ when encrypting the plaintext $M = 123$. Use square-and-multiply or some similar efficient method.

(2 points)

**d)** Try to find arguments proving that if Eve knows $d$ in an RSA system with public keys $(n, e)$, then she most likely can compute $p$ and $q$.

Hint: Try to reach an expression of the form $X^2 = Y^2 \bmod n$ for some choice of $X, Y$ and then use what you learned in the first project. (4 points)

## Problem 5

**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 $y_2 = 30$, participant 3 holds the private share $y_3 = 20$, and participant 7 holds the private share $y_7 = 7$. Help the three participants to reconstruct the shared secret $K$.

(5 points)

**b)** In an authentication system, Alice would like to send a source message $(s_1, s_2)$, $s_1, s_2 \in \mathbb{F}_{37}$ 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 $M = (s_1, s_2, t)$, where $t = e_1 + s_1 e_2 + s_2 e_2^2$. Eve observes the message $M = (0, 0, 10)$. Find another message that maximizes her chances of getting this other message accepted instead of $M$.

(5 points)