Special instructions for home exam in

EDIN01 CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

10.00 on August 25, 2020, until 12.00 on August 26.

- Hand-out of exam: at 10.00 on August 25 the exam will be available on the course web page for download. Use your own white sheets for writing solutions. Alternatively, a copy of the exam and empty sheets of paper can be picked up in boxes outside EIT (third floor in E-building) from 10.00.
- Hand-in of exam: During 10.00-12.00 on August 26 you can hand in your exam solutions at the department (third floor in E-building, hand-in boxes in stairwell). Alternatively, you can hand in by scanning your solutions and email them to the examiner on email address: thomas@eit.lth.se no later than 12.00! But you must then also send the original solutions and this first page with original signature by regular mail to the address below.[1] The exam will not be corrected until this is received.
- Exam contents: In the home exam there will be problems similar to a standard exam. The grading will require 25/35/45 points for grade 3/4/5, respectively, out of a total of 50. To get grade 5 you additionally need to be approved on an oral exam.
- Sign-up: You need to have signed up to take the exam.
- Help and assistance: You are allowed to use any written information you have access to and you are allowed to use computers and programming for computations. **You are not allowed to get assistance in any way from any other person to help you with your solutions.** This includes asking people to post information on forums, etc. It also includes assisting any other person doing the exam. To assure this, you have to formally sign such a statement.[2] **This first page with original signature must be handed in together with your solutions!**

Name:

Personal Code Number:

I solemnly declare that I have not used help from any other person in the process of preparing the exam solutions that I now hand in.

Signature:

Hand in this page with original signature!

[1] Address: Thomas Johansson, Dept. of EIT, Box 118, 22100 Lund, Sweden

[2] Overstepping the rules of help and assistance may lead to suspension from the university.

Final exam in

CRYPTOGRAPHY

August 25, 2020,

- 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 English text. She decides that she wants extra protection by encrypting the text first by one cipher and then by a second cipher. If E_K denotes the encryption by the first cipher and $E_{K'}$ denotes the encryption by the second cipher, the encryption process would be as follows.

A sequence of message symbols $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertext symbols $C_1, C_2, \ldots, C_n$ by

$$C_i = E_{K'}(E_K(M_i)), \quad \forall i, 1 \leq i \leq n.$$

a) Determine the unicity distance if the first cipher is a simple substitution cipher and the second cipher is the identity map ($E_{K'}(M_i) = M_i$).

b) Determine the unicity distance if the first cipher is a simple substitution cipher and the second cipher is a Caesar cipher.

Hint: Two keys are different if they represent different mappings from plaintext symbol to ciphertext symbol.

c) If we want to make the unicity distance for the system above even larger than in **a)** and **b)**, suggest what we could do.

(10 points)

Problem 2

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

$$s = [0, 0, 0, 1, 1]^{\infty}$$

over $\mathbb{F}_2$.

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

$$s = (1, 0, 1, 2\alpha, 2\alpha, \alpha + 1, 2)$$

over $\mathbb{F}_{3^2}$, generated by $p(x) = x^2 + x + 2$ and $p(\alpha) = 0$.

(10 points)

Problem 3

a) A Shamir threshold scheme for $n = 5$ 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, 2, and 3 hold the private shares $y_1 = 40$, $y_2 = 50$, and $y_3 = 60$. Help them to reconstruct the secret.

b) In an authentication system the source message S and the key E are given as,

$$S = (s_1, s_2), \quad E = (e_1, e_2),$$

where

$$s_1, s_2, e_1, e_2 \in \mathbb{F}_3.$$

The coded message M is a 3-tuple generated by

$$M = (s_1, s_2, t),$$

where

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

Find the value of P_I and P_S. Recall that P_S is calculated as

$$P_S = \max_{M, M' : M' \neq M} P(M' \text{ valid} | M \text{ observed}).$$

(10 points)

Problem 4

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 5

Consider the polynomial $p(x) = 1 + x^3 + x^5$.

a) Show that $p(x)$ is irreducible ("primpolynom") over $\mathbb{F}_2$.

b) Determine whether $p(x)$ is primitive ("primitivt polynom") over $\mathbb{F}_2$ or not.

c) Determine whether $p(x)$ is irreducible ("primpolynom") over $\mathbb{F}_{2^5}$ or not.

(10 points)