Special instructions for home exam in

EDIN01 CRYPTOGRAPHY

Dept. of Electrical and Information Technology
Lund University

12.00 on January 11, 2021, until 14.00 on January 12.

- Hand-out of exam: at 12.00 on January 11 the exam will be available on the course web page for download. Use your own white sheets for writing solutions.
- Hand-in of exam: During 10.00-14.00 on January 12 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 14.00! But you must then also send the original solutions and this first page with original signature by regular mail to the address below (or leave them in the hand-in boxes), to be received within a week.[1] The exam will not be corrected until the original 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 and expected to use computers and programming for computations (maple). **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!**

☐ Markning here means that I want to do an oral exam in case I get ≥ 45 points.

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:

Print and 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 and legal actions.

Final exam in

CRYPTOGRAPHY

January 11, 2021,

- You are allowed to use any written information and any computational resources.
- 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

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

$$s = [0, 1, 2, 2, 0, 2, 1, 1]^{\infty}$$

over $\mathbb{F}_3$. Show the steps of your calculation.

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

$$s = (0, 1, \alpha, \alpha^2 + 1, \alpha^3 + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1)$$

over $\mathbb{F}_{2^4}$, generated by $p(x) = x^4 + x^3 + 1$ and $p(\alpha) = 0$. Show the steps of your calculation.

(10 points)

Problem 2

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,

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

Show the steps of your calculation. Note that factoring n by trial division is not allowed.

(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 $y_1 = 45$, $y_2 = 56$, and $y_3 = 67$. Help them to reconstruct the secret.

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

$$S = (s_1, s_2, s_3), \quad E = (e_1, e_2, e_3),$$

where

$$s_i, e_i \in \mathbb{F}_3, \forall i.$$

The coded message M is a 4-tuple generated by

$$M = (s_1, s_2, s_3, t),$$

where

$$t = e_1 + s_1e_2 + s_2e_3 + s_3e_2e_3.$$

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

Alice encrypts 128-bit blocks using a cipher with a 128-bit key K. Assume there are two types of sources of messages, either the source is producing messages with independent bits with probability $P(m_i = 0) = 0.11$ (we call this source type 1). Alternatively, the messages are from a source with independent bits with probability $P(m_i = 0) = 0.5$ (type 2).

Let E_K denotes the encryption function for the specified block cipher. There are two possible mode of operations: In counter mode style (type A) the encryption process would be as follows. A sequence of message blocks $M_1, M_2, \ldots, M_n$ is encrypted to a sequence of ciphertext blocks $C_1, C_2, \ldots, C_n$ by

$$C_i = E_K([i]) \oplus M_i, \quad \forall i, 1 \leq i \leq n,$$

where $[i]$ denotes the 128-bit block corresponding to the binary representation of the integer i. In ECB mode (type B), we simply encrypt by computing

$$C_i = E_K(M_i), \quad \forall i, 1 \leq i \leq n,$$

a) Determine the unicity distance if the mode of operation is counter mode style (type A) and the message source is of type 1.

b) Continuing a), if Eve has infinite computing power, how many blocks of ciphertext does she roughly need to observe in order to be able to determine the value of the secret key (with high probability).

c) Determine the unicity distance if the mode of operation is ECB (type B) and the message source is of type 2.

d) Assume Eve has limited computing power, say she can do at most 2^{70} computations. Alice is now encrypting messages using ECB mode (type B), all from one of these two message types and it is the task of Eve to determine the type (1 or 2), after observing a sequence of ciphertext blocks.

Help Eve to solve her task, such that the correct answer to the type is given with large probability. Give the minimum expected number of observed ciphertexts that you will need in your attack and explain how it is done. You need to do some numerical computations on the computer (maple).

(10 points)

Problem 5

Consider the basic RSA signature scheme, generating a signature s for a message m by computing $s = h(m)^d \bmod N$, where $h()$ is a hash function and d is the secret key in RSA. Let the public key consist of $N = 64006001$ and $e = 7$. Furthermore, let $m = (m_1, m_2)$, $m_i \in \mathcal{Z}_{64006001}$. The hash function is defined as $h(m) = 723m_1^3 + m_2 + m_1 \cdot m_2 + 3 \bmod N$.

a) Is the signed message $(m, s) = (2, 3, 13370301)$ a correctly signed message? Show the steps of your calculation.

b) If you know that one factor of N is 8101, compute a valid signature for $m = (4, 5)$. Show the steps of your calculation.

c) Assume that we cannot factor N. Find a valid signed message with signature 0. Use a preimage attack on h and the fact that the hash function is not a proper cryptographic hash function.

d) Assume instead that we use a somewhat better hash function,

$$h(m) = m_1^3 + m_2^3 + m_1 \cdot m_2 + 3(m_1^2 + m_2^2 + 1234)^2 \bmod N.$$

Give your best existential forgery attack on the signature scheme. Consider an active attack, where you can get one message signed by the signing oracle. Then you produce another correctly signed message that was never signed by the oracle. Describe the attack through pseudo-code or a similar description, and determine the expected computational complexity (number of awarded points depends on the computational complexity).

(10 points)