TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 22 January 2018

Name :

TU/e student number :

Exercise	1	2	3	4	5	6	total
points							

Notes: Please hand in this sheet at the end of the exam. You may keep the sheet with the exercises.
This exam consists of 6 exercises. You have from 13:30 – 16:30 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are not allowed to use any books, notes, or other material.
You are allowed to use a simple, non-programmable calculator without networking abilities. Usage of laptops and cell phones is forbidden.

1. This exercise is about LFSRs. Do the following subexercises for the sequence

$$s_{i+5} = s_{i+4} + s_i.$$

   (a) Draw the LFSR corresponding this sequence. | 2 points |

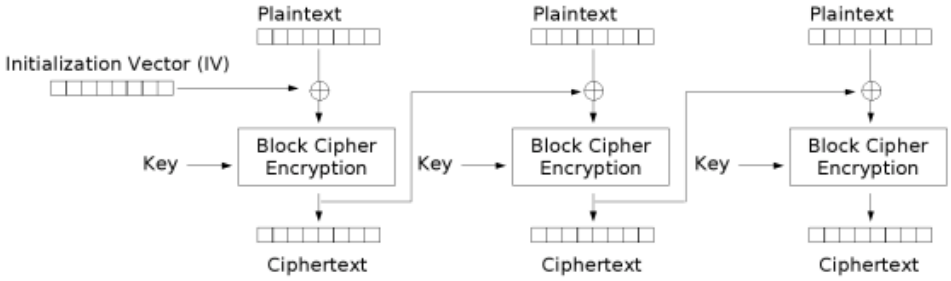
   (b) State the characteristic polynomial f and compute its factorization. You do not need to do a Rabin irreducibility test but you do need to argue why a factor is irreducible. | 12 points |

   (c) For each of the factors of f compute the order. | 8 points |

   (d) What is the longest period generated by this LFSR? Make sure to justify your answer. | 3 points |

   (e) State the lengths of all subsequences so that each state of n bits appears exactly once. Make sure to justify your answer. | 8 points |

2. This exercise is about modes. Here is a schematic description of the CBC (Cipher Block Chaining) mode.



Cipher Block Chaining (CBC) mode encryption

[Picture by White Timberwolf, public domain]

This encryption uses a block cipher of block size b. Let $\mathrm{Enc}_k(m)$ denote encryption of a single block m using this block cipher with key k and let $\mathrm{Dec}_k(c)$ denote decryption of a single block c using the block cipher with key k. Let IV be the initialization vector of length b, let m_i be the b-bit strings holding the message and c_i be the b-bit strings holding the ciphertexts.

(a) Describe how encryption and decryption of long messages work, i.e., write c_0, c_1, and a general c_i in terms of IV, m_0, m_1, m_i, and (if necessary) other m_j and c_j; and write m_0, m_1, and a general m_i in terms of IV, c_0, c_1, c_i, and (if necessary) other m_j and c_j. [6 points]

(b) Ciphertexts are received with explicit sequence numbers (i, c_i). Assume that ciphertext c_j gets modified in transit. Show which messages get decrypted incorrectly. [4 points]

3. This problem is about RSA encryption.

(a) Alice's public key is $(n, e) = (13231, 7)$. Encrypt the message $m = 234$ to Alice using schoolbook RSA (no padding). [6 points]

(b) Let $p = 449$ and $q = 569$. Compute the public key using $e = 3$ and the corresponding private key. **Reminder:** The private exponent d is a positive number. [6 points]

4. This problem is about the DH key exchange. The public parameters are that the group is $(\mathbb{F}_{971}^*, \cdot)$ and that it is generated by $g = 11$.

(a) Compute the public key belonging to the secret key $b = 18$. [6 points]

(b) Alice's public key is $h_a = 473$. Compute the shared DH key with Alice using b from the previous part. [8 points]

5. The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. Alice's public key is $h_a = g^a = 11$. Use the Baby-Step Giant-Step method to compute Alice's private key a. Verify your result, i.e. compute g^a. [12 points]

6. The ANSI X9.17/X9.31 random number generator (RNG) produces pseudorandom numbers using a block cipher. Outputs are blocks of b bits, where b is the block size of the block cipher.

   An implementation of this RNG has a secret key k for the block cipher hard coded in the system and maintains an internal state S_i that it updates after every output block. A second input to the RNG is a sequence of time stamps $T_1, T_2, T_3, \ldots$, where each output block uses one of the time stamps and each time stamp is a b-bit value.

   The system starts with an initial state S_0 and the key k, each having b bits.

   To compute the first output block, the system first computes an intermediate value $I_1 = \mathrm{Enc}_k(T_1)$ and then computes the first output block $O_1 = \mathrm{Enc}_k(I_1 \oplus S_0)$, where as usual $\oplus$ denotes bitwise xor, i.e., addition in $\mathbb{F}_2^b$. Finally, the internal state is updated to $S_1 = \mathrm{Enc}_k(O_i \oplus I_1)$.

   In general, to compute the i-th output block, the system computes the i-th intermediate value $I_i = \mathrm{Enc}_k(T_i)$, the i-th output block $O_i = \mathrm{Enc}_k(I_i \oplus S_{i-1})$, and the i-th state $S_i = \mathrm{Enc}_k(O_i \oplus I_i)$.

   (a) Draw a diagram of the data flow in the ANSI X9.17/X9.31 RNG, showing output values, state, and intermediate values. [4 points]

   (b) State the output O_1 in terms of T_1, S_0, and k. [2 points]

   (c) State the output O_i in terms of T_i, S_{i-1}, and k. [2 points]

   (d) Many implementations of ANSI X9.17/X9.31 use the same fixed key k. The state values S_i differ per device. Show how to recover S_1 given output O_1, time stamp T_1 and the key k. [4 points]

   (e) Show how to recover S_0 from O_i, key k, and time stamps $T_1, T_2, T_3, \ldots, T_i$. [3 points]

   (f) The previous parts assumes exact knowledge of T_1. Assume that you have captured O_1 and O_2 at times T_1' and T_2' close to T_1 and T_2. Find a relation between O_1, O_2, T_1, and T_2, so that you can test for the correct times by searching around T_i'. [4 points]