TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 26 January 2026

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 9:00 – 12:00 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document *all steps and intermediate results*, in particular of algorithms, on the exam paper, do not use the scrap paper. It is not sufficient to state the correct result without the explanation and the steps that lead to it.
If the problem statement asks for 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
$$s_{i+7} = s_{i+4} + s_{i+2} + s_{i+1} + s_i.$$

   (a) Draw the LFSR corresponding this sequence. 3 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.
   Reminder: Factors may appear with multiplicity larger than one. 10 points

   (c) Write the factorization of f from (b) in the form $f = \prod f_i^{e_i}$ with integers $e_i > 0$ and f_i different irreducible polynomials, i.e., group equal factors.
   For each of the $f_i^{e_i}$ compute the order.
   Reminder: We have shown in class that $f_i^{e_i}$ has order different from that of f_i (for $e_i > 1$) and you need to compute the order directly. We do not have a theorem for this. 7 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 7 bits appears exactly once.
   Make sure to justify your answer and to check that all 2^7 states are covered. 13 points

2. Let $E_K(\cdot)$ be a block-cipher working over 64 bit and instantiated with a 64-bit key K. Our goal is to set up a cipher that guarantees 128 bits of security, via a modified a version E instantiated with a pair of 64-bit keys (K_1, K_2).

   Your task is to analyze the security of each one of the following modifications of the cipher E assuming the knowledge of several plaintext/ciphertexts pairs encrypted under the same keys (K_1, K_2) (remember to justify your estimation).

   (a) $E_{E_{K_2}(K_1)}(\cdot)$. 3 points

   (b) $E_{K_1}(\cdot) \oplus K_2$. 3 points

   (c) $E_{K_2}(E_{K_1}(\cdot))$. 3 points

   (d) $E_{K_2}(E_{K_2}(E_{K_1}(\cdot)))$. 3 points

(e) $E_{K_1}(E_{K_2}(E_{K_1}(\cdot)))$. 3 points

[Notation: $\oplus$ = bit-wise XOR.]

3. This problem is about schoolbook RSA encryption. Let $p = 307$ and $q = 521$. Compute the public key using $e = 65537$ and the corresponding private key.
Reminder: The private exponent d is a positive number.
8 points

4. This problem is about the DH key exchange. The public parameters are the group G and generator g, where $G = (\mathbb{F}_{1229}^*, \cdot)$ and $g = 11$. Alice's public key is $h_A = 127$. Bob's private key is $b = 27$, compute the DH key that Bob shares with Alice. 8 points

5. The integer $p = 37$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{37}^*$ with generator $g = 5$. Alice's public key is $h_A = 5^a = 31$. Use the Baby-Step Giant-Step method to compute Alice's private key a.
Verify your result, i.e. compute g^a. Make sure to detail the steps you take in verifying the result. 11 points

6. Shamir's Secret Sharing is not the only way to set up a secret sharing scheme. Blakley's secret sharing scheme is based on hyper plane geometry. To solve a (t, n)-threshold secret sharing scheme problem, each of the n participant is given a hyper-plane equation in a t dimensional space such that each hyper plane passes through a certain point (linked to the secret information).

   (a) An affine hyper plane in a t-dimensional space with coordinates can be described by a linear equation of the following form

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_t \cdot x_t = b.$$

   Describe how to set up the Blakley's secret sharing scheme working modulo an integer prime p (remember that t out of n participants must be sufficient to recover the secret information).
   [**Hint:** identify the secret s to share as the point $(s, r_2, r_3, \ldots, r_t) \in \mathbb{Z}_p^t$ for random integers $r_2, r_3, \ldots, r_t \in \mathbb{Z}_p$. Note that if $r_2, r_3, \ldots, r_t$ are fixed known values (e.g., $r_2 = r_3 = \ldots = r_t = 0$), then the Blakley's secret sharing scheme cannot work. Explain the reason.]
   12 points

(b) Use Blakley's secret sharing scheme to share $s = 5$ modulo 103 in a 2-out-of-3 fashion. Verify for two sets of 2 users that you can recover the secret. $\boxed{\text{8 points}}$

(c) Assume that one participant is more important than the others, and must have more decisional power. Explain how to set up the Blakley's secret sharing for this particular case. $\boxed{\text{2 points}}$