TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 13 April 2026

Name :

TU/e student number :

Exercise	1	2	3	4	5	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 5 exercises. You have from 18.00 – 21.00 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.

Important:

- examinees are only permitted to visit the toilets under supervision;
- it is not permitted to leave the examination room within 15 minutes of the start and within the final 15 minutes of the examination, unless stated otherwise;
- examination scripts (fully completed examination paper, stating name, student number, etc.) must always be handed in;

- the house rules must be observed during the examination;
- the instructions of subject experts and invigilators must be followed;
- keep your work place as clean as possible: put pencil case and breadbox away, limit snacks and drinks;
- examinees are not permitted to share examination aids or lend them to each other.

During written examinations, the following actions will in any case be deemed to constitute fraud or attempted fraud:

- using another person's proof of identity/campus card (student identity card);
- having a mobile telephone or any other type of media-carrying device on your desk or in your clothes;
- using, or attempting to use, unauthorized resources and aids, such as the internet, a mobile telephone, smartwatch, smart glasses etc.;
- having any paper at hand other than that provided by TU/e, unless stated otherwise;
- copying (in any form);
- visiting the toilet (or going outside) without permission or supervision.

First-year bachelor students: The final grade for this exam will be announced no later than fifteen working days after the date of this exam, unless this exam takes place in Q4 or the interim period. For Q4 final exams, grades will be announced within five working days after the end of the Q4 final test period. For interim period final exams, grades will be announced no later than five working days before September 1.
All other students: Generally, the final grade for this exam will be announced no later than fifteen working days after the date of this examination. Specifically for bachelor exams administered in the interim period, exam grades will be announced no later than five working days before September 1.

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

$$s_{i+7} = s_{i+6} + s_{i+2} + s_{i+1} + s_i.$$

   (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.
   Reminder: Factors may appear with multiplicity larger than one. | 6 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. | 4 points |

   (d) What is the longest period generated by this LFSR?
   Make sure to justify your answer. | 2 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. | 12 points |

2. Let $\mathsf{E}_K : \{0,1\}^n \to \{0,1\}^n$ and $\mathsf{E}'_K : \{0,1\}^{2 \cdot n} \to \{0,1\}^{2 \cdot n}$ be two block ciphers instantiated via a secret key K picked uniformly at random. Let $M = M_1 \| \ldots \| M_l \in \{0,1\}^{n \cdot l}$ be a message (already padded).

   Consider the following two alternative definitions of a MAC function, which receives as input $M \in \{0,1\}^{n \cdot l}$ and returns a tag T. Show how neither definition provides the security property of existential unforgeability (for example, by finding two chosen messages that return the same tag, or by forgining a new valid message-tag pair).

   (a) $T = \mathsf{E}_K(M_1) \oplus \mathsf{E}_K(M_2) \oplus \ldots \oplus \mathsf{E}_K(M_l)$. | 4 points |

   (b) $T = \mathsf{E}'_K(\langle 1 \rangle \| M_1) \oplus \mathsf{E}'_K(\langle 2 \rangle \| M_2) \oplus \ldots \oplus \mathsf{E}'_K(\langle l \rangle \| M_l)$. | 12 points |

   [Notation: $\oplus$ = bit-wise XOR, $\|$ = concatenation, $\langle i \rangle$ = n-bit representation of the integer i.]

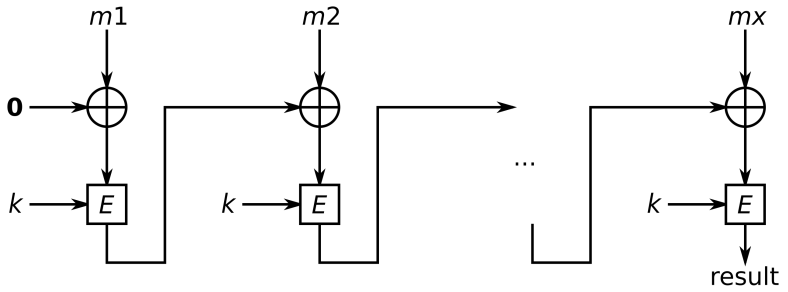

Figure 1: CBC-MAC (with $IV = 0$). Image credit: Wikipedia.

An alternative way to construct a MAC from a block cipher is the "cipher block chaining message authentication code" (CBC-MAC), illustrated in Figure 1 for $IV = 0$. Let T be the tag of the (already padded) message $M = M_0 \| M_1 \| M_2$, and let T' be the tag of the (already padded) message $M' = M'_0 \| M'_1 \| M'_2$. Show that the tag of the (already padded) message $M'' := M_0 \| M_1 \| M_2 \| (T \oplus M'_0) \| M'_1 \| M'_2$ is again T'. Is CBC-MAC secure? 4 points

3. This problem is about schoolbook RSA encryption.

   (a) Exploit a primality test to show that the following numbers $\{551, 561\}$ are not prime (factorization is *not* accepted as a correct answer). 4 points

   (b) Let $p = 479$ and $q = 449$. Compute the public key using $e = 65537$ and the corresponding private key.
   Reminder: The private exponent d is a positive number.
   8 points

   (c) An RSA encryption routine calculates the value m^e mod n using a square-and- multiply algorithm (right-to-left binary exponentiation). During the execution of that algorithm, you can briefly hear a buzzing sound (through radio-frequency interference) on an AM radio receiver located near the computer. You record that sound, and discover that it is actually the following sequence of two different sounds A and B:

   $$BABAABABAABAB.$$

   What is the value of e?

   3 points

(d) Consider a variant of RSA in which the two primes are equal, that is, $n = p^2$ for a certain prime p. Is this variant of RSA secure? (Justify your answer.)

Next, consider the case in which $n = p^2 \cdot q$ for p, q being two distinct primes. Explain how key-generation, encryption, and decryption work for this case. Prove that (1st) decryption always returns the correct message *if* the message is *not* a multiple of p (do not forget the case in which the message is a multiple of q), and (2nd) present an example of two messages multiple of p that result in the same ciphertext. | 7 points |

4. The integer $p = 43$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{43}^*$ with generator $g = 3$. Alice's public key is $h_A = 3^a = 2$. 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. | 8 points |

5. This exercise is about ElGamal encryption.

(a) Describe ElGamal encryption over a prime field $\mathbb{Z}_p$, including key-generation, encryption, and decryption. Prove that decryption always returns the correct plaintext. | 6 points |

(b) Is ElGamal encryption IND-CPA secure? Justify your answer (e.g., with arguments discussed in class, no formal proof needed). If not, explain how to make it secure. | 10 points |

(c) Is ElGamal encryption IND-CCA2 secure? Justify your answer (e.g., with arguments discussed in class, no formal proof needed). If not, propose a variant that is secure. | 8 points |