Permitted items:

- The following items are permitted
  - Books (phyisical or pdf), printouts, digital documents on the computer or online, handwritten notes
  - Your homeworks and the corrections you received
  - Blank paper for taking notes (no upload of pictures)
  - Pens, pencils, etc
  - Calculators
  - You may run computer algebra systems as well as your own code on the computer and in online calculators
  - You may use spell-checking tools and pepare text in other editors.
- You may **not** communicate with any other person regarding the exercises by any means during the exam. As an exeption you may contact Tanja Lange if you encounter any problems.
- Looking up existing webpages is permitted; posting the questions or answers counts as communication and is not permitted.
- You may visit the bathroom during the exam time and you may have food and drink on your desk.

Instructions for answering questions:
All answers should be entered into the answer fields in Ans; do not write on paper and upload photos of your answers.

The exam has numerical questions, i.e. questions you answer with a single number, and open questions, i.e. questions where you get a text field and can type arbitrary text. For the latter type of questions, make sure to justify your answers in detail and to give clear arguments. Use your own words, do not copy text. Document all steps, in particular of algorithms. It is not sufficient to state the correct result without explanation.

You may copy instructions and outputs from your computer algebra system into the answers but need to explain what they do and why you invoke them.

If an exercise requires usage of a particular algorithm, other approaches will not be accepted even if they give the correct result.

Video upload:
After this first part finishes you should record a video of you explaning your solution. Choose 3 exercise parts which are not numerical questions and aim for 5 min of recording (no longer than 10 min). Show your student ID and state your name at the beginning of the video.
Please use https://surfdrive.surf.nl/files/index.php/s/iYdPNL9Mq6gpB5q
for uploading your video. Name the file as
ID_{student ID]_[Last name].[file format]
filling in your TU/e student ID, your last name, and the file format (mp4, webm) instead of the brackets.
If your connection is too weak, store the video on your computer and compute the SHA-256 checksum of it and mail that to Tanja Lange at t.lange@tue.nl.

Support:
If you want to indicate that any unwanted disturbances occurred that might be registered as an irregularity, or if your exam does not go as expected due to technical problems that hindered your exam (for example power or Internet failure in the region), you can report this within 24 hours to the Examination Committee via the Webform Online Exam at https://educationguide.tue.nl/studying/corona/webform-online-exams/.

1 RSA

This exercise is about the RSA cryptosystem.

1.0p **a** Carry out the RSA key generation for primes p =1697 and q =1291 and exponent $e = 2^{16} + 1$. The results will be used in this and the following 2 exercise parts.

Answer this question with n.

Answer

1.0p **b** In the setting of part a),
answer this question with $\varphi(n)$.

Answer

2.0p **c** In the setting of part a),
answer this question with d.

Answer

2.0p **d** Bob has public key $(n, e) = (2774999, 65537)$ and private key $(n, d) = (2774999, 2096225)$. He receives ciphertext $c = 631739$ which was encrypted using schoolbook RSA to his public key. Decrypt c to compute the corresponding message.

Answer

2 BSGS

This exercise is about the baby-step giant-step attack on the discrete logarithm problem.

6.0p **a** Describe in your own words how and why the BSGS attack works to compute the discrete logarithm a of $h = g^g$ given the group generator g and its order ℓ.

9.0p b Let $p = 18143$ which is prime and let $F = \mathbb{F}_p$.
The element $g = 15862$ generates a subgroup of order $\ell = 47$.
You are given a target $h = 3913$ which is in the subgroup generated by g, i.e.., $h = g^a$ for some a.

Use the baby-step giant-step algorithm to compute a.

Verify the solution you got by computing g^a and comparing it to h.

Make sure to document in your answer all baby steps and all the giant steps you took.

Hint: Remember that BSGS depends on the order of g for the choice of m and that all computations take place in F.

3 LFSR

This exercise is about LFSRs.

15.0p a You are given an LFSR of state length 15
via its characteristic polynomial
$P(x) = f_1 \cdot f_2$ with
f1=x^5 + x^4 + x^3 + x + 1
f2=x^10 + x^9 + x^5 + x^4 + 1
in fully factored form, i.e., both of these factors are irreducible.

Determine the order of each factor with as little computation as possible. State which powers of x you needed to test. Solutions by brute force, e.g., trying all powers of x, will not be accepted.

You should provide full justifications for the correctness of the obtained orders using the results proved in the course, i.e., use the results proved in the course to substantiate why the computations you performed indeed result in the correct orders.

Note: the polynomials are provided in raw form so that you can easily copy and paste them. Please do not make typos by manually copying them.

4.0p **b** What is the longest period generated by the LFSR from part a?

Make sure to justify your answer.

16.0p **c** State the lengths of all subsequences of the LFSR from part a) so that each state of 15 bits appears exactly once.

For this exercise you need to justify the number of different sequences and their periods using the orders obtained in part a) and the theoretical results obtained in the course. Solutions by brute force/scripts running through all possible states will not be accepted.

4 Schoolbook RSA

This is an exercise about schoolbook RSA.

10.0p Rob sends an invitation to three friends. You know that they all use schoolbook RSA encryption, i.e., there is no padding in the message and that Rob sent the same message m to all three friends.

Their public keys are $(n_1, e_1), (n_2, e_2)$, and (n_3, e_3) with
$n_1 =$
30924020082496294295765222743494110742613331546067108186069453881212461286489
$n_2 =$
32344819287449588645226118368867425992916414506018491506077669686369772112101
$n_3 =$
35003958473581520076795238372884855526843052673528571553286465252587435775031
and they all use the same exponent $e_1 = e_2 = e_3 = 3$.

You observe ciphertexts c_1, c_2, and c_3 encrypted to their public keys with
$c_1 =$
76883393233914718408369928383761299932763061329613407969083159802637998122 19
$c_2 =$
32191233655664214942502091651773074946381380809016714869374157940996527414681
$c_3 =$

576000168465538203272374898184586729594913596863623793184020777632635387808 4

Compute the message m that Rob has encrypted to them.

Verify your answer by re-encrypting m to (n_3, e_3).

You can use base36 encoding to see the message, but that is not required for the solution.

5 MAC

This exercise is about a message authentication code built on top of the PCBC mode.

3.0p a Enc is an n-bit block cipher. Alice and Bob share a key k for Enc.
IV is an n-bit initialization vector chosen freely by the sender when generating MAC(m).
Assume for simplicity that all messages have a length that is a multiple of n and split into ℓ blocks of n bits as $m = (M_0, M_1, M_2, \ldots, M_{\ell-1})$.

This picture shows how MAC(m) is computed. The input are the key k and message $m = (M_0, M_1, M_2, \ldots, M_{\ell-1})$. The output are the chosen IV and MAC(m).

Describe in words and formulas how MAC(m) is computed for PCBC-MAC (shown on the picture above).

8.0p b PCBC-MAC as defined here is not a secure MAC.
Show how Eve can use a valid message-MAC pair
$(m, t) = ((M_0, M_1, M_2, \ldots, M_{\ell-1}), (\text{IV}, \text{MAC}(m)))$
to compute a different valid message-MAC pair
$(m', t') = ((M'_0, M'_1, M'_2, \ldots, M'_{\ell-1}), (\text{IV}', \text{MAC}(m)'))$
for M'_0 of her choice, without knowing k.
I.e. describe how to choose $M'_1, M'_2, \ldots, M'_{\ell-1}$ IV,MAC$(m)'$ and why this will pass verification.

6 Modes of operation - CFB | CBC

The following diagram shows a mode of operation. The mode uses a block cipher
$\text{Enc}_k : \{0,1\}^n \to \{0,1\}^n$, where k is the key and n is the block length.

Assume for simplicity that all messages have a length that is a multiple of the block length, i.e., $m = (M_0, M_1, M_2, \ldots, M_{t-1})$ and each M_i has length n.

It is helpful to open the image in a separate window while solving the exercise parts.

8.0p a Scroll up if you got here without seeing the description of the mode.

Describe how encryption and decryption of long messages work,
i.e., write C_0 and a general C_i for $i > 0$ in terms of IV$_1$, IV$_2$, M_0, M_i, and (if necessary) other M_j and C_j.
Then write M_0 and a general M_i for $i > 0$ in terms of IV$_1$, IV$_2$, C_0, C_i, and (if necessary) other M_j and C_j.

This means understanding the data flow in the diagram and expressing it in formulas.

7.0p b Alice encrypts two messages, m and m' which differ only in one block M_i and she uses the same IVs, i.e., she encrypts $m = (M_0, M_1, M_2, \ldots, M_i, \ldots, M_{t-1})$ leading to $c = (C_0, C_1, C_2, \ldots, C_i, \ldots, C_{t-1})$ and $m' = (M_0, M_1, M_2, \ldots, M'_i, \ldots, M_{t-1})$ leading to $c' = (C'_0, C'_1, C'_2, \ldots, C'_i, \ldots, C'_{t-1})$ and the only difference between m and m' is in position i.

Investigate and describe which blocks of the respective ciphertexts c and c' differ. Note that i can take any value between 0 and $t-1$, both values included.

Make sure to check for possible cancellations.

8.0p c Assume that ciphertext c gets modified in transit to c' and that c' and c differ only in one block C_i, i.e., $c = (C_0, C_1, C_2, \ldots, C_i, \ldots, C_{t-1})$ arrives as $c' = (C_0, C_1, C_2, \ldots, C'_i, \ldots, C_{t-1})$ and the only difference between c and c' is in position i.

Investigate and describe which blocks in the resulting plaintext m' after decryption differ from the correct plaintext m. Note that i can take any value between 0 and $t-1$, both values included. The IVs are transmitted correctly.

Make sure to check for possible cancellations.