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/Wk5zdCD31Lvierh
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 Diffie-Hellman

This question is about the Diffie-Hellman key exchange. Alice and Bob use this system in the multiplicative group $\mathbb{F}_p^*$ for $p = 10037$ with generator $g = 7$.

3.0p a This exercise is a numerical question. The answer field takes a number. No justifications are needed.

Scroll up if you got here without seeing the parameters p and g.

Alice picks variable $a = 1408$.
Compute Alice's publlic key h_A.

Answer

3.0p b This exercise is a numerical question. The answer field takes a number. No justifications are needed.

Scroll up if you got here without seeing the parameters.

Bob's public key is $h_B = 2072$.
Compute the shared secret of Alice and Bob as an element of the integers modulo p, i.e. no application of the hash function is requred.

Answer

2 LFSR

This exercise is about LFSRs.

15.0p a You are given an LFSR of state length 15
via its characteristic polynomial
P(x) = (x^5 + x^4 + x^3 + x^2 + 1) * (x^10 + x^8 + x^7 + x^4 + x^2 + x + 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 give full justifications for the order using the results proved in the course.

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.

14.0p c State the lengths of all subsequences of the LFSR from part a) so that each state of 15 bits appears exactly once.

Make sure to justify your answer.

3 Message authentication codes

This exercise is about symmetric systems.

6.0p The Simple MAC is defined for key k and ciphertext c as $\text{MAC}(c, k) = H(k\,c)$,where H is a cryptographic hash function and k and c are simply concatenated.

Explain in your own words why the Simple MAC is not secure if H is constructed using the Merkle-Damgård construction. I.e., explain how to forge a MAC on some c' given a valid MAC on c for $c' \neq c$ without knowing the key k.

As a reminder, here is the Merkle-Damgård construction for computing $H(c)$.
Note, the picture does not show the MAC, in particular it does not include the key k. It does show how the input needs to be padded to reach a multiple of n in length.

C is a compression function from $2n$ to n bits and $\text{pad}(c) = C_0C_1C_2 \dots C_{t-1}$ is the padding of c so that each C_i has exactly n bits. The IV has also n bits.

4 Modes of operation - OFB|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 length a multiple of the block length, i.e., $m = (M_0, M_1, M_2, \dots, M_{t-1})$ 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.

6.0p b Alice sends two messages, m and m' which differ only in one block M_i and she uses the same IVs.

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

6.0p c Assume that ciphertext c gets modified in transit to c' and that c' and c which differ only in one block C_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 including 0 and $t-1$. The IVs are transmitted correctly.

5 Schoolbook RSA

This is an exercise about schoolbook RSA.

15.0p Patty is not giving up on having private parties and using schoolbook RSA encryption, i.e., there is no padding in the message. Her friends continue to use RSA keys with the same public exponent, namely $e = 3$, and their individual moduli.

Patty wants to send each of them the same message m but has learned that this is a problem with attacks. She thus decides to randomize the messages by picking random numbers r_1, r_2, and r_3 for her friends and encrypting the respective messages $m_i = r_i \cdot m$ to each of them. Of course the friends need to obtain the real message m and thus she sends each of them a second ciphertext with the encryption of their respective r_i.

The public keys of her friends are
$(n_1, e) =$
$(525310289568552547566207275498559894283467699200917953813389330653968107317 87, 3)$,
$(n_2, e) =$
$(262157219363592501093241855879909978172484310660651711999402477758606885963 49, 3)$,
and $(n_3, e) =$
$(584837220570103284755620563253250689929263391530605903242544668465530050162 99, 3)$.

You observe ciphertexts
$c_{11} =$
$33405395106290226929049812637082935314282761633772405620388793131141129302945$,
$c_{21} =$
$215485991874836472642447222518997628796633639460818551783149891405705153765 11$
being sent to the user with key $(n_1, 3)$, where the c_{11} is the encryption of $r_i \cdot m$ and c_{21} is the encryption of r_1.

With the same meaning and r_2 in place of r_1 you observe $c_{12} =$
$261159319903607217358312736685882260121917078945663664130083366485724005292 79$,
$c_{22} =$
$165004194429212341805735759293364678609320160295763909903261217749259047119 84$
being sent to the user with key $(n_2, 3)$ and finally $c_{13} =$
$373297816428041456230950694002673863193730021696549344636889255712601710671 43$,
$c_{23} =$
$223306649004190696215526304241787782700187006058466908800534231413822942223 73$ sent to the user with key $(n_3, 3)$ and using r_3 in place of r_1.

Compute the message m that Patty has encrypted to them.

Verify your answer by reencrypting m to at least one of the public keys.

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

You *do not need to* document intermediate steps in XGCD or CRT, or exponentiation or such.

You *do need to* say what numbers you do what computation on and why and you need to document the results of divisions, exponentiations, and CRT. Also document the commands you use in the computations.

6 Special signature system

Anna designs a special signature system based on the RSA assumption to be used for online exams. The exam has 3 diferent answer fields, leading to messages m_1, m_2, and m_3. After submitting the exam the student should receive a signature from the system that messages m_1, m_2, m_3, were received and the signature should be such that

- The student can convince the grader for exercise i that they submitted m_i without having to show them their other messages m_j for $j \neq i$.
- The student is bound to m_1, m_2, m_3, i.e., the student should not be able to produce a valid signature

for m_1', m_2', m_3', which is different in at least one m_i.

Here is the system she designs:

KeyGen:

1. Pick primes $p, q; p \neq q$.
2. Compute $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$.
3. Pick $1 < e < n$ with $\gcd(e, \varphi(n)) = 1$.
4. Compute $d \equiv e^{-1} \bmod \varphi(n)$.
5. Pick random integers $Z, S, R_1, R_2, R_3 \in (\mathbb{Z}/n)^\times$, i.e., coprime to n.
6. The public key is $(n, e, Z, S, R_1, R_2, R_3)$. The private key consists of d and the public key.

Sign:

1. To sign messages (m_1, m_2, m_3) pick a random $0 < v < \varphi(n)$ and compute $Q \equiv Z/(S^v R_1^{m1} R_2^{m2} R_3^{m3}) \bmod n$.
2. Compute $A \equiv Q^d \bmod n$.
3. Output (A, v) as signature.

Verify signature (A, v) on all (m_1, m_2, m_3)

1. Compute $Z' \equiv A^e S^v R_1^{m1} R_2^{m2} R_3^{m3} \bmod n$.
2. Output "true" if $Z' \equiv Z \bmod n$, else output "false".

Turn (A, v) into a signature on m_i

1. Compute $R = \prod_{j=1, j\neq i}^{3} R_j^{mj}$.
2. Output (A, v, R) as signature on m_i

Verify signature (A, v, R) on m_i

1. Compute $Z' \equiv A^e S^v R R_i^{mi} \bmod n$.
2. Output "true" if $Z' \equiv Z \bmod n$, else output "false".

6.0p a The public key is $n = 663861706567570333042052341$, $e = 65537$, $Z = 244192842881252214952755621$, $S = 15791926344074038583124008 2$, $R_1 = 149998982020844856869351866$, $R_2 = 619895325849876704368957058$, $R_3 = 621832299220421586386983761$.

Verify that $(A, v) = (40504662109642965842624439 8, 439743564773183987455743086)$ is a valid signature for $m_1 = 41755592377367284289256782 0$, $m_2 = 99272869200555325461494 36$, $m_3 = 41661695945811393494224046 1$.

You do not need to document the steps within each exponentiation but you need to show the results of each of the 5 exponentiations and what commands you used for the computation.

5.0p b Explain why a properly generated signature (A, v) passes verification for (m_1, m_2, m_3), i.e., explain why Z' computed in the verification step matches Z in the signer's public key.

3.0p c Explain why a signature (A, v, R) on m_i passes verification if (A, v) passes verification on (m_1, m_2, m_3) and R is properly computed.

6.0p d Student Jan has obtained (A, v) as a valid signature on (m_1, m_2, m_3) after submitting his answers. Unfortunately he notices that he got exercise 1 wrong and that the correct answer would be $m_1' \neq m_1$.

Find a way for Jan to produce a valid signature (A', v', R') on m_1' and explain how hard the computations are that he needs to do in order to compute it.