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 comuter 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/zEMWneajryx58yu
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 indered 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 $p = 10007$ with generator $g = 5$.

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 $a = 2518$.
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.

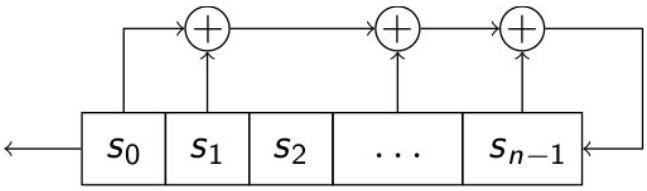
Bob's public key is $h_B = 5821$.
Compute the shared secret of Alice and Bob as an element of the integers modulo p, i.e. no application of the hash function is requred.

Answer

2 LFSR

This exercise is about LFSRs.

6.0p a For an LFSR of state length n given by a drawing as follows,



describe how you find the characteristic polynomial.

Note: You are not suposed to repeat the proofs, but describe the procedure of how you get the polynomial.

10.0p b You are given an LFSR of state length 17
via its characteristic polynomial
P(x) = (x^7 + x^6 + x^5 + x^3 + x^2 + x + 1) * (x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 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, 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 c What is the longest period generated by the LFSR from part b?

Make sure to justify your answer.

15.0p d State the lengths of all subsequences of the LFSR from part b) so that each state of 17 bits appears exactly once.

Make sure to justify your answer.

3 Symmetric systems

This exercise is about symmetric systems..

6.0p a Explain in your own words what goes wrong when a block cipher is used in ECB mode and why a block cipher needs to be used with a different mode of operation.

6.0p b In your own words, describe the difference between a MAC and a signature both in terms of what they achieve and what they require.

4 Message authentication codes

Charlie realizes that the weakness in his hash function from homework sheet 3 came from the fact that the key k was publicly known. He thus decides to rebrand his construction as a MAC.

His construction uses a block cipher
Enc: $\{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n$, where ℓ is the key length and n is the block length.

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

To compute MAC(m) using the key k that she shares with Bob, Alice first picks a random IV and then follows the computations as indicated by the diagram below. She then sends IV and MAC(m) along with m to authenticate message m.

5.0p a Describe how the MAC is computed, i. e., state MAC(m) as a function of the M_i, k, and IV.

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

5.0p b Eve obtains a message m and the matching $t =$MAC(m) and IV.

Show how she can use this information to find a different message m' for which she can produce a valid tag $t' =$MAC(m') and IV' without knowing the key k.

Note that the message m' must differ from m in at least one block.

5 Schoolbook RSA

This is an exercise about schoolbook RSA.

13.0p Patty invites three friends to her party. You know that they all use schoolbook RSA encryption, i.e., there is no padding in the message and that Patty sent the same message m to all three friends.

Their public keys are
$(n_1, e_1) =$
$(26076853516668117308994979027028880218616971929183804151970314334914474612431, 3), (n_2, e_2) =$
$(35502649610003692554201028256007082822675574831297820371244167622708884657263, 3),$ and
$(n_3, e_3) = (34648661536159444969987427715663335196678883123306428512444747333575722717163, 3)$.

You observe ciphertexts
$c_1 = 24638044348670340589306418254782284063206614439796392148786923592779824487 25, c_2 =$
$30837856998191621093018802199239492260736926818763395567633083609208973886618,$ and $c_3 =$
$25912217018638330108871222631238449838301660600139330973676625562334400499789$ encrypted to the public keys.

Compute the message m that Patty has encrypted to them.

Verify your answer by reencrypting m.

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 but you need to say what numbers you do what computation on and why.

6 Bad randomness

You find an implementation of the RSA cryptosystem with a creative way to generate primes.

First of all, there are only 61 bits of randomness and even those are not fully used. But the structure of the prime generation is more weird.

You find a constant $a = 3141592653589793239$ and see that all primes have a sepcial form:

First of all, some integer s is generated as
$s = 2^{63} + 2^{62} + 1 + 2 \cdot random(0, 2^{61} - 1)$, where the function $random(0, 2^{61} - 1)$ returns an integer in $[0, 2^{61} - 1]$. This random choice is repeated until s is prime. Then

$p = s2^{2 \cdot 64} + s_1 2^{64} + s_2$
with
$s_1 \equiv s \cdot a \bmod 2^{64}$,

$s_2 \equiv s \cdot a^2 \bmod 2^{64}$, is computed and tested for primality. If p is not prime, the process returns to computing a new s.

The second prime q is computed similarly
by sampling random numbers until
$t = 2^{63} + 2^{62} + 1 + 2 \cdot random(0, 2^{61} - 1)$
is prime. Then putting
$q = t2^{2 \cdot 64} + t_1 2^{64} + t_2$
with
$t_1 \equiv t \cdot a \bmod 2^{64}$, and
$t_2 \equiv t \cdot a^2 \bmod 2^{64}$
and testing q for primality. If q is not prime, the process returns to computing a new t.

6.0p a [Scroll up if you navigated here without seeing the exercise setting.]

Compute the prime starting from
$s = 15544563259347033551$.

Document the intermediate steps of your computation.

Note that this value is chosen already so that s is prime and that the p you will compute is also prime. However, you should check that both are prime. For that you can use your computer algebra system.

8.0p b Analyze the generation procedure and describe how you can find pieces of $s \cdot t$ in the expression $n = p \cdot q$.

Use this information to show how you can recover $s \cdot t$, and thus s and t, from $n = p \cdot q$.

Describe how can you factor n using this information.

Note that while 61 bits are not enough for security, a brute-force search through all prime s and t is not a valid solution.

Hint: Split the multiplication of two 64-bit numbers into pieces involving their high and low bits using $b \cdot c = (b_{\text{high}} \cdot 2^{32} + b_{\text{low}})(c_{\text{high}} \cdot 2^{32} + c_{\text{low}})$.

10.0pc You find RSA modulus

$n =$
$27301244608580338854539059998976941299986322121694309708069794802722046969855729922564000647477535$

generated by this method. Use your attack from the previous part to compute s and t and expand them to p and q.

Make sure to test that all the purported primes are prime and that n is the product of p and q.

Hint: Keep in mind the hint from above and also notice that integer multiplication involves carries.