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. 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 explaining 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/gKFDORxXA5Oek7I
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 RSA

This exercise is abou the RSA cryptosystem.

1.0p **a** Carry out the RSA key generation for primes p =1613 and q =1949 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** Aswer this question with $\varphi(n)$ in the setting of part a).

Answer

2.0p **c** Aswer this question with d in the setting of part a).

Answer

2.0p **d** Bob has public key $(n, e) = (1173031, 65537)$ and private key $(n, d) = (1173031, 378449)$. He receives ciphertext $c = 601090$ which was encrypted using schoolbook RSA to his public key. Decrypt c to compute the corresponding message.

Answer

2 Factorization

This exercise is about factoring integers. The integer n is a product of two primes.

1.0p **a** [Scroll up to see the settting of the exercise in case you navigated here without seeing it.]

Use the $p-1$ method to factor $n = 246106655759$ with base $a = 3875506$ and exponent s the lcm of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$.
Make sure to compute the value for s and to compute the result b of the exponentiation modulo n.

For this part filll in the value for s.

Answer

1.0p **b** This is a continuation of the previous exercise. For this answer fill in the value of b (the result after exponentiation, but before subtracting 1).

Answer

1.0p **c** This is a continuation of the previous exercise. Fill in the factor you obtained from the gcd.

Answer

1.0p **d** This is a continuation of the previous exercise. Fill in the other factor of n.

Answer

10.0p **e** This is a continuation of the previous exercise.

Explain why the $p-1$ method was successful in factoring this n.

Consider whether the exponent s would have worked for any base a for these factors and if not, give conditions for which a it does work and how restrictve these are.
Call p the factor you found under part c) and q the other factor of n.

- For what fraction of bases a does p divide the gcd?
- For what fraction of bases a does q divide the gcd?
- For what fraction of bases a does the algorithm succeed in factoring n?

Hint: To gvie a proper argument you will need to compute the factorizations of $p-1$ and $q-1$.

For the factorizations and other computations in this exercise you can use a computer algebra system (Sage, Pari-GP, ...). You do not need to run Pollard's rho method or such for obtaining factorizations. Make sure to state what computations you made,what the answers were, and how they help in solving this question.

3 Elliptic-curve discrete logarithm

This exercise is about the elliptic-curve discrete-logarithm problem (ECDLP).

For this exercise we will be considering an elliptic curve given in Weierstrass form $M : y^2 = x^3 + Ax^2 + x$ with $A = 471$ over the finite field $\mathbb{F}_p$ for $p = 3373$.
There are $n = 3440 = 2^4 \cdot 5 \cdot 43$ points on the curve over $\mathbb{F}_p$ and the group is cyclic.

A generator for the group is $P = [1278, 981]$. You are given $Q = [1043, 630]$, another point on this curve, and the task through this exercise is to compute the discrete logarithm of Q with base P, i.e., compute a with $Q = aP$.

12.0p a [Scroll up to see the definitions of M, P, Q etc. if you navigated here without seeing them.]

The following is - up to notation - a more detailed instruction of the Pohlig-Hellman computation for prime 2.

Compute $a \equiv a_{2,0} + a_{2,1}2 + a_{2,2}2^2 + a_{2,3}2^3 \bmod 2^4$ by first determining images of the base P and target Q in the subgroup of order 2 that allow to compute $a_{2,0}$, and then updating the target to another element of in the subgroup of order 2 to compute $a_{2,1}$ using the same table of multiples of P as in the first step. Continue the same for $a_{2,2}$ and $a_{2,2}$.

Explain your steps and verify your answer.

4.0p b [Scroll up to see the definitions of M, P, Q etc. if you navigated here without seeing them.]

Compute $a \bmod 5$.

12.0p c [Scroll up to see the definitions of M, P, Q etc. if you navigated here without seeing them.]

Let $\ell = 43$. Use the baby-step giant-step algorithm to compute $a \bmod \ell$.

For this, start by first determining images of the base P and target Q in the subgroup of order ℓ. Then compute and state the table of baby steps. Finally compute giant steps till you can compute $a \bmod \ell$.

Verify your answer.

4.0p **d** [Scroll up to see the definitions of M, P, Q etc. if you navigated here without seeing them.]

Combine the results from the previous three exercise parts to compute a with $Q = aP$. Verify your answer.

If you do not have all results, combine those that you do have and perform the verification on that part, i.e. in the matching subgroup.

5.0p **e** [Scroll up to see the definitions of M, P, Q etc. if you navigated here without seeing them.]

The elliptic curve M is a Montgomery curve. Compute the twisted Edwards curve E which is birationally equivalent to it and compute the images of P and Q on it, i.e., compute the coefficients a and d and images P_E and Q_E so that P_E and Q_E are on $E : ax^2 + y^2 = 1 + dx^2y^2$.

Verify that both image points satisfy this curve equation.

7.0p **f** This exercise uses the twisted Edwards curve E and points P_E and Q_E computed in exercise part e).

On E compute $3P_E$. Document the coordinates of intermediate points.

What does the result tell you about the discrete logarithm of Q_E with basis P_E?

4 Coppersmith's method

This exercise is about Coppersmith's method for factoring integers if part of a prime factor is known. Company C is implementing RSA for encryption. They have a random number generator that outputs 40 bits at once. They use primes p and q of 123 bits, generated as follows:

For each prime they generate 3 blocks of 40 bits, B_0, B_1, and B_2. Then the compute the odd integer $3 \cdot 2^{121} + B_2 \cdot 2^{81} + B_1 \cdot 2^{41} + B_0 \cdot 2 + 1$, check for primality, and increment by 2 until the primality proof returns that the number is prime.

You learn that their random number generator often has problems starting up and that they generate the blocks in this order: first B_2, B_1, and B_0 for p and then for q.

6.0p a Compute p following the above instructions for $B_2 = B_1 = 0, B_0 = 727630662689$.

Make sure to obtain a prime and to document how you ensure this.

7.0p b Explain how and why you can compute p from n given the above information if $B_2 = B_1 = 0$.

The solution does not require knowledge of how q was generated.

Note that generic factoring methods such as Pollard rho, p-1, or NFS do not count as solutions. Those take too long for the numbers generated here, even though these are smaller than recommended for proper RSA.

8.0p c The RSA modulus $n = 698194396347186616845744692889297606150908831129606585503540411883011540 79$ was generated using the above approach and for p the blocks B_2 and B_1 ended up as 0.

Compute the factors p and q of n.

Make sure to document all computation and results.

5 Elliptic-curve signatures

This exercise is about the elliptic-curve signature algorithm ECDSA.
As a reminder, ECDSA works on a fixed elliptic curve E given in Weierstrass form over a finite field $\mathbb{F}_p$ for a prime p. The point P is on E and has prime order ℓ. The system parameters are p, E, P, and ℓ. ECDSA has the following components:

KeyGen:
Pick random $1 < a < \ell$ as private key.
Compute public key $Q = aP$.

Sign:
Pick random $1 < r < \ell$.
Compute $R = rP$.
Let $R' = x(R) \bmod \ell$, i.e., R' is the x-coordinate of R taken as an integer and then reduced modulo ℓ.
Compute $s \equiv r^{-1}(H(m) + R'a) \bmod \ell$, where H is a cryptographic hash function.
Output the signature (R', s).

Verify:
Compute $w_1 \equiv s^{-1}H(m) \bmod \ell$ and $w_2 \equiv s^{-1} \cdot R' \bmod \ell$.
Accept the signature as valid if $x(w_1P + w_2Q) \equiv R' \bmod \ell$, i.e. if the x-coordinate of $w_1P + w_2Q$ equals the first component of the signature.

5.0p a Explain in your own words and with formulas why a correctly generated signature is accepted as valid.

10.0p b Assume that at some later time Eve wants to be able to claim that the signature on m_1 was actually a signature on m_2. In principle this is not possible because of the use of hash functions, but she notices that only the x-coordinate of R is used. This gives her an idea of how to circumvent the signature system if she fixes the two messages before generating her key.

Let $h_1 = H(m_1)$ and $h_2 = H(m_2)$. Show how Eve can choose her private key a and nonce r so that the signature (R', s), computed using a and r verifies correctly for m_1 and m_2.

Note: Eve is not powerful enough to break discrete logarithms on E and the hash function is a strong cryptographic hash function. You need to use properties of ECDSA to solve this exercise.

Hint: Compute a as an expression in h_1, h_2, and r.