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
  - 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 exception you may contact Tanja Lange if you encounter any problems.
- You may visit the bathroom during the exam time and you may have food and drink on your desk.

Instructions for answering 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 explaning your solution. Choose 3 exercise parts which are not numerical questions and aim for 5 min of recordinng (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/FFqRc3CGR2VbIZG
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 $p = 1000003$ with generator $g = 2$.

2.0p a Alice picks variable $a = 322470$.
Compute Alice's publlic key h_A.

Thiis is a copy of the description above as the Ans Deft review after the exam does not seem to show the problem descriptions:
This question is about the Diffie-Hellman key exchange. Alice and Bob
use this system in the multiplicative group $\mathbb{F}_p^*$ for $p = 1000003$ with generator $g = 2$.

Answer

2.0p b Bob's public key is $h_B = 55013$. 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 Discrete logarithm

This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 29009$.

The element $g = 11$ has order $p - 1$. The factorization of $p - 1$ is $p - 1 = 2^4 \cdot 7^2 \cdot 37$.

Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 12542$, i.e. perform the following exercises.

4.0p a In your own words, give a short explanation of how and why the Pohlig-Hellman attack works and why the steps below allow you to compute all of b (modulo $p - 1$).

Thiis is a copy of the description above as the Ans Deft review after the exam does not seem to show the problem descriptions
This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 29009$.

The element $g = 11$ has order $p - 1$. The factorization of $p - 1$ is $p - 1 = 2^4 \cdot 7^2 \cdot 37$.

Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 12542$, i.e. perform the following exercises.

8.5p b The following is - up to notation - a more detailed instruction of the Pohlig-Hellman computation for prime 2.

Compute $b \equiv b_{2,0} + b_{2,1}2 + b_{2,2}2^2 + b_{2,3}2^3 \bmod 2^4$ by computing each bit $b_{2,i}$ separately; i.e., by first determining elements in the group of order 2 that give b_0, then updating the target to another element in the group of order 2 to get $b_{2,1}$, then updating the target to another element in the group of order 2 to get $b_{2,2}$, and finally updating the target to another element in the group of order 2 to get $b_{2,3}$. For each step state elements of the correct order.

Combine the results to compute b modulo 2^4.

Verify your answer. State clearly why this calculation verifies the result.

7.0p c Compute $b \equiv b_{7,0} + b_{7,1}7 \bmod 7^2$ by first determining images of the base g and target h in the subgroup of order 7 that allow to compute $b_{7,0}$, and then updating the target to another element of order 7 to compute $b_{7,1}$ using the same table of powers of g as in the first step.

Explain your steps and verify your answer.

12.5p d Use the Pollard-rho method with Floyd's cycle finding method to compute b modulo 37.

Let G and H be the generator and target in the group of order 37 and choose starting point G^s with $s = 31$.

Note: This exercise is auto-generated so that you should find a collision after 4 steps. You are supposed to do the steps of the algorithm, even if you "see" the result from G and H.

The step function is defined as a multiplicative walk with 5 precomputed steps, $s_i = G^{ri} H^{ti}$ for
$r_0 = 3, r_1 = 25, r_2 = 12, r_3 = 4, r_4 = 9$,
$t_0 = 17, t_1 = 13, t_2 = 25, t_3 = 10$, and $t_4 = 32$.
Step s_i is chosen if the current element, considered as an integer in $[0, p-1]$ is congruent to i modulo 5.

First compute the 5 precomputed steps.

Then compute the steps of the slow and fast walk until you find a collision.

3.0p e In the setting of the previous exercise part compute $b \bmod 37$ from the exponents of the fast and slow walk. Verify your result.

3.0p f Combine the results above to compute b.
Document your steps.

Verify your answer.

3 Factorization

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

1.0p a Use the $p-1$ method to factor $n = 14802907667$ with base $a = 934311$ and exponent s the lcm of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.
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.

Thiis is a copy of the description above as the Ans Deft review after the exam does not seem to show the problem descriptions:
This exercise is about factoring integers. The integer n is a product of two primes.

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

9.5p d 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.

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.

4 Edwards curves

This exercise is about twisted Edwards curves.

8.0p a Point $P=(172,161)$ is on the twisted Edwards curve $E: 83x^2+y^2=1+149x^2y^2$ over the field $\mathbb{F}_p$ with $p=239$.

Compute $3P$. Make sure to state how you compute this and include enough intermediate results to make it possible to follow your computation.
For each intermediate point that you compute, verify that it is on the curve.

Thiis is a copy of the description above as the Ans Deft review after the exam does not seem to show the problem descriptions:
This exercise is about twisted Edwards curves.

6.0p b Let $\tilde{E} : x^2 + y^2 = 1 + dx^2y^2$ be an Edwards curve over a finite field $\mathbb{F}_p$, where d is not a square. Explain how to find a Montgomery curve that is birationally equivalent to $\tilde{E}$ and how to map all points of the Edwards curve over $\mathbb{F}_p$ to points on the Montgomery curve in a way that respects point addition. Make sure to investigate which points are exceptional points of the main map and how to handle them.

Note: You are not supposed to do this computation for a concrete curve but should describe the steps you would take.

10.0p c You are given a point $Q = (x_Q, y_Q)$ on an Edwards curve $\bar{E} : x^2 + y^2 = 1 + dx^2y^2$ over a finite field $\mathbb{F}_p$ with d not a square in that field. You also know that there are 120 points on $\bar{E}$ and that the group is cyclic.

Explain how you can determine the order of Q with as little computation as possible.

Use the symmetries and points of known order to reduce computations.

5 Access control with RSA

This question presents you with the cryptographic details of an access control protocol.

To let you compute efficiently and to let Ans Delft generate parameters, the RSA modulus n is only 180 bits. Your attacks have to work for cryptographic sizes of n. Solutions factoring n will not be accepted.

Systems engineer Steve is tasked with setting up a new access control system for building access. The old system used DES with 56-bit keys and each user U already has a smart card which holds their personal access secret u. These per-user secrets are registered with the central computer.

Steve is concerned about Eve sniffing the connection and has learned that DES is outdated. The smart card offers support for RSA encryption, so he lets the server generate an RSA key pair (n, e) and (n, d) and puts (n, e) on the smart card along with the personal access secret u per user.

Because the smart card is a small computation device he chooses $e = 3$ to make the encryption comptuation fast. He knows that short messages are risky with such a small exponent, so he devises padding schemes. Finally he is concerned about Eve simply replaying a message, so he chooses to vary the padding.

3.5p a Steve's first scheme assumes that the smart card and the server can keep track of how many messages have been sent. He constructs the i-th message for user U with secret u as $m_i = u \cdot 2^{123} + i$, where u is taken as a 56-bit integer.

You are Bob. Your user secret is $b = 34100010166843172$. Compute m_i for $i = 1909$ and encrypt this plaintext to the server key $(n, e) = (135304092231989671072994844074211352614066206912423757 1, 3)$.

Thiis is a copy of the description above as the Ans Deft review after the exam does not seem to show the problem descriptions:
This question presents you with the cryptographic details of an access control protocol.

To let you compute efficiently and to let Ans Delft generate parameters, the RSA modulus n is only 180 bits. Your attacks have to work for cryptographic sizes of n. Solutions factoring n will not be accepted.

Systems engineer Steve is tasked with setting up a new access control system for building access. The old system used DES with 56-bit keys and each user U already has a smart card which holds their personal access secret u. These per-user secrets are registered with the central computer.

Steve is concerned about Eve sniffing the connection and has learned that DES is outdated. The smart card offers support for RSA encryption, so he lets the server generate an RSA key pair (n, e) and (n, d) and puts (n, e) on the smart card along with the personal access secret u per user.

Because the smart card is a small computation device he chooses $e = 3$ to make the encryption comptuation fast. He knows that short messages are risky with such a small exponent, so he devises padding schemes. Finally he is concerned about Eve simply replaying a message, so he chooses to vary the padding.

8.0p b You are Eve and observe three consecutive accesses by Victor. The public key of the system is $(n, e) = (135304092231989671072994844074211352614066206912423757 1, 3)$ (same as above) and the padding scheme is the same as in part a.

Find an attack to obtain Victor's user secret v given the consecutive ciphertexts
$c_j = 164867525413631686108542244605590332657131844994186648$,
$c_{j+1} = 669330273667331356154438891368274712878935740757554990$, and
$c_{j+2} = 853109242122207805055956523445529343243869885591747755$.

Explain how and why your attack works and use it to obtain v.

Hint: explore the algebraic relalations between the ciphertexts knowing that they are consecutive and using the same v.

Note that you do not know j but it is significantly below 2^{123} so v will be the top 56 bits of m_j once you have decrypted c_j.

10.0p c Steve has noticed that keeping counters on the server and the smart card is complicated, and he has noticed Eve in the building. The latter means that he is in a rush to issue new secrets and to update the protocol.

His random-number generator is slow, so he decides that 30-bit per-user secrets need to suffice. He changes the protocol to be interactive and have the server send a 80-bit challenge integer s to the card and to open the door, if the card can reply with an encryption of $m = s \cdot 2^{99} + u$ for one of the registered user secrets u. He keeps the RSA key $(n, e) = (1353040922319896710729948440742113526140662069124237571, 3)$ as before.

You are Eve and observe Alice entering the bullding after having received $s = 661795599945365472793374$ and answered with $c = 1304427715737794183639527703843118636234043562220564999$.

Find a new attack to compute Alice's user secret a from s, c and the RSA key.

Explain how and why your attack works and use it to obtain a.

Hint: This is a different attack than in the previous exercise part (different length and position of the secret, you only have one ciphertext).