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 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/uWvzGC0mGsnfNsc
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.

0.5p a Carry out the RSA key generation for primes p =1993 and q =1153 and exponent $e = 2^{16} + 1$. The results will be used in this and the following 2 exercise parts.

Answer this questions with n.

Answer

0.5p b Aswer this questionn with $\varphi(n)$ in the setting of part a).

Answer

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

Answer

2.0p d Bob has public key $(n, e) = (2831813, 65537)$ and private key $(n, d) = (2831813, 1759553)$. He receives ciphertext $c = 1517117$ which was encrypted using schoolbook RSA to his public key. Decrypt c to compute the corresponding message.

Answer

2 Discrete logarithm

This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 22916251$.

The element $g = 10$ has order $p - 1$. The factorization of $p - 1$ is $p - 1 = 2 \cdot 3^3 \cdot 5^4 \cdot 7 \cdot 97$.

Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 14876484$, i.e. perform the following exercises.

2.0p a [Scroll up to see the definitions of p, g, h etc. if you navigated here without seeing them.]

Compute $b \equiv b_{2,0} \bmod 2$.

2.0p b You learn that $b \equiv 14 \bmod 27$. Verify this answer.

12.0p c

The following is - up to notation - a more detailed instruction of the Pohlig-Hellman computation for prime 5 .

Compute $b \equiv b_{5,0} + b_{5,1}5 + b_{5,2}5^2 + b_{5,3}5^3 \bmod 5^4$ by first determining images of the base g and target h in the subgroup of order 5 that allow to compute $b_{5,0}$, and then updating the target to another element of in the subgroup of order 5 to compute $b_{5,1}$ using the same table of powers of g as in the first step. Continue the same for $b_{5,2}$ and $b_{5,2}$.

Explain your steps and verify your answer.

14.5p d Use the Pollard-rho method with Floyd's cycle finding method to compute b modulo 97.

Let G and H be the generator and target in the group of order 97.

The step function is defined as a multiplicative walk with 5 precomputed steps, $s_i = G^{r_i} H^{t_i}$ for
$r_0 = 10, r_1 = 95, r_2 = 15, r_3 = 1, r_4 = 14$,
$t_0 = 84, t_1 = 1, t_2 = 28, t_3 = 84$, and $t_4 = 67$.

First compute the 5 precomputed steps.

Then compute the steps of the slow and fast walk until you find a collision. Choose $x_0 = G^s$ with $s = 6$ as starting point for the slow and the fast walk.

The walk chooses step s_i if the current position x , considered as an integer in $[0, p-1]$ is congruent to i modulo 5.
This means $x \mapsto x \cdot s_{x \bmod 5}$.

Make sure to compute the exponents so that at every moment it holds that $x_i = G^{a_i} H^{c_i}$.

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 earlier.

3.0p e In the setting of the previous exercise part compute $b \bmod 97$ from the exponents of the fast and slow walk. Verify your result.

4.0p f Combine the results above together with the information that $b \equiv 2 \bmod 7$ to compute b.
Document your steps.

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.

3 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 $n = 626583719$ with base $a = 16661$ and exponent s the lcm of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$.
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

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.

7.5p a Points $P = (187, 317)$ and $Q = (352, 66)$ are on the twisted Edwards curve $E : 456x^2 + y^2 = 1 + 283x^2y^2$ over the field $\mathbb{F}_p$ with $p = 547$.

Compute $2P + Q$. 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.

8.5p b For the twisted Edwards curve above, $E : 456x^2 + y^2 = 1 + 283x^2y^2$ over $\mathbb{F}_p$ with $p = 547$ compute the coefficients of a Montgomery curve that is birationally equivalent to E. Show how to map all points of the twisted 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 any concrete point but describe it for all points of E that are defined over $\mathbb{F}_p$.

10.0p c You are given a point $R = (x_R, y_R)$ 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 72 points on $\bar{E}$ over $\mathbb{F}_p$ and that the group is cyclic.

Explain how you can determine the order of R on $\bar{E}$ with as little computation as possible.

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

5 Not so random primes

Benjamin, the Ans developer, thinks that 32 bits of randomness is enough for everybody, even for RSA key generation.

You don't know the full details of the implementation but learn that he generates the first prime p for the RSA cryptosystem by picking a 32-bit random number r, putting $p' = \lfloor \pi \cdot 10^{39} \rfloor \cdot 10^{11} + 2r + 1$ and then repeatedly adding 2 to p' until hitting a prime

You don't know how the second prime is generated.

5.0p a [Scroll up to see the description of the exercise in case you navigated here without seeing it.]

Compute the prime that Benjamin's program finds for $r = 4174787949$.

For clarity: $\lfloor \pi \cdot 10^{39} \rfloor = 314159265358979323846264338327950288419 7$.

Use the primality test of your computer algebra system, such as `p.is_prime()` in Sage and `isprime(p)` in Pari-GP, on p'.

This should take 5 update steps.

7.0p b Describe how you can factor RSA numbers $n = p \cdot q$ generated by Benjamin's program.

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.

7.0p c You learn that $n = 85397342226735670654635508695465744950338290459323016319434988214268887865669909148767449445636761$ has been generated using Benjamin's implementation. Find the factors p and q of n.