TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 04 February 2025

Name :

TU/e student number :

Exercise	1	2	3	4	5	total
points						

Notes: Please hand in *this sheet* at the end of the exam. You may keep the sheets with the exercises.
This exam consists of 5 exercises. You have from 18:80 – 21:00 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps and intermediate results, in particular of algorithms, on the exam paper, do not use the scrap paper. It is not sufficient to state the correct result without the explanation and the steps that lead to it. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are allowed to use any books, printouts, and notes on paper, e.g. your homework. You are not allowed to use the textbooks of your colleagues.
You are allowed to use a calculator without networking abilities. Usage of personal laptops and cell phones is forbidden. You can use the laptops provided in the exam room.

1. This problem is about the Diffie–Hellman key exchange. The system parameters are a prime $p = 1019$ and generator $g = 2$ of $\mathbb{F}_p^*$.

   (a) Alice chooses $a = 196$ as her private key, compute her public key. 2 points

   (b) Bob uses public key $h_B = 44$. Compute the shared DH key between Bob and Alice. 2 points

2. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 2113$. The element $g = 5$ has order $p-1 = 2112$. The factorization of $p-1$ is $p-1 = 2^6 \cdot 3 \cdot 11$. Use the Pohlig-Hellman attack to compute the discrete logarithm a of Alice's key $h_A = g^a = 412$, i.e., perform the following steps.

   (a) Compute a modulo 2^6 by first computing a modulo 2, then modulo 2^2, then modulo 2^3, then 2^4, then 2^5, and finally modulo 2^6.
   Verify your answer.
   Reminder: Document all steps, that includes the steps during verification. 15 points

   (b) Compute a modulo 3 4 points

   (c) Compute a modulo 11. 3.5 points

   (d) Combine the results above to compute a.
   Verify your answer.
   If you have only two parts of the result combine those and verify your result on the matching subgroup. 3.5 points

3. This exercise is about factoring.

   (a) Use the $p-1$ method to factor $n = 229043$ with basis $a = 4$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Make sure to state the value for s and the result of the exponentiation modulo n. Determine both factors of n. 4 points

   (b) The factorization of 226 is $226 = 2 \cdot 113$ and that of 1008 is $1008 = 2^4 \cdot 3^2 \cdot 7$. Explain why the factorization in (a) was successful and explain what fraction of bases a works to factor n. 5 points

(c) Use Pollard's rho method for factoring to find a factor of 77 with iteration function $x_{i+1} = x_i^2 + 6$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 77)$ until a non-trivial gcd is found. Start with $x_0 = 37$ and compute both factors.

8 points

4. The Edwards curve

$$E : x^2 + y^2 = 1 - 4x^2y^2$$

over $\mathbb{F}_{19}$ has 24 points

(a) Find all affine points, i.e. points of the form (x, y), on E.

9 points

(b) The point $P = (9, -6)$ is on the curve. Compute the order of P.
Hint: You may use information learned about the order of points on (twisted) Edwards curves.

9 points

(c) Translate the curve to Montgomery form **and** compute the image P' of P on that curve

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u,$$

i.e. compute A, B and the resulting point P' on $M_{A,B}$.
Verify that the resulting point P' is on the Montgomery curve.

5 points

(d) In (b) you computed $2P$ on E and in (c) you computed the image P' of P on $M_{A,B}$. Compute the image of $2P$ on $M_{A,B}$ and then on $M_{A,B}$ from (c) double P' to compute $2P'$ directly. Compare the results.

6 points

5. This exercise is about Coppersmith's attack for stereotyped messages.

   (a) Explain in your own words how Coppersmith's attack for stereotyped messages works to recover the missing plaintext bits in the situation where the bottom bits are missing and exponent $e = 3$ is used.

   For concreteness consider the following situation: Alice has key $(n, e) = (n, 3)$ with n an integer of 4096 bits. Alice receives an encrypted message from Bob and Eve knows all but the bottom k bits of the plaintext message because it has some fixed format and only the last part varies.

   Explain how you set up the 4×4 matrix.
   Make sure to state all the steps you need to do incl. what the entries of this matrix are.

   8 points

   (b) Explain with calculations, the theorem of Howgrave-Graham, and estimates on the length of outputs from LLL how many of the 4096 message bits must be known in order for the attack to work.

   10 points

   (c) Bob learns about Coppersmith's attack and changes the format of his messages. He still starts with a fixed part on the left but then repeats the actual contents of the message 6 times, spaced by 512 bits.

   Let F be the known fixed part of the message and $0 < M < 2^{512}$ be the message he wants to send. He first prepares the encoding of M as

$$m = \sum_{i=0}^{5} M 2^{512i} + F 2^{3072}$$

   and then computes $c \equiv m^3 \bmod n$ as usual.

   Show how Eve can adapt Coppersmith's method to this situation and still recover M given c, F, and Alice's public key (n, e), where n has 4096 bits.

   6 points