TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 23 January 2024

Name :

TU/e student number :

Exercise	1	2	3	4	5	6	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 6 exercises. You have from 13:30 – 16:30 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps by giving intermediate results and stating what they compute, in particular of algorithms. It is not sufficient to state the correct result without the explanation. 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 $a = 123$ as her private key, compute her public key. [2 points]

   (b) Bob uses public key $h_B = 38$. 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 $h_A = g^a = 592$, 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. [15 points]

   (b) Compute a modulo 3 [4 points]

   (c) Compute a modulo 11. [3 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. [4 points]

3. This exercise is about factoring.

   (a) Use the $p-1$ method to factor $n = 208363$ with basis $a = 6$ 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 2062 is $2062 = 2 \cdot 1031$ and that of 100 is $100 = 2^2 \cdot 5^2$. Explain why the factorization in (a) was successful and explain what fraction of bases a works to factor n. [5 points]

(c) To prove that $q = 1031$ is prime using the Pocklington primality proof we need to factor $q - 1 = 1030 = 2 \cdot 5 \cdot 103$ which in turn requires us to factor $102 = 2 \cdot 51$.

Use Pollard's rho method for factoring to find a factor of 51 with iteration function $x_{i+1} = x_i^2 + 5$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 51)$ until a non-trivial gcd is found. Start with $x_0 = 5$ and compute both factors.

8 points

(d) In class we used Pocklington's primality proof to show that 103 is prime. Use this result in Pocklington's primality proof to show that 1031 is prime. Use basis $a = 2$. Make sure to document your tests of all conditions. 4 points

4. The twisted Edwards curve

$$E : -x^2 + y^2 = 1 + 6x^2y^2$$

over $\mathbb{F}_{17}$ has 20 points

(a) The point $P = (10, 9)$ 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

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

Alice has key $(n, e) = (n, 5)$ 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.

(a) Explain in your own words how Coppersmith's attack for stereotyped messages works to recover the missing plaintext bits in the situation above, i.e., for exponent $e = 5$, for the basic setup using a 6×6 matrix.
Make sure to state all the steps you need to do incl. what the entries of this matrix are.

9 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.

11 points

6. You are called to investigate a data breach. Here is what you find:

The server connections use a Montgomery curve

$$E_M : y^2 = x^3 + Ax^2 + x$$

over a finite field $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$. The curve has order 4ℓ for ℓ a large prime and the implementation uses x-coordinate arithmetic with the Montgomery ladder and differential addition and doubling. This means, the server publishes the x-coordinate x_P of a point $P = (x_P, y_P)$ of order ℓ and the x-coordinate x_Q of its public key $Q = aP = (x_Q, y_Q)$. Remember that the Montgomery ladder formulas only use the x-coordinate, so y is not needed. Here are the formulas for differential addition and doubling: Let $P_3 - P_2 = P_1$ and let P_i have x-coordinate x_i. Then the x-coordinate of $P_4 = 2P_2$ is $x_4 = (x_2^2 - 1)^2/(4x_2(x_2^2 + Ax_2 + 1)$ and the x-coordinate of $P_5 = P_2 + P_3$ is $x_5 = (x_2x_3 - 1)^2/(x_1(x_2 - x_3)^2)$.

You were called because the private key has leaked. You check the logs to see if there is anything suspicious so that you could understand what broke the system. What you expect to see is recordings of Diffie–Hellman key exchanges, so you expect to see a received x-coordinate x_R from some user who computed $R = bP = (x_R, y_R)$, then the computation of the x-coordinate of aR (and a matching bQ on their side) resulting in a connection using a symmetric key derived from $aR = bQ$.

Instead, you notice that there are many connections that break as soon as a packet after the DH computation is received from the other user because they do not use the correct symmetric key. Looking deeper, you see many connections with the same x_R until one of then succeeds on the first symmetric message and then that connection is closed by the other side and the records show a similar sequence, now with a different repeated x coordinate, again until eventually the connection succeeds, and then the next, and the next, and the next.

You also notice that there are no points on the curve E_M with any of these suspicious x-coordinates. You pick up a book and learn the following about quadratic twists of curves: Each curve has a quadratic twist, a curve $\bar{E}$ which is closely related to E and in particular has $\bar{E}| = 2p + 2 - |E|$ points and equation $-y^2 = x^3 + Ax^2 + x$.

While the order of the curve E_M chosen by the server is secure for cryptographic purposes, that of the quadratic twist is not; In this case it has many small primes as factors and none of them is larger than 2^{20}. You suspect that this active attack is somehow using that the group order of the twist has many small factors.

The following exercises give first an example with small numbers for you to try your ideas of how the attack works and then asks for the full explanation.

(a) For a concrete, yet very small example take $p = 1019, E_M : y^2 = x^3 + 82x^2 + x$ with $4 \cdot 251$ points. Its quadratic twist has $4 \cdot 7 \cdot 37$ points. The base point of order 251 on E_M is specified as $x_P = 326$, coming from $P = (326, 161)$. The server's public key is $x_Q = 106$.

The points the server received have x-coordinates $x_{R1} = 62$ for the first batch and $x_{R2} = 401$ for the second batch. Your records show that the server computed the shared Diffie–Hellman value ∞ for the first one, meaning that $aR_1 = \infty$, and 560 for the second one, meaning that aR_2 has x-coordinate 560.

From this information, compute the server's private key.

Hint: The Montgomery differential addition formulas do not use the B in $By^2 = x^3 + Ax^2 + x$.

Hint: Compute the order of the points which you received, i.e., of the points with x-coordinates x_{R1} and x_{R2}.

10 points

(b) Explain how an active attacker, i.e., one who interacts with the server, can compute the server's secret key in a way that is consistent with the data you observe.

Hint: The sender finds out if the symmetric key that they computed is correct based on whether the connection continued to dropped.

10 points