TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 31 October 2023

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 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, 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 RSA encryption.

   (a) Alice chooses $p = 521$ and $q = 331$. Compute Alice's public key (n, e), using $e = 65537$, and the matching private key (n, d). [2 points]

   (b) Bob uses public key $(n, e) = (165157, 65537)$ and $d = 2753$. He receives ciphertext $c = 82114$.
   Decrypt the ciphertext. Verify your answer by re-encrypting the message. [2 points]

   (c) Decrypt the same message as under b) but this time using RSA with CRT for $p = 521$ and $q = 317$. Make sure to document your computation, i.e., state the values for $u, c_p, d_p, \ldots$ [5 points]

2. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 3313$. The element $g = 11$ has order $p - 1 = 3312$. The factorization of $p - 1$ is $p - 1 = 2^4 \cdot 3^2 \cdot 23$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 2345$, i.e. perform the following steps.

   (a) Compute b modulo 2^4 by first computing b modulo 2, then modulo 2^2, then modulo 2^3 and finally modulo 2^4.
   Verify your answer. [9 points]

   (b) Compute b modulo 3^2, by first computing it modulo 3 and then, using the same table of powers of g, computing it modulo 3^2.
   Verify your answer. [6 points]

(c) Compute b modulo 23 using the Pollard-rho method in the schoolbook version with Floyd's cycle-finding method, on $G = g^{(p-1)/23}$ and $H = h^{(p-1)/23}$. The fast and slow walk both start at $s_0 = f_0 = G^3H^2, a_0 = 3, b_0 = 2$.

$$s_{i+1} = \begin{cases} s_i \cdot G \\ s_i \cdot H \\ s_i^2 \end{cases}, a_{i+1} = \begin{cases} a_i + 1 \\ a_i \\ 2a_i \end{cases}, b_{i+1} = \begin{cases} b_i \\ b_i + 1 \\ 2b_i \end{cases} \text{ for } s_i \equiv \begin{cases} 0 \bmod 3 \\ 1 \bmod 3 \\ 2 \bmod 3 \end{cases},$$

where to select the step one takes s_i as an integer in $[0, p-1]$.
The twice as fast walk has $f_i = s_{2i}$.
Document all s_i you compute and verify the answer for b mod 23.
Hint: Remember that you need to wait for a collision between s_i and f_i at the same i even if you see the same values appear already earlier – bubt the latter still simplifies your computation as you know what step to take next and you see the collision coming. Here you will need 5 steps. **12 points**

(d) Combine the results above to compute b.
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) Explain in your own words how the $p-1$ method works to factor $n = p \cdot q$ and why it works.
Make sure to state and explain the conditions on a, s and how this relates to $p-1$ and $q-1$. **6 points**

(b) Use the $p-1$ method to factor $n = 165157$ with basis $a = 5$ 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**

(c) The factorization of 520 is $520 = 2^3 \cdot 5 \cdot 13$ and that of 316 is $316 = 2^2 \cdot 791$. Explain why the factorization in (b) was successful and explain what fraction of bases a works to factor n. **5 points**

4. (a) Find all affine points, i.e. points of the form (x, y), on the Edwards curve
$$E : x^2 + y^2 = 1 + 5x^2y^2$$
over $\mathbb{F}_{23}$. 11 points

   (b) The point $P = (19, 6)$ is on the curve. Compute the order of P.
Hint: You may use information learned about the order of points on Edwards curves. 7 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 uses the following method to generate RSA moduli $n = p \cdot q$ with p, q of ℓ bits having the top up to $\ell - 2$ bits of n fixed to a user-chosen bit string s (having in a 1 in the most-significant position because otherwise the length of n would be smaller). This idea was described by A. Lenstra in Asiacrypt 1998.

   Let $N = s2^{\ell+2}$ be the integer having the user-chosen string of bits s in the top $\ell - 2$ positions followed by 0s. Let p be a randomly chosen prime of ℓ bits. Compute $N' = \lceil N/p \rceil p$, the smallest multiple of p larger than N, and let $q' = N'/p$. Put q the next prime larger than q' and $n = p \cdot q$. If n fails to have the correct bit pattern, start with a new choice of p.

   You find an RSA implementation which combines ECC, RSA, and symmetric authenticated encryption. The implementation uses points P, Q on the Weierstrass curve $W : v^2 = u^3 + a_4u + a_6$. in a finite field K. Here are the steps taken in key generation

   [Step 1] Pick a random r and compute $R = rP$ on W.

[Step 2] Compute $S = rQ$ and $k = \mathsf{hash}(u(S))$, where $u(S)$ denotes the u-coordinate of S..

[Step 3] Pick a random prime p of ℓ bits, let p_T denote the top 2/3 bits of p.

[Step 4] Pick a random IV of 128 bits. Compute the symmetric encryption of p_T using key k and the IV and compute an authentication tag t of 128 bits.
Note that $c = \mathsf{Enc}(k, p_T)$ has the same length as p_T.

[Step 5] Let s be the bit string $u(R)||IV||c||t$, where $||$ denotes concatenation.

[Step 6] Use Lenstra's method to compute the RSA modulus n with n having its top bits match s and having p as one of its factors.

[Step 7] Complete the rest of RSA KeyGen by computing d.

(a) Show that this method can work for $\ell = 2048$ and K a field of 256 bits, i.e., show that there is enough space in n to accommodate all of s and successfully find a matching prime q. 6 points

(b) You grow suspicious of this method. Show how this method can work to leak information on p and q from n and explain what extra information the backdoor owner needs in order to break RSA keys generated by this method. 10 points