TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 29 October 2019

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 sheet 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, 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 and notes, 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 uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 25801$. The element $g = 7 \in \mathbb{F}_{25801}^*$ has order 25800 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 314$ as her secret key. Compute Alice's public key h_A. 2 points

   (b) Alice receives $h_B = g^b = 11245$ from Bob as his Diffie-Hellman keyshare.
   Compute the key shared between Alice and Bob, using Alice's secret key a from the first part of this exercise. 2 points

2. This problem is about RSA encryption.

   (a) Alice chooses $p = 521$ and $q = 331$. Compute Alice's public key (n, e), using $e = 7$, and the matching private key d. 2 points

   (b) Bob uses public key $(n, e) = (396553, 17)$ and secret key $d = 302273$. He receives ciphertext $c = 234040$.
   Decrypt the ciphertext. Verify your answer by re-encrypting the message. 3 points

   (c) Decrypt the same message as under b) but this time using RSA with CRT for $p = 733$ and $q = 541$. Make sure to document your computation, i.e., state the values for $c_p, d_p, \ldots$ 5 points

3. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 25801$. The element $g = 7$ has order $p - 1 = 25800$. The factorization of $p - 1$ is $p - 1 = 2^3 \cdot 3 \cdot 5^2 \cdot 43$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 11245$, i.e. perform the following steps.

   (a) Compute b modulo 2^3 by first computing b modulo 2, then modulo 2^2 and finally modulo 2^3.
   Verify your answer. 6 points

   (b) Compute b modulo 3. 2 points

   (c) Compute b modulo 5^2 by first computing b modulo 5 and then modulo 5^2 using the same table of powers of g.
   Verify your answer. 6 points

(d) Compute b modulo 43 using the Pollard-rho method in the schoolbook version, on $G = g^{(p-1)/43}$ and $H = h^{(p-1)/43}$, starting with $t_0 = G, a_0 = 1$, and $b_0 = 0$.

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

where to select the step one takes t_i as an integer in $[0, p-1]$. The twice as fast walk has $r_i = t_{2i}$.
Verify your answer. 10 points

(e) Combine the results above to compute b.
Verify your answer. 4 points

4. This exercise is about factoring.

(a) Use the $p-1$ method to factor $n = 396553$ with basis $a = 8$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. 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 540 is $540 = 2^2 \cdot 3^3 \cdot 5$ and that of 732 is $732 = 2^2 \cdot 3 \cdot 61$. Explain why the factorization in (a) was successful. **Hint:** Check whether $a = 2$ would have worked.

4 points

(c) Use Pollard's rho method for factorization to find a factor of 473 with iteration function $x_{i+1} = x_i^2 + 7$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 473)$ until a non-trivial gcd is found. Start with $x_0 = 5$.

5 points

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

$$E : x^2 + y^2 = 1 + 3x^2y^2$$

over $\mathbb{F}_{19}$. 9 points

(b) Verify that $P = (5, 8)$ is on the curve. Compute the order of P.
Hint: You may use information learned about the order of points on Edwards curves. 9 points

(c) Translate the curve **and** P to Montgomery form

$$Bv^2 = u^3 + Au^2 + u,$$

i.e. compute A, B and the resulting point P'.
Verify that the resulting point P' is on the Montgomery curve.
5 points

6. Consider the curve $C : y^2 = x^3$ over $\mathbb{F}_p$ with $p = 1009$. On the set of points of $C(\mathbb{F}_p) \setminus \{(0, 0)\}$ one can define the same addition law as on an elliptic curve in short Weierstrass form, i.e. use $(x, y) + (x, -y) = \infty$, and otherwise for $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$

$$P_1 + P_2 = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & P_1 \neq \pm P_2 \\ \frac{3x_1^2}{2y_1} & P_1 = P_2 \neq -P_2 \end{cases}$$

Note that all computations take place in $\mathbb{F}_p$.

(a) Show that C is not an elliptic curve over $\mathbb{F}_p$. 2 points

(b) Let $P = (x_1, y_1) = (9, 982)$. Compute $2P = (x_2, y_2)$ and $3P = (x_3, y_3)$. 6 points

(c) For the results from (b), verify that $2P$ and $3P$ satisfy the curve equation for C and compute x_1/y_1, x_2/y_2, and x_3/y_3. 5 points

(d) Solve the discrete logarithm problem for $Q = (897, 710)$ with base $P = (9, 982)$, i.e., find a natural number k so that $Q = kP$ holds. Verify your answer, i.e., compute kP.
Hint: This needs information from (c). 9 points