TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 21 January 2020

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 statement asks for 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 any material of other students
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 $p = 35533$. The element $g = 2 \in \mathbb{F}_{35533}^*$ has order 35532 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 2101$ 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 $p = 821$ and $q = 701$. Compute Alice's public key (n, e), using $e = 2^{16} + 1$, and the matching private key (n, d). | 3 points |

   (b) Bob uses public key $(n, e) = (374861, 5)$ and secret key $(n, d) = (374861, 149453)$. He receives ciphertext $c = 153497$.
   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 $p = 673$ and $q = 557$. Make sure to document your computation, i.e., state the values for $c_p, d_p, m_p, \ldots$ | 5 points |

3. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 35533$. The element $g = 2$ has order $p - 1 = 35532$. The factorization of $p - 1$ is $p - 1 = 2^2 \cdot 3^3 \cdot 7 \cdot 47$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_B = g^b = 33123$, i.e. perform the following steps.

   (a) Compute b modulo 2^2 by first computing b modulo 2 and then modulo 2^2.
   Verify your answer. | 4 points |

   (b) Compute b modulo 7. Document all steps | 4 points |

   (c) Compute b modulo 3^3 by first computing b modulo 3, then modulo 3^2, and finally modulo 3^3 using the same table of powers of g.
   Verify your answer. | 8 points |

(d) Compute b modulo 47 using the Pollard-rho method in the schoolbook version, on $G = g^{(p-1)/47}$ and $H = h_B^{(p-1)/47}$, starting with $t_0 = G^{17} \cdot H^2, a_0 = 17$, and $b_0 = 2$.

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

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. 12 points

(e) Combine the results above to compute b.
Verify your answer.
If you miss parts of the answers above, solve and verify for the parts you have. 4 points

4. This exercise is about factoring.

(a) Use the $p-1$ method to factor $n = 374861$ with basis $a = 4$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. 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 672 is $672 = 2^5 \cdot 3 \cdot 7$ and that of 556 is $556 = 2^2 \cdot 139$. 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 851 with iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. after each increment in i compute $\gcd(x_{2i} - x_i, 851)$ until a non-trivial gcd is found. Start with $x_0 = 4$. 6 points

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

$$E : x^2 + y^2 = 1 + 11x^2y^2$$

over $\mathbb{F}_{17}$. 9 points

(b) Verify that $P = (3, 7)$ 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. In 2019, the Moscow Internet voting system used triple-ElGamal, a scheme based on ElGamal encryption, for encrypting the votes.
Setup: Randomly select 3 primes p_1, p_2, p_3 of 256 bits each which satisfy $p_1 < p_2 < p_3$ and such that $p_i' = (p_i - 1)/2$ is prime for all $1 \leq i \leq 3$. For each prime p_i,$1 \leq i \leq 3$, pick a generator of the subgroup of $\mathbb{F}_{p_i}^*$ of order p_i'. Publish g_i, g_2, g_3 along with p_1, p_2, p_3.
KeyGen: Randomly select a_1, a_2, a_3, with $a_i \in [0, p_i' - 1]$ for all $1 \leq i \leq 3$, and put $\mathsf{sk} = (a_1, a_2, a_3)$ and $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2, \mathsf{pk}_3) = (g_1^{a_1}, g_2^{a_2}, g_3^{a_3})$.
Enc: To encrypt message m, an integer in $[0, p_1 - 1]$ pick random exponents k_1, k_2, k_3, with $k_i \in [0, p_i' - 1]$ for all $1 \leq i \leq 3$, and compute

- $(r_1, c_1) = (g_1^{k_1}, m \cdot \mathsf{pk}_1^{k_1})$, consider r_1 an integer in $[0, p_1 - 1]$;
- $(r_2, c_2) = (g_2^{k_2}, r_1 \cdot \mathsf{pk}_2^{k_2})$, consider r_2 an integer in $[0, p_2 - 1]$;
- $(r_3, c_3) = (g_3^{k_3}, r_2 \cdot \mathsf{pk}_3^{k_3})$.

Send (c_1, c_2, r_3, c_3) as ciphertext.
Dec: As in regular ElGamal decryption, recover r_2 from (r_3, c_3) using a_3; then recover r_1 from (r_2, c_2) using a_2, and finally recover m from (r_1, c_1) using a_1.

(a) Show that the encryption scheme is sound, i.e. that properly encrypted messages can be decrypted.
Hint: you need to use $p_1 < p_2 < p_3$ in your answer. Without this condition decryption can fail. [8 points]

(b) Show how to break the scheme in time significantly less than an attack on the regular ElGamal scheme for a prime of $3 \cdot 256$ bits. [4 points]

(c) Give an estimate in p_1, p_2, and p_3 (using O notation or L notation) of the complexity of your attack. [4 points]