TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 30 October 2018

Name :

TU/e student number :

Exercise	1	2	3	4	5	total
points						

Notes: Please hand in *all sheets* at the end of the exam. This exam consists of five 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 your steps. In particular for algorithms do include all relevant parts of the internal state of the algorithm (at least the information given in the examples that were done during the lecture); it is not sufficient to state the correct result without the explanation.
If the exercise asks for the 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. Text written with one of the two will be ignored.
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 cell phones or laptops (other than the ones brought be the TAs) is forbidden.

1. **Warm-up: Diffie-Hellman.** This exercise is about the Diffie-Hellman key exchange. The system uses the multiplicative group $\mathbb{F}_p^*$ modulo the prime $p = 22369$. The element $g = 11 \in \mathbb{F}_{22369}^*$ has order 22368 and is thus a generator of the full multiplicative group.

   (a) Alice chooses $a = 258$ as her secret key. Compute Alice's public key.

   1 point

   (b) Alice receives $h_b = g^b = 10877$ 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. **Discrete logarithms.** This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ for $p = 22369$. The element $g = 11$ has order $q = 22368$. The factorization of q is $q = 22368 = 2^5 \cdot 3 \cdot 233$. Use the Pohlig-Hellman attack to compute the discrete logarithm b of Bob's key $h_b = g^b = 10877$. I.e., you should break down the computation into discrete logarithms in subgroups of the smallest order possible. So you will have to eventually compute discrete logarithms in subgroups of order 2, 3 and 233. To solve the discrete logarithm in the subgroup of order 233 use the baby-step, giant-step algorithm. Verify your intermediate and your final solutions!

   27 points

3. **RSA Encryption.** This exercise is about RSA encryption.

(a) Generate an RSA key pair. For this, you are given three digit random numbers $x_1, ..., x_4$ below for which you have to check primality until you found two prime numbers. (Hint: Use the x_i according to the order of the indices.) For primality testing use the Miller-Rabin primality test. As a-values in Miller-Rabin use the $a_1, ..., a_6$ given below (do only use each a_i once, i.e., if you already used a_1 in the primality test for x_1 do not use it in the primality test for x_2 and so on). For this exercise it is sufficient to achieve a probability of 0.75 that a number is prime.

i	1	2	3	4
x_i	731	733	737	739

i	1	2	3	4	5	6
a_i	43	4	57	101	11	13

i. How many iterations of Miller-Rabin are necessary to achieve a probability of 0.75 that a number is prime?

1 point

ii. Output p, q, as well as public key (N, e) and secret key (N, d) using public exponent $e = 2^{16} + 1$.

9 points

(b) Bob uses public key $(N, e) = (151313, 17)$. Encrypt the message 131515 for Bob using schoolbook RSA in combination with 'square & multiply'.

3 points

(c) Bob just received some interesting message but you only saw the ciphertext: $c = 79593$. So, lets break Bob's key. Factor Bob's $N = 151\,313$ using Pollard's roh method with iteration function $x_{i+1} = x_i^2 + 5$ and Floyd's cycle finding algorithm. Start with $x_0 = 333$ Do not do the gcd over 100 pairs, but do it for each pair x_i, x_{2i}.

9 points

(d) Because this was so much fun, factor Bob's N once more, this time using Pollard's $(p - 1)$ method. Use as exponent $s = \text{lcm}\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$ and as basis $a = 13$.

5 points

(e) Now decrypt $c = 79593$ using Bob's secret key. Provide Bob's secret key (N, d), and the decrypted message.

3 points

4. **Hash functions.** One of the first signature schemes was by Lamport. The Lamport signature scheme Π is actually not a full signature scheme but something called a one-time signature scheme. This scheme only requires a hash function $h : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ that is preimage resistant. The most basic version of $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ has a message space $\{0,1\}$, i.e., it signs single bits, and the algorithms are as follows:

   $\mathsf{Gen}(1^n)$:

   (a) Sample hash index $k \leftarrow_R \{0,1\}^n$

   (b) Sample two uniformly random n-bit strings x_0, x_1, i.e., $x_b \leftarrow_R \{0,1\}^n$ for $b \in \{0,1\}$

   (c) Compute $(y_0, y_1) = (h_k(x_0), h_k(x_1))$, i.e., the hashes of the x_b.

   (d) Output public key $\text{pk} = \langle k, (y_0, y_1)\rangle$ and secret key $\text{sk} = (x_0, x_1)$.

   $\mathsf{Sign}_{\text{sk}}(m)$: Given a message $m \in \{0,1\}$, return signature $\sigma := x_m$.

   $\mathsf{Vrfy}_{\text{pk}}(m, \sigma)$: Return 1 if $h_k(\sigma) = y_m$, and 0 otherwise.

   (a) Prove that Π is unforgable under key only attacks if h is preimage resistant.

   Unforgable under key only attacks means that an adversary $\mathcal{A}$ that is given the public key is unable to generate a valid signature on any message. Stated differently, the adversaries task in the unforgability under key only attacks game is given a public key to output a message-signature pair $(m, \sigma) \leftarrow \mathcal{A}(\text{pk})$ such that $\mathsf{Vrfy}_{\text{pk}}(m, \sigma) = 1$.

   Recall, a preimage finder $\mathcal{B}$ takes as input a random function index k and the image y of a random domain element $(x \leftarrow_R \{0,1\}^n, y := h_k(x))$. Its goal is to output a value $x' \leftarrow \mathcal{B}(k, y)$ such that $h_k(x') = y$.

   10 points

   (b) Describe a variant of Π that has a message space $\mathcal{M} = \{0,1\}^\ell$, i.e., it signs ℓ-bit strings.

   5 points

   (c) Extend your security proof to the case of the new scheme.

   5 points

5. **Perfect secrecy.** Let $q \in \mathbb{Z}$, $q > 1$. Consider the following secret key encryption scheme $\mathcal{E}$ over message space $\mathcal{M} = \{0, \ldots, q-1\}$:

   $\mathsf{Gen}()$: Outputs $k \leftarrow_R \{0, \ldots, q-1\}$, a random number mod q, as secret key.

   $\mathsf{Enc}_k(m)$: Returns $c = k + m \mod q$.

   $\mathsf{Dec}_k(c)$: Returns $m = c - k \mod q$.

   Prove that $\mathcal{E}$ is a perfectly secret encryption scheme.

   20 points