TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology, Tuesday 24 January 2017

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 sheet 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 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 laptops and cell phones is forbidden.

1. This problem is about RSA encryption.

   (a) Bob's public key is $(n, e) = (27887, 5)$. Compute the encryption of $m = 1234$ to Bob. **1 point**

   (b) Alice's chooses $p = 1259$ and $q = 2531$. Compute Alice's public key (n, e), using $e = 3$, and the matching private key d. **2 points**

   (c) Alice receives ciphertext $c = 2766602$. Use the secret key d computed in the first part of this exercise and compute the CRT private keys d_p and d_q. Decrypt the ciphertext using the CRT method.
   Verify correctness of your answer by using d from the previous exercise directly. **6 points**

2. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ with $p = 221537$. Note that $p - 1 = 2^5 \cdot 7 \cdot 23 \cdot 43$. A generator of $\mathbb{F}_p^*$ is $g = 5$. Charlie's public key is $h = g^c = 32278$.

   (a) Use the Pohlig-Hellman attack to compute Charlie's secret key c modulo 2^5 and modulo 7.
   Note: This is not the full attack, the computations modulo 23 and modulo 43 and the CRT computation are done in the next parts. Also remember that Pohlig-Hellman computes one prime at a time, not one prime power at a time. **10 points**

   (b) The computation for the group of order 43 starts with the DLP $h^{(p-1)/43} = 9972$ to the base $g^{(p-1)/43} = 127913$. Use the Baby-Step Giant-Step attack in the subgroup of size 43 to compute c modulo 43. **9 points**

   (c) Use the Baby-Step Giant-Step attack in the subgroup of size 23 to compute c modulo 23. Make sure to compute the correct powers of h and g at the start. **8 points**

   (d) Combine the results from the previous two parts to compute c. Verify your answer, i.e., compute g^c. **7 points**

3. This exercise is about factoring $n = 27887$.

(a) Use Pollard's rho method for factorization to find a factor of 27887. Use starting point $x_0 = 17$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 27887)$ until a non-trivial gcd is found. Make sure to document the intermediate steps. **10 points**

(b) Use the $p-1$ method to factor 27887 with basis $a = 2$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 11\}$. **4 points**

4. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 + 8x^2y^2$ over $\mathbb{F}_{11}$. **8 points**

   (b) Verify that $P = (9, 2)$ is on the curve. Compute $3P$. **8 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 P' is on the Montgomery curve. **6 points**

5. The ElGamal signature scheme works as follows. Let $G = \langle g \rangle$ be a group of order ℓ. User A picks a private key a and computes the matching public key $h_A = g^a$. To sign message m, A picks a random nonce k and computes $r = g^k$ and $s \equiv k^{-1}(r + \text{hash}(m)a) \bmod \ell$. The signature is (r, s).

   We have shown that one can compute a from knowing k and stated that repated nonces allow recovery of a as well.

   Bob wants to avoid these issues and deterministically generates k by incrementing k by 1 for each signature.

   (a) This part is a reminder of what we sketched in class. You obtain (r, s_1) on m_1 and (r, s_2) on $m_2 \neq m_1$ and know that these were generated using the same k. Show how to obtain a. **5 points**

   (b) You obtain (r_1, s_1) on m_1 and (r_2, s_2) on m_2 and know that these were generated such that $k_2 = k_1 + 1$.
   Show how to obtain a. **9 points**

   (c) You obtain (r_1, s_1) on m_1 and (r_3, s_3) on m_3 and know that these were generated not too long after one another, such that $k_3 = k_1 + i$ for some small i. Show how to obtain i and a. **7 points**