TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptology/Cryptography I, Tuesday 27 October 2015

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) Alice's chooses $p = 239$ and $q = 457$. Compute Alice's public key (n, e), using $e = 5$, and the matching private key d. **2 points**

   (b) Alice receives ciphertext $c = 70721$. 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. **5 points**

2. This exercise is about computing discrete logarithms in the multiplicative group of $\mathbb{F}_p$ with $p = 232357$. Note that $p - 1 = 2^2 \cdot 3 \cdot 17^2 \cdot 67$.

   A generator of $\mathbb{F}_p^*$ is $g = 2$. Charlie's public key is $h = g^c = 41592$.

   (a) Use the Pohlig-Hellman attack to compute Charlie's secret key c modulo 2^2, modulo 3, and modulo 17^2.
   Note: This is not the full attack, the computation modulo 67 and the CRT computation is done in the next parts. **18 points**

   (b) The computation for the group of order 67 starts with the DLP $h^{(p-1)/67} = 211529$ to the base $g^{(p-1)/67} = 46410$. Use the Baby-Step Giant-Step attack in the subgroup of size 67 to compute c modulo 67. **10 points**

   (c) 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 $n = 679$.

   (a) Use Pollard's rho method for factorization to find a factor of 679. Use starting point $x_0 = 3$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 679)$ until a non-trivial gcd is found. Make sure to document the intermediate steps. **10 points**

   (b) Use the $p-1$ method to factor 679 with basis $a = 2$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5\}$. **4 points**

4. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 + 7x^2y^2$ over $\mathbb{F}_{11}$. 8 points

   (b) Verify that $P = (8, 3)$ is on the curve. Compute the order of P.
   Hint: You may use information learned about the order of points on Edwards curves. 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'. 4 points

   (d) Compute the x-coordinate of $3P'$ on the Montgomery curve using the Montgomery ladder. 10 points

5. This exercise introduces RSA signatures and a way these can leak the secret key if some errors happen in the computation. The key set up for RSA signatures works similar to that in RSA encryption: Let p and q be large primes, let e be an integer coprime to $(p-1)(q-1)$, put $n = pq$, compute $\varphi(n) = (p-1)(q-1)$ and compute $d \equiv e^{-1} \bmod \varphi(n)$. The public key is (n, e), the private key is d.

   To sign message $m \in \mathbb{Z}/n$, compute $s \equiv m^d \bmod n$.

   To verify a signature s under public key (n, e), compute $m' \equiv s^e \bmod n$. The signature is valid if $m' = m$.

   To speed up signature generation, users can use the CRT method the same way that it is used in decryption; i.e. the user computes the values of $d_p \equiv d \bmod (p-1)$ and $d_q \equiv d \bmod (q-1)$, then computes $s_p \equiv m^{d_p} \bmod p$ and $s_q \equiv m^{d_q} \bmod q$, and finally uses the Chinese Remainder Theorem to compute s modulo n from s_p and s_q.

   Note: This is a schoolbook version of the system, in real applications the message m is replaced by its hash $h(m)$ and some padding and randomization. However, the attack you are finding in this exercise will work just the same.

   (a) Set up the public and private keys with $p = 449$, $q = 557$, and $e = 3$. 2 points

   (b) Compute the signature on $m = 56789$ using the secret key from part (a). 1 point

(c) Verify that $s = 139239$ is a valid signature on $m = 144871$ with the key $(n, e) = (290729, 5)$. 1 point

(d) Assume that Dave is using the CRT method to sign. Eve manages to disturb his computer during the computation of s_p or s_q (but not both), so that the computation is incorrect. He then outputs the signature s on m using the faulty s_p and s_q. Show how Eve can use (n, e), s and m to compute the factors of Dave's n. 8 points

(e) Dave's public key is $(n, e) = (290729, 5)$. After Eve's intervention he outputs $s = 242487$ as a signature on $m = 123456$. Factor $n = 290729$. 2 points