TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Tuesday 28 January 2014

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 14:00 – 17:00 to solve them. You can reach 50 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 public key is $(n, e) = (13589, 5)$. Encrypt the message $m = 2801$ to Alice using schoolbook RSA (no padding). **1 point**

   (b) Let $p = 653$ and $q = 701$. Compute the public key using $e = 3$ and the corresponding private key. **2 points**

   (c) Decrypt the message $c = 4839$ which was encrypted to your key under (b). Feel free to use p and q. **3 points**

2. This exercise is about computing discrete logarithms in some groups. The order of 2 in $\mathbb{F}_{211}^*$ is 210. Alice uses the group generated by $g = 2$ for cryptography. Her public key is $g_c = 107$. Your task is to compute $0 \leq k < 210$ with $2^k \equiv 107 \bmod 211$ in the following two steps:

   (a) Compute k modulo 2 and modulo 3. **3 points**

   (b) Use the baby-step-giant-step algorithm to determine k. Note, you can make use of the result obtained under (a). **6 points**

3. This exercise is about factoring $n = 2014$. Obviously, 2 is a factor, so the rest of the exercise is about factoring the remaining factor $m = 2014/2 = 1007$.

   (a) Use Pollard's rho method of factorization to find a factor of 1007. Use starting point $x_0 = 1$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 1007)$ until a non-trivial gcd is found. **5 points**

   (b) Perform one round of the Fermat test with base $a = 2$ to test whether 19 is prime. What is the answer of the Fermat test? **2 points**

   (c) Use Pollard's $p - 1$ factorization method to factor the number $n = 1007$ with base $u = 2$ and exponent $2^3 \cdot 3^2$. **3 points**

4. (a) Find all affine points on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. [4 points]

   (b) Verify that $P = (6, 3)$ is on the curve. Compute the order of P. [4 points]

   (c) Translate the curve and P to Montgomery form

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

[2 points]

5. The curve $y^2 = x^3$ is not an elliptic curve over $\mathbb{F}_{71}$ but the set of points $\{(x, y)|x, y \in \mathbb{F}_{71}^*, y^2 = x^3\} \cup \{P_\infty\}$ forms a group under the addition and doubling laws on (short) Weierstrass curves.

   (a) The point $(1, 1)$ is on the curve. Compute $2P, 3P, 4P$, and $8P$. [6 points]

   (b) Compute the fractions x/y for $2P, 3P, 4P$, and $8P$. [2 points]

   (c) Compute the discrete logarithm of $(6, 43)$ with base $(1, 1)$. Make sure to justify your approach. [7 points]