TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Friday 29 January 2010

Name :

Student number :

Exercise	1	2	3	4	5	total
points						

Notes: 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. One copy of the textbook is available at the examiner's desk, you are not allowed to use the textbooks of your colleagues.
You are allowed to use a simple, non-graphical pocket calculator. Usage of laptops and cell phones is forbidden.

1. This problem is about ElGamal encryption in the subgroup generated by $g = 2$ of $\mathbb{F}_{47}$.

   (a) Your secret key is $s = 9$. Compute your public key. $\boxed{\text{1 point}}$

   (b) Alice's public key is $P_A = 14$. Use the random nonce $r = 3$ to encrypt the message $m = 27$ to Alice. $\boxed{\text{3 points}}$

2. This problem is about the discrete logarithm problem in $\mathbb{F}_{41}$.

   (a) Show that the multiplicative order of 7 is 40. Document how you compute high powers of 7 in $\mathbb{F}_{41}$ efficiently. 3 points

   (b) Show how the Pohlig-Hellman algorithm reduces the problem of computing m with $7^m = c$ to two smaller problems. 3 points

   (c) Set up all preliminary work to solve $7^m = c$ in general. 3 points

   (d) Now solve $7^m = 29$ in this way. 2 points

3. This exercise is about factoring $n = 1001$.

   (a) Use Pollard's rho method of factorization to find a factor of 1001. Use starting point $x_0 = 1$ and iteration function $x_{i+1} = x_i^2 + 1$. 4 points

   (b) Perform one round of the Fermat test with base 2 to test whether 77 is prime. What is the answer of the Fermat test? 2 points

   (c) Use Pollard's $p - 1$ factorization method to factor the number $n = 1001$ with base $u = 2$ and exponent $2^3 \cdot 3^2$. 4 points

4. (a) Find all affine points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. 4 points

   (b) Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve. Compute $[2]P + Q$ in affine coordinates. 4 points

   (c) Translate the curve and P to Weierstrass form. 4 points

5. This problem is about the Fiat-Shamir identification protocol. The public key is $n = 119$.

   (a) You are the trusted party in charge of setting up users for the system. You know that your private key is $p = 7$, $q = 17$. Create a private key s for the user with identity $ID = 93$. 9 points

   (b) Take over the role of the prover. Your secret key is $s = 34$ and your identity is $ID = 85$. Execute *two* rounds of the Fiat-Shamir identification protocol. In the first round, use $r = 12$ to compute the witness. The verifier presents you with challenge $e = 1$. In the second round, use $r = 78$. The verifier presents you with challenge $e = 0$. 4 points