TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Thursday 15 April 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 exercise is about Shamir's secret sharing scheme.

   (a) Set up a Shamir secret sharing scheme over $\mathbb{F}_{11}$ with threshold $(4, 3)$ to share the secret 8. [2 points]

   (b) Show how users $1, 2$ and 3 can reconstruct the secret from their shares. [3 points]

2. Of the "large" integer $n = 299$ it is known that its smallest prime factor p has the additional property that $p - 1$ is $\{2, 3\}$ smooth, i.e. that $p - 1 = 2^a 3^b$ for some integers $a, b > 0$. Demonstrate Pollard's $p - 1$ factorization method by means of the following questions.

   (a) Give an upper bound on a and on b. Call these bounds A and B and state them explicitly. [1 point]

   (b) Let $R = 2^A 3^B$ and let u be randomly selected from $\{1, 2, \ldots, p-1\}$. Prove that $u^R \equiv 1 \bmod p$. [2 points]

   (c) Now select a random u with $1 < u < n$. Prove that almost always $\gcd(u^R - 1, n) = p$. [3 points]

   (d) When does this method fail? [2 points]

   (e) Demonstrate this method with $u = 3$. [2 points]

3. This exercise is about computing discrete logarithms in $\mathbb{F}_{79}^*$. The order of 3 in $\mathbb{F}_{79}^*$ is 78 and 78 factors as $2 \cdot 3 \cdot 13$. The discrete logarithm problem is to find $k \leq 78$ so that $71 = 3^k$ in $\mathbb{F}_{79}^*$.

   (a) Compute k modulo 2 and modulo 3. [4 points]

   (b) Use the baby-step giant-step algorithm with parameter $t = 0.5$ to compute k modulo 13. [4 points]

   (c) Compute k. [2 points]

4. (a) Find all affine points on the twisted Edwards curve $-x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{11}$. | 4 points |

   (b) Verify that $P = (10, 9)$ and $Q = (5, 6)$ are on the curve. Compute $[2]P + Q$ in affine coordinates. | 4 points |

   (c) Translate the curve and P to Weierstrass form

   $$v^2 = u^3 + (A/B)u^2 + (1/B^2)u.$$

   | 4 points |

5. This problem is about RSA encryption.

   (a) Let $p = 11$ and $q = 23$. Compute a public key and the corresponding private key. | 2 points |

   (b) Alice's public key is $(n, e) = (1073, 5)$. Encrypt the message $m = 42$ to Alice using schoolbook RSA (no padding). | 1 point |

   (c) Your private key is $d = 365$ and your public key is $(n, e) = (1739, 245)$. Decrypt the ciphertext $c = 1457$ which is encrypted using schoolbook RSA. | 2 points |

   (d) Show how you can speed up decryption if you know the factors p and q of n and also $d_p \equiv d \bmod p$ and $d_q \equiv d \bmod q$. Demonstrate this in decrypting $c = 1457$ with private key $(p, q, d_p, d_q) = (37, 47, 5, 43)$ and modulus $n = pq = 1739$. | 8 points |