TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Practice Exam Cryptology I, Friday 14 January 2011

Name :

Student number :

Exercise	1	2	3	4	5	total
points						

Notes: This exam consists of 5 exercises. You have 3 hours 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 the clock group.
   Let k be a field. An operation $\circ$ is defined on the set

$$S = \{(x, y) \in k^2 | x^2 + y^2 = 1\}$$

   as

$$(x_1, y_1) \circ (x_2, y_2) = (x_1y_2 + x_2y_1, y_1y_2 - x_1x_2).$$

   (a) Show that $(S, \circ)$ forms a group. | 7 points |

   (b) Is this group abelian? | 1 point |

2. This exercise is about polynomials.

   (a) Let $f(x) = x^4 + x^3 + x^2 + 2 * x + 1, g(x) = x^2 + 2 * x + 1$ be polynomials in $\mathbb{F}_3[x]$. Use the extended Euclidean algorithm to compute $\gcd(f, g)$ and a linear combination $\gcd(f, g) = a(x)f(x) + b(x)g(x)$ for some polynomials $a(x)$ and $b(x)$. | 5 points |

   (b) Count the number $N_5(14)$ of irreducible polynomials of degree 14 over $\mathbb{F}_5$. | 4 points |

3. 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 $d_p \equiv d \bmod (p - 1)$ and $d_q \equiv d \bmod (q - 1)$. Demonstrate this in decrypting $c = 1457$ with private key $(p, q, d_p, d_q) = (37, 47, 5, 43)$ and modulus $n = pq = 1739$. | 6 points |

4. This problem is about the discrete logarithm problem in $\mathbb{F}_{37}^*$.

   (a) Show that the multiplicative order of 2 is 36. [2 points]

   (b) Show how the Pohlig-Hellman algorithm reduces the problem of computing m with $2^m = c$ to two smaller problems. [3 points]

   (c) Set up all preliminary work to solve $2^m = c$ in general. [3 points]

   (d) Now solve $2^m = 27$ in this way. [2 points]

5. (a) Find all points on the Edwards curve $x^2 + y^2 = 1 - 4x^2y^2$ over $\mathbb{F}_{11}$. [3 points]

   (b) Verify that $P = (2, 7)$ and $Q = (3, 8)$ are on the curve. Compute $[2]P + Q$ in affine coordinates. [4 points]

   (c) Translate the curve and P to Montgomery form

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

   state the curve coefficients A, B and the coordinates of the translated point $\phi(P)$. [3 points]

   (d) Compute $[2](\phi(P))$. [2 points]