TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Monday 11 April 2011

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. 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 groups. Let M be the set of rotation matrices:

$$M = \left\{ \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \middle| \, \alpha \in \mathbb{R} \right\}.$$

We define an operation $\circ$ on M as matrix multiplication

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \circ \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

(a) Check whether $(M, \circ)$ is a group. | 4 points

(b) Is $(M, \circ)$ an abelian group? Justify your statement. | 1 point

Hint: You can use the trigonometric addition formulas

$$\begin{aligned} \sin(a+b) &= \sin(a)\cos(b) + \cos(a)\sin(b), \\ \cos(a+b) &= \cos(a)\cos(b) - \sin(a)\sin(b). \end{aligned}$$

2. This exercise is about polynomials.

(a) Compute the number $N_{11}(6)$ of irreducible polynomials of degree 6 over $\mathbb{F}_{11}$. | 2 points

(b) Factor $f(x) = x^5 - 1$ over $\mathbb{F}_{11}$. | 3 points

(c) Let p be prime. State all subfields of $\mathbb{F}_{p^{12}}$. | 2 points

3. This exercise is about discrete logarithms in $\mathbb{F}_{61}$. The integer $p = 61$ is prime. Make sure to document all steps of the computations.

(a) Show that $\mathbb{F}_{61}^* = \langle 2 \rangle$, i.e. show that the order of 2 in $\mathbb{F}_{61}$ is 60. | 2 points

(b) Use the baby-step giant-step algorithm to break the discrete logarithm problem given by $g = 2$, $h = g^a = 26$, i.e., find a. | 5 points

(c) Use the Pohlig-Hellman algorithm to break the discrete logarithm problem given by $g = 2$, $h = g^a = 26$, i.e., find a. | 5 points

4. (a) Find all affine points on the twisted Edwards curve $-x^2 + y^2 = 1 - 7x^2y^2$ over $\mathbb{F}_{13}$. | 4 points |

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

   (c) Translate the curve and P to Montgomery form

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

   | 3 points |

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

5. In this exercise you can use Rabin's irreducibility test and the theory behind it, but it might not be the fastest way.
   Hint: The polynomials g and h divide $x^5 - 1$; this gives you information about the order (in $\mathbb{F}_p^*$) of potential roots over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

   (a) Let $g(x) = x^5 - 1$ over $\mathbb{F}_{19}$. What is the factorization pattern of g, i.e., what are the degrees of the irreducible factors of g over $\mathbb{F}_{19}$. Which is the smallest extension of $\mathbb{F}_{19}$ over which g factors into linear factors? | 5 points |

   (b) Let $h(x) = x^4 + x^3 + x^2 + x + 1$ be a polynomial over $\mathbb{F}_p$ where $p \equiv 2 \bmod 5$ or $p \equiv 3 \bmod 5$. Show that h is irreducible. Which is the smallest extension of $\mathbb{F}_p$ over which g factors into linear factors? | 4 points |

   (c) Let p be prime with $p \equiv 2 \bmod 7$. Show that there is no irreducible binomial of degree 7 over $\mathbb{F}_p$. In other words: Show that all polynomials of the form $x^7 - b$ over $\mathbb{F}_p$ are reducible if $p \equiv 2 \bmod 7$. | 4 points |