Tanja Lange Fall 2009

TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Practice Exam Cryptology I, Friday 15 January 2009

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 exercise require 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. (a) Use the Euclidean algorithm to compute integers n and m, so that

$$11n + 91m = 1$$

holds. | 4 points |

(b) Find the smallest positive integer solution x of the system of congruences:

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 4 \\ x &\equiv 4 \bmod 7 \end{aligned}$$

| 4 points |

2. 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 |

3. Of the "large" integer $n = 119$ 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. | 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 $u = 5$. | 2 points |

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

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

   Note: the correct transformation formulas are on the webpage. [4 points]

5. Protocols

   (a) Let the public key of user U be (G_U, t_U) with

   $$G_U = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

   and $t_U = 1$. Demonstrate the usage of the McEliece cryptosystem by encrypting $m = (1\,0\,0)$. [5 points]

   (b) Let $G = \langle 64 \rangle \subset \mathbb{F}_{67}$ be the subgroup of order 11 of $\mathbb{F}_{67}^*$. Make a public key in G and execute one Schnoor's identification protocol to prove knowledge of your secret key. [5 points]