TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Friday 21 January 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. The set $\mathbb{Z}/26$ forms a commutative group with respect to addition of residue classes. The set $(\mathbb{Z}/26)^*$ is the set of elements having a multiplicative inverse modulo 26. Use $\cdot$ to denote multiplication of residue classes.

   (a) State the order of $(\mathbb{Z}/26, +)$. | 1 point |

   (b) Investigate whether $(\mathbb{Z}/26, +, \cdot)$ is a ring with unity. You may assume that $(\mathbb{Z}/26, +)$ is a commutative group and that $(\mathbb{Z}, +, \cdot)$ is a ring. | 3 points |

   (c) State all elements of $((\mathbb{Z}/26)^*, \cdot)$. Which orders can appear for elements in $((\mathbb{Z}/26)^*, \cdot)$? For every element in $((\mathbb{Z}/26)^*, \cdot)$ state its order. | 4 points |

2. This exercise is about polynomials and finite fields.

   (a) Let $f(x) = x^4+x^3+2x^2+x+1$ be a polynomial in $\mathbb{F}_5[x]$. Compute

   $$\gcd(x^5 - x, f(x)).$$

   | 4 points |

   (b) Use the result of the previous part to give the factorization of f over $\mathbb{F}_5$. | 3 points |

   (c) Which is the smallest extension field of $\mathbb{F}_5$ over which f factors completely into linear factors? | 2 points |

3. This exercise is about computing discrete logarithms in some groups.

   (a) The integer $p = 10007$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 1234$. You observe $h_a = 2345$ and $h_b = 4567$. What is the shared key of Alice and Bob? | 4 points |

   (b) The order of 2 in $\mathbb{F}_{71}^*$ is 35. Charlie uses the subgroup generated by $g = 2$ for cryptography. His public key is $g_c = 29$. Use the baby-step giant-step algorithm to compute an integer c so that $g_c \equiv g^c \bmod 71$. | 5 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 $P = (3, 7)$ and $Q = (1, 2)$ 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 |

5. Batch RSA was invented by Amos Fiat. It is a method by which multiple messages can be signed or decrypted using only one full modular exponentiation. This method is applicable if public exponents are small (which means that encryption and signature verification are fast) and a user uses two different small e's with the same n.

   In an abstract setting a user wants to compute c_1^{1/e_1} and c_2^{1/e_2} for some small values e_1 and e_2 in some group. E.g., he wants to compute $c_1^{1/3}$ and $c_2^{1/5}$. He first computes $c_{12} = c_1^5 \cdot c_2^3$ and $m_{12} = c_{12}^{-1/15}$. Thus $m_{12} = c_1^{-1/3} \cdot c_2^{-1/5}$.

   Note that $m_{12}^5 = c_1^{-5/3} \cdot c_2^{-1}$ and so $c_1^{1/3} = m_{12}^5 \cdot c_1^2 \cdot c_2$, and that $m_{12}^9 = c_1^{-3} \cdot c_2^{-9/5}$ and so $c_2^{1/5} = m_{12}^9 \cdot c_1^3 \cdot c_2^2$.

   (a) Show how to compute $c_1^{1/3}$ and $c_2^{1/7}$ by computing $c_{12}^{-1/21}$ for some definition of c_{12} and a few small exponentiations. | 5 points |

   (b) Show how to compute c_1^{1/e_1} and c_2^{1/e_2} by computing $c_{12}^{-1/(e_1e_2)}$ for some definition of c_{12} and a few small exponentiations. | 8 points |