TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Exam Cryptography 1, Friday 13 April 2012

Name :

Student number :

Exercise	1	2	3	4	5	total
points						

Notes: Please hand in this sheet at the end of the exam. You may keep the sheet with the exercises.
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. Let $(\mathbb{C}, +, \cdot)$ denote the field of complex numbers with regular addition and multiplication. Let the sets M_1 and M_2 be defined as follows:

$$M_1 = \{a + b\sqrt[3]{6} + c\sqrt[3]{6}^2 | a, b, c \in \mathbb{Z}\} \subseteq \mathbb{C},$$
$$M_2 = \{a + b\sqrt{2} + c\sqrt{3} | a, b, c \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

   (a) Study whether $(M_1, \cdot)$ is a semigroup. **2 points**

   (b) Study whether $(M_2, \cdot)$ is a semigroup. **2 points**

   (c) Is $(M_1, +, \cdot)$ a subring of $(\mathbb{C}, +, \cdot)$? Why?
   Hint: You do not need to show associativity, commutativity, or the distributive laws because $\mathbb{C}$ is known to be a field. **4 points**

2. This exercise is about polynomials and finite fields.

   (a) Compute the number $N_9(4)$ of irreducible polynomials of degree 4 over $\mathbb{F}_9$. **2 points**

   (b) Factor $f(x) = x^3 - 2$ over $\mathbb{F}_7$. **2 points**

   (c) Let p be prime. State all subfields of $\mathbb{F}_{p^{60}}$. **2 points**

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

   (a) The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. You observe $h_a = 12$ and $h_b = 14$. What is the shared key of Alice and Bob? **5 points**

   (b) The order of 5 in $\mathbb{F}_{73}^*$ is 72. Charlie uses the subgroup generated by $g = 5$ for cryptography. His public key is $g_c = 2$. Use the Baby-Step Giant-Step method to compute an integer c so that $g_c \equiv g^c \bmod 73$.
   10 points

4. (a) Find all affine points on the twisted Edwards curve $-x^2 + y^2 = 1 - 3x^2y^2$ over $\mathbb{F}_{17}$. 5 points

   (b) Verify that $P = (6, 10)$ is on the curve. Compute $4P$. 4 points

   (c) Translate the curve and P to Montgomery form

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

2 points

5. In 1995 Shamir suggested an improvement to RSA called "RSA for paranoids". In this system encryption and decryption work the usual way with $c \equiv m^e \bmod n$ and $m \equiv c^d \bmod n$ but the primes p and q have significantly different sizes – for an 80-bit security level p has the usual 500 bits while q has 4500 bits. This means that the attacker is faced with the problem of factoring a huge number. There is also some performance hit for the sender of a message since he has to work modulo a larger number $n = pq$, but Shamir is nice enough to limit the size of the messages m to be smaller than p and to suggest a small-ish encryption exponent such as $e = 23$.

   (a) Explain why in the above scenario $e = 3$ would lead to an insecure system.

   2 points

   (b) Explain how the use of these parameters $m < p \ll q$ speeds up decryption.

   Hint: You do not need to determine q. 4.5 points

   (c) Decipher the ciphertext $c = 187008753$ knowing that $e = 17, p = 11, n = 214359541$.
   Hint: You are likely to do some modular reduction by hand for this one, I do not expect your pocket calculator to handle computations modulo n. 3.5 points