TEN 1

MAA063 Cryptography
Mälardarlens University

Course Responsible: Tianqi Liu
Examiner: Olof Bergvall

27.3.2025
14:30-18:30

There are five questions in total in this exam, each is of 20 points but you only need to answer four of them, so the full mark will be 80 points. You can freely choose the four questions you wish to answer or you can submit answers to all five questions and we will count the highest scoring four questions (and only the highest four questions will be counted into your score). You are allowed to use basic calculators but no mobile phone usage is allowed. The PASS-marks 3,4, and 5 requires at least 40, 54, and 64 points out of the 80 possible. **All solutions must include rigorous justification and clear presentation of the answers.** Good luck!

Question 1

In the following question, you need to decide whether each of the following statements is true or false. A correct answer will be awarded 2 points, while a false answer will be deducted 2 points. The minimum of points that can be awarded for this question is 0. (20 pts)

1. Translating a given number between arbitrary bases (e.g. from base 2 to base 237) can be done in polynomial time.
2. There is a unique solution to the following system of congruence equations:
$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}. \end{cases}$$
3. All finite groups admit a single generator.
4. The field $\mathbb{F}_9$ is the same as the ring $\mathbb{Z}/9\mathbb{Z}$.
5. For p a prime number, $\left(\frac{a}{p}\right) = 1$ means that there exists $b \in \mathbb{Z}$ such that $b^2 \equiv a \pmod{p}$
6. In classical crypto-systems, (e.g. Caesar Cipher), the knowledge of how to encrypt a message is the same as the knowledge of how to decrypt a message.
7. In a public-key system, two users require the knowledge of both of their private keys together for safe communication: i.e., both A and B need both private keys to encrypt and decrypt messages.
8. In the RSA system, an attacker who knows the information $\varphi(n)$ can deduce the information of the primes p and q, where $n = pq$ and φ is the Euler-phi function.
9. The Fermat primality test is a deterministic primality test.
10. Every elliptic curve over a finite field is a cyclic group.

Question 2

1. Show that for the class of 3×3 matrices over a ring $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

is invertible if and only if the 2×2 minor,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

is invertible. (5 pts)

2. Show that the matrix

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

is invertible over $\mathbb{Z}/29\mathbb{Z}$, and find its inverse. (5 pts)

3. Consider the English alphabet with the following extension: $',' = 26$, $'\_' = 27$,$'!' = 28$. Use the above matrix A as the enciphering matrix to encrypt the following message: '$HONG\_KONG$'. (5 pts)

4. The cipher-text: $'TIO, GL, !K'$ with 9 letters is encrypted using A, find the original plain-text. (5 pts)

Letter	Number	Letter	Number	Letter	Number
A	0	J	9	S	18
B	1	K	10	T	19
C	2	L	11	U	20
D	3	M	12	V	21
E	4	N	13	W	22
F	5	O	14	X	23
G	6	P	15	Y	24
H	7	Q	16	Z	25
I	8	R	17		

Table 1: English Alphabet Corresponding to Numbers Starting from 0

Question 3

One of the key ideas of modern day cryptographic systems is that of public key encryption. These are based on trapdoor functions. Suppose you have two users A and B with their respective trapdoor functions: f_A using key e_A and f_B using key e_B together with their respective decryption function and keys f_A^{-1}, d_A, f_B^{-1}, d_B.

1. Describe, what a trapdoor function is and how it differs from a one-way function. (4 pts)

2. What are the public and private information (with respect to each user) for a public key cryptographic system using the above trapdoor functions and keys. (6 pts)

3. For A and B users of the above public-key system, how can A send a signature through the system, together with some plain-text P, in order for B to make sure that the message P is indeed from A, not some third-party. (10 pts)

Question 4

The safety of key exchange protocols like Diffie-Hellman is guaranteed by the mathematical difficulty of computing discrete logarithms. Its converse, the computation of discrete power, is not that hard. The finite field we will work in is $\mathbb{F}_{37}$.

1. Write 34 in terms of base 2. (3 pts)
2. Denote the binary digits of 34 by $n_0, ..., n_k$, i.e.: $(34)_2 = n_k n_{k-1} ... n_0$. Calculate, for each number $n_i \neq 0$, $2^{2^i} \equiv b_i \mod 37$. (Hint: this can be simplified by computing squares and then modulo 37 a couple of times). (6 pts)
3. Set $a = 1$. For each $n_i \neq 1$, update a by calculating $a \equiv ab_i \mod 37$, show your list of a's following this calculation. Explain why the last a gives the congruence class of $2^{34} \mod 37$. (8 pts)
4. Use the information to calculate the discrete logarithm of 56 over the base 2. (3 pts)

Question 5

Consider the elliptic curve $E : y^2 = x^3 - x$ over the finite field $\mathbb{F}_{71}$. Recall $\chi(x)$ is a function in a finite field $\mathbb{F}_q$ determining whether the element x is a quadratic residue. In particular, for $q = p$ a prime number, $\chi(x) = \left(\frac{x}{p}\right)$.

1. Show that for $x \in \mathbb{F}_{71}^*$, we have that $\chi(x) = \left(\frac{x}{71}\right)$. (2 pts)
2. Show that for $u \in \mathbb{F}_{71}$, $\chi(u) = -\chi(-u)$. Use this to show that the number of points of E over $\mathbb{F}_{71}$ is $N_{71} = 71 + 1 = 72$. (Hint: recall $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, and that $N_q = q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + ax + b)$, for a general elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$.) (6 pts)

We now aim to determine the complete group structure of E over $\mathbb{F}_{71}$.

3. Recall an element is of order two, if and only if it is on the $x-$axis. Count the number of elements of order at most 2 in E (including O). (4 pts)
4. Show that the point $(2, 19)$ is of order greater than 3. (Recall addition formulae for points on a general elliptic curve:

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2,\ y_3 = -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3),$$

$$x_4 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1,\ y_4 = -y_1 + (\frac{3x_1^2 + a}{2y_1})(x_1 - x_4).$$

   for $P = (x_1, y_1),\ Q = (x_2, y_2),\ P + Q = (x_3, y_3),\ 2P = (x_4, y_4).$) (6 pts)
5. Knowing the point $(70, 0)$ is the 9-th power of $(14, 48)$, what can you say about the order of $(14, 48)$. (2 pts)

The above is sufficient to show that $E(\mathbb{F}_{71}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ (This is simply a statement, not part of the question).

Solutions

1

T F F F T T F T F F

2

1: omitted; 2: $\begin{pmatrix} 19 & 10 & 0 \\ 23 & 16 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ 3: $\begin{pmatrix} 1 & 3 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & 6 & 14 \\ 14 & 27 & 13 \\ 13 & 10 & 6 \end{pmatrix} = \begin{pmatrix} 49 & 87 & 53 \\ 70 & 105 & 95 \\ 13 & 10 & 6 \end{pmatrix} \equiv \begin{pmatrix} 20 & 0 & 24 \\ 12 & 18 & 8 \\ 13 & 10 & 6 \end{pmatrix} \mod 29$ which correspond to 'UMNASKYIG' 4: GOOD_LUCK

3

omitted

4

1: 100010 2: easy to calculate to be 7 and 4. 3: 28 4: 56 is 35th power of 2.

5

1: definition; 2: omitted 3: 4; 4: just calculate that this point: (2,19) - (4,29) - (19,38) = 3(2,19) not O. 5: Easy.