Indian Institute of Technology
Major Test
MTL-730 (Cryptography)

Time: 1 Hour 30 minutes Max. Marks: 25

Attempt all questions. All notations are standard. All parts of a question must be answered at one place. Exhibit clearly all the steps. No marks will be awarded for direct answers. No query will be entertained. Upload your solutions on Moodle . Extra time of 30 minutes is given for uploading.

Questions 1 - 5 (two marks each). Questions 6 - 10 (three marks each).

1. Solve the following system of congruences: [2]

$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv 3 \ (mod\ 17)$$

$$x \equiv 6 \ (mod\ 18)$$

2. Consider the elliptic curve of char 2: [2]

$$E = \ \{(x, y) \in \ \mathbb{F}_4 \times \mathbb{F}_4 \,|\, y^2 + xy = x^3 + x^2 + 1\} \cup \{\infty\}.$$

Find the order of E and all points of E.

3. If p is a prime, prove that $x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1$ is irreducible over $\mathbb{Q}$. [2]

4. Using Pollard's ρ algorithm, determine if exists, $dlog_7 15$ in $\mathbb{Z}^*_{131}$. [2]

5. Consider the elliptic curve over $\mathbb{F} = \mathbb{F}_{23}$ [2]

$$E_{\mathbb{F}} = \ \{(x, y) \in \ \mathbb{F} \times \mathbb{F} \,|\, y^2 = x^3 + x + 1\} \cup \{\infty\}.$$

   (a) Find the bound for order of $E_{\mathbb{F}}$.

   (b) Is the curve $E_{\mathbb{F}}$ a singular curve? If yes, find all the singular points.

6. Consider the elliptic curve over $\mathbb{F} = \mathbb{F}_{23}$ [3]

$$E_{\mathbb{F}} = \ \{(x, y) \in \ \mathbb{F} \times \mathbb{F} \,|\, y^2 = x^3 + x + 1\} \cup \{\infty\}.$$

   (a) Find all the points of $E_{\mathbb{F}}$.

   (b) Write the structure of group $E_{\mathbb{F}}$.

7. Find all solutions of the congruence [3]

$$3x^2 + 5x + 2 \equiv 0 \ (mod\ 2537).$$

8. Determine $dlog_x(x^2 + 1)$ in $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$. [3]

9. Let $E := \{(x, y) \in \mathbb{Z}_{23} \times \mathbb{Z}_{23} |\ y^2 = x^3 + 9x + 17\} \bigcup \{\infty\}$ be an Elliptic curve. Under the El-Gamel cryptosystem Alice received a message $((16, 5)\ ,\ (10, 7))$. If Alice's private key is $a = 5$, then what is the decryption of the message for Alice? [3]

10. Somebody sent you the following message:

!IWGVIEX!ZRADRYD

If the message was encrypted on digraphs from the English language alphabet consisting of A, B, C, ..., X, Y, Z, Blankspace, ?, ! (numbered as 0, 1, ... ,25, 26, 27, 28 respectively) using matrix Hill cipher and you know that the last five letters of the plain text are the sender's signature "MARIA", then decrypt the message. [3]