M E T U
Department of Mathematics

Group	**Elliptic Curves in Cryptography** **Midterm II**	List No.

Code : *IAM 505* Acad. Year : *2013* Semester : *Fall* Instructor : *Küçüksakallı* Date : *19/12/2013* Time : *10:40* Duration : *110 minutes*	Name : Last Name : Signature : 6 QUESTIONS ON 6 PAGES 30 TOTAL POINTS

1	2	3	4	5	6		

1. (5pts) Consider the elliptic curve $y^2 = x^3 + x + 3$ defined over $\mathbb{F}_{101}$. This question is an application of the baby step, giant step algorithm. We choose

$$P = (60, 78), \quad Q = (101 + 1)P = (33, 57), \quad m = 4$$

and obtain the following tables. Explain how we guarentee a match by using $m = 4$. Find the order of the point P. Using the fact that $x^3 + x + 3$ is irreducible over $\mathbb{F}_{101}$, find the order of $E(\mathbb{F}_{101})$.

j	0	1	2	3	4
jP	∞	$(60, 78)$	$(95, 36)$	$(4, 77)$	$(71, 101)$

k	-4	-3	-2	$\ldots$	2	3	4
$Q + k(2mP)$	$(97, 6)$	$(24, 69)$	$(60, 23)$	$\ldots$	$(95, 36)$	$(47, 34)$	$(70, 73)$

2. (5pts) Let E be an elliptic curve over $\mathbb{F}_p$ and suppose that E is supersingular with $a = p + 1 - \#E(\mathbb{F}_p) = 0$. Let N be a positive integer.

- Explain how NP can be computed quickly

- If there exists a point in $E(\mathbb{F}_p)$ of order N, then show that $E[n] \subseteq E(\mathbb{F}_{p^2})$.

3. (5pts) Let E be the curve given by the Weierstrass equation $y^2 = x^3 + x + 3$ defined over $\mathbb{F}_7$. Is E an elliptic curve? Find the number of elements in $E(\mathbb{F}_7)$. Let $\phi : (x, y) \mapsto (x^7, y^7)$ be the Frobenius automorphism. Show that $\phi^2 - 2\phi + 7 = 0$. Find the number of elements in $E(\mathbb{F}_{7^2})$ and $E(\mathbb{F}_{7^3})$.

4. (5pts) Let E be the elliptic curve $y^2 = x^3 + x + 6$ defined over $\mathbb{F}_{307}$. The point $P = (2, 4)$ is of order 331 and therefore generates $E(\mathbb{F}_{307})$. Let $Q = (3, 301)$ which is a point on the elliptic curve. There exists k such that $Q = kP$. This question illustrates the use of Pollard ρ-method to solve a discrete logarithm problem. We choose

$$M_0 = 2P + 3Q, \quad M_1 = 5P + 7Q, \quad M_2 = 11P + 23Q$$

Let $f : E(\mathbb{F}_{307}) \to E(\mathbb{F}_{307})$ be defined by $f(x, y) = (x, y) + M_i$ if $x \equiv i \pmod 3$ where x is regarded as an integer $0 \leq x < 307$. Starting with $P_0 = P + 2Q$ we obtain the following points iteratively. More precisely $P_{i+1} = f(P_i)$ for all $i \geq 0$. Determine k modulo 331.

i	0	1	2	3	4	5	6	7	8	9
$x(P_i)$	29	122	129	23	133	218	99	219	127	122
$y(P_i)$	103	104	105	60	34	110	99	39	186	104

5. (5pts) Alice wants to send a message to Bob using ElGamal public key encryption. Bob's public key consists of $E(\mathbb{F}_q), P, B$.

- How can Alice represent her message as a point on $E(\mathbb{F}_q)$?

- Explain how Alice sends a message to Bob using this scheme.

6. (5pts) Let $n = 16259$. One can easily check that $2^{n-1} \not\equiv 1 \pmod{n}$. Thus n is not a prime. Let E be the curve given by $y^2 = x^3 - 18x + 18$ considered modulo n. Note that $P = (1, 1)$ satisfies this equation. One can find that $2P = (4119, 14625)$. However $3P$ cannot be expressed as an affine point.

- Find a factor of n.

- Explain the elliptic curve factorization method briefly and compare it with the $p - 1$ factorization method.