Chapter 3

ELLIPTIC CURVE CRYPTOGRAPHY (ECC):

3.1 Introduction

The use of elliptic curves in cryptography was first proposed by Neil Koblitz [16]and Victor Miller [20] in 1985. Koblitz and Miller did not invent a new cryptographic algorithm but they implemented certain existing algorithms using elliptic curve arithmetic. Since its founding elliptic curve cryptography has been studied a lot in the academic world. The use of elliptic curves in cryptography is very inviting because shorter key lengths can be used than in the case of conventional cryptography e.g. RSA.

As points on an elliptic curve over $GF(2^n)$form a finite group of order $n = E(GF(2^n))$, with the point addition as a group operation. Multiplication over an elliptic curve is defined as in Section 2.1, i.e. it is performed by sequentially adding a point to itself. Multiplication is the basic operation of any elliptic curve cryptosystem and many efficient algorithms to compute it have been developed. All elliptic curve cryptography (ECC) algorithms rely on the fact that calculating the point multiplication kP, where k is an integer and P is a point on an elliptic curve, is relatively easy and fast, but it is a very hard task to calculate k, if P and kP are given. The problem that must be solved, to calculate k, is called elliptic curve discrete logarithm problem and it requires an exponential time to solve.

Elliptic curve cryptography has better security with a shorter key length than any other published public-key cryptography method. Elliptic curve cryptosystem with a 173-bit key is considered as secure as RSA using a 1024-bit key and ECC with a 313-bit key is considered as secure as 4096-bit RSA . Elliptic curve cryptography is thus a very attractive alternative, especially in communication systems with limited bandwidth.

Elliptic curves have been studied by mathematicians for more than a century. An extremely rich theory has been developed around them, and in turn they have been the basis of numerous new developments in mathematics. As far as cryptography is concerned, elliptic curves have been used for factoring and primality proving. The idea of using elliptic curves for public-key cryptosystems is due to Victor Miller

[Miller85] and Neal Koblitz [Koblitz87] in the mid-eighties. As with all cryptosystems, and especially with public-key cryptosystems, it takes years of public evaluation before a reasonable level of confidence in a new system is established. The elliptic curve public-key cryptosystems (ECPKCs) seem to have reached that level now. In the last couple of years, the first commercial applications have appeared(email security, web security, smart cards, etc.). Before we look at how the ECPKC s work, we will give a short introduction to elliptic curves

3.2 Mathematical of Elliptic Curve Cryptography:

Definition of elliptic curves: Elliptic curves are not ellipses. They are called this because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, an elliptic curve is the set of solutions of an equation of the form

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$ .....(1)

Where the coefficients ai are elements of some field (R, Z or Zp) which satisfy some Simple conditions in order to avoid singularities. Such an equation is said to be Cubic, or of degree 3, because the highest exponent it contains is 3. The Eq.1 is Called Weierstrass *equation*. Also included in the definition of any elliptic curve is a single element denoted O and called *point of infinity* or the *zero point*

An elliptic curve over real numbers may be defined as the set of points (x,y) which satisfy an elliptic curve equation of the form:

$y^2 = x^3 + ax + b$, where x, y, a and b are real numbers.

Each choice of the numbers a and b yields a different elliptic curve. For example, a =1 and b =1 gives the elliptic curve with equation $y^2 = x^3 + x + 1$; the graph of this curve is shown below:

If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2$ is not 0, then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

Figure:

Elliptic Curve (y2 = x3+x +1)

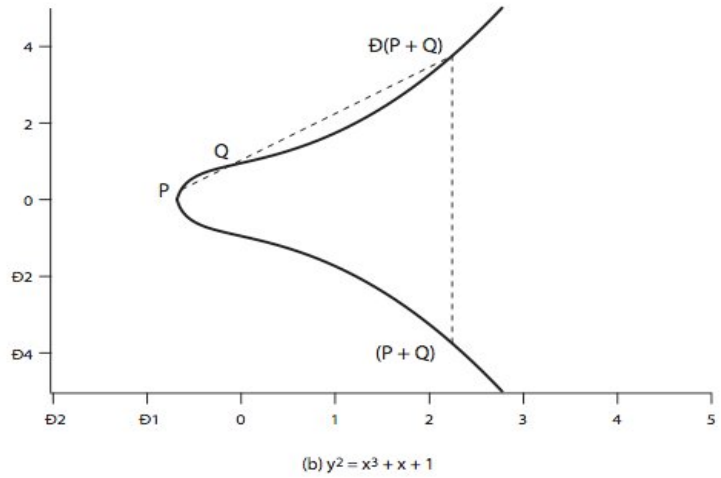


Figure 3.1

3.2.1 **Point addition**: **Elliptic Curve Addition**: A Geometric Approach:

P + Q = R is the additive property defined geometrically.

Elliptic curve groups are additive groups; that is, their basic function is addition. The addition of two points in an elliptic curve is defined geometrically.

The negative of a point P = (X_1,Y_1) is its reflection in the x-axis: the point -P is $(X_1,-Y_1)$. Notice that for each point P on an elliptic curve, the point -P is also on the curve.

Adding distinct points P and Q : The resulted point of adding two different points on the elliptic curve is computed as shown below in figure 2

When P = (X_1,Y_1) and Q = (X_2,Y_2) are not negative of each other,

$(X_1,Y_1)+ (X_2,Y_2)= (X_3,Y_3)$; where $X_1 \neq X_2$

P + Q = R where

$\lambda = (Y_2 - Y_1) / (X_2 - X_1)$

$X_3 = \lambda^2 - X_1 - X_2$ and

$Y_3 = -Y_1 + \lambda (X_1 - X_3)$

Note that λ is the slope of the line through P and Q.

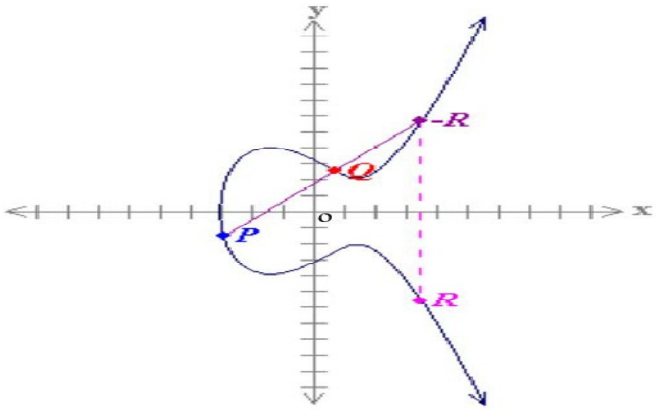


Figure 3.2

Point Addition:

Suppose that P and Q are two distinct points on an elliptic curve, and the P is not -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R..

3.2.2 Point doubling :

$(X_1, Y_1) + (X_2, Y_2) = (X_3, Y_3)$;

where $Y_1 \neq 0$

2P = R where

$\lambda = (3X_1^2 + a) / (2Y_1)$

$X_3 = \lambda^2 - 2X_1$ and

$Y_3 = \lambda (X_1 - X_3) - Y_1$

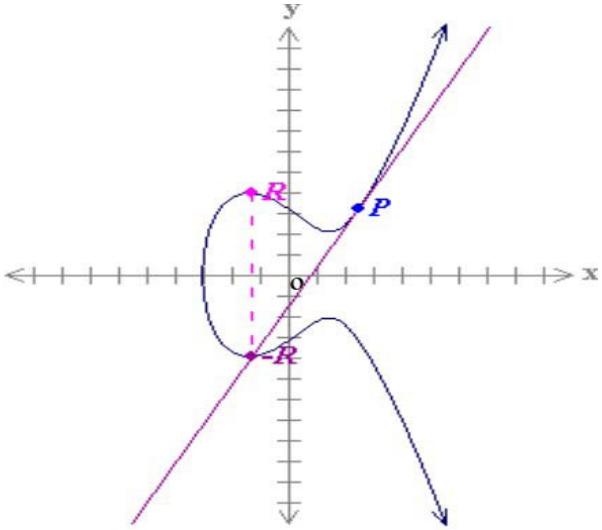


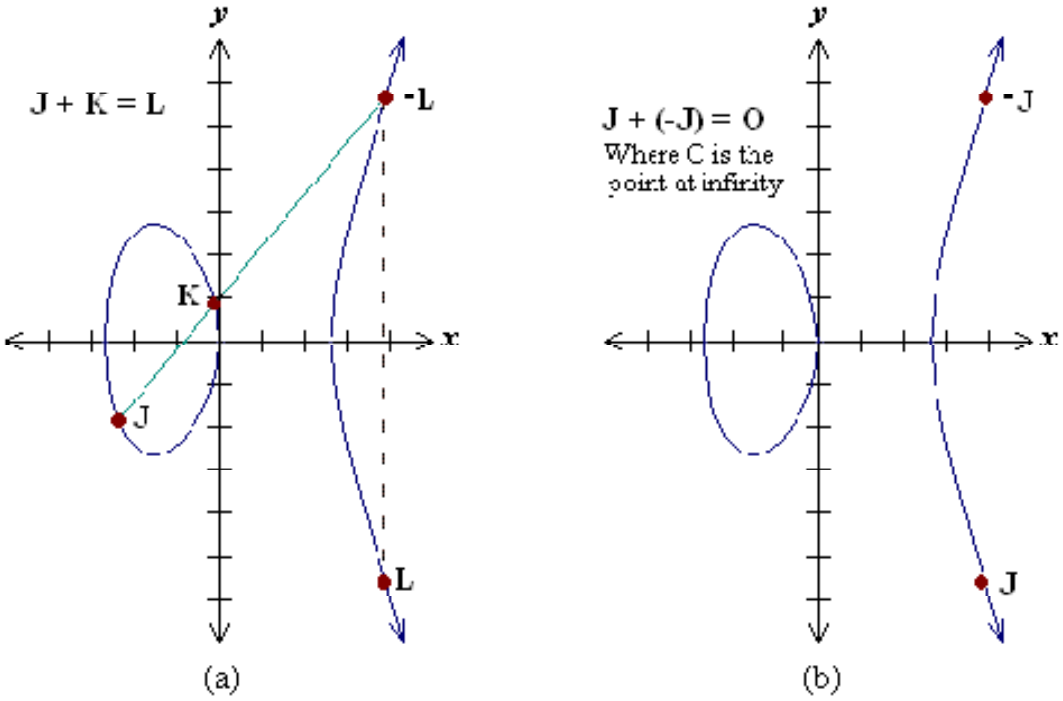
Figure 3.3

Shows how a point can be doubled graphically on the elliptic curve. Suppose we want to double a point P on the elliptic curve. A tangent line to the curve and passing by P is taken to double the point. The line must cross the curve through another point; the point is noted as -R. Then we reflect the point –R in the x-axis to the point R where R=2P.

The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and -P cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity O. By definition, P + (-P) = O. As a result of this equation, P + O = P in the elliptic curve group . O is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity.

Point P and the Negative of P from

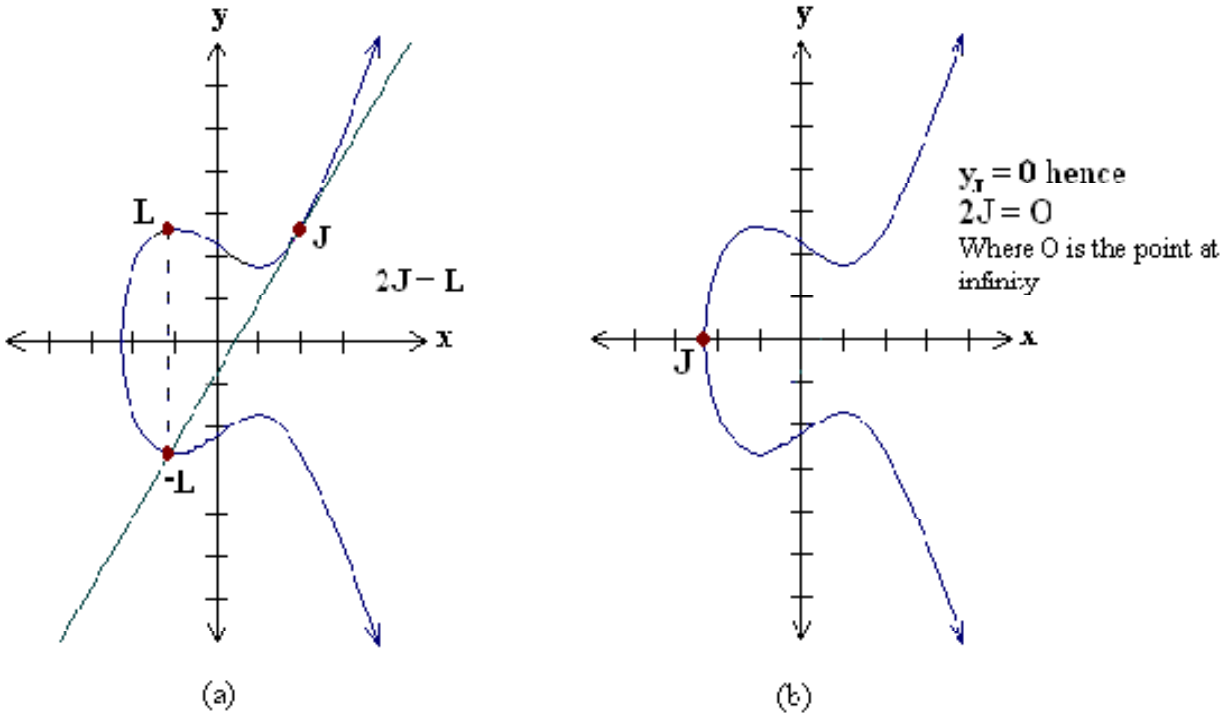
Figure 3.4



To add a point P to itself, a tangent line to the curve is drawn at the point P. If yP is not 0, then the tangent line intersects the elliptic curve at exactly one other point, -R. -R is reflected in the x-axis to R. This operation is called doubling the point P; the law for doubling a point on an elliptic curve group is defined by:

J+J=2L.

Figure 3.5



Doubling the point P if $Y_j = 0$ 2J=0.

If a point P is such that $Y_p = 0$, then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point.

By definition, 2P = O for such a point P. If one wanted to find 3P in this situation, one can add 2P + P. This becomes P + O = P Thus 3P = P.

3P = P, 4P = O, 5P = P, 6P = O, 7P = P,

Figure 3.6

Elliptic curves over real numbers: $y^2=x^3+ax+b$ with a=9,b=-2.

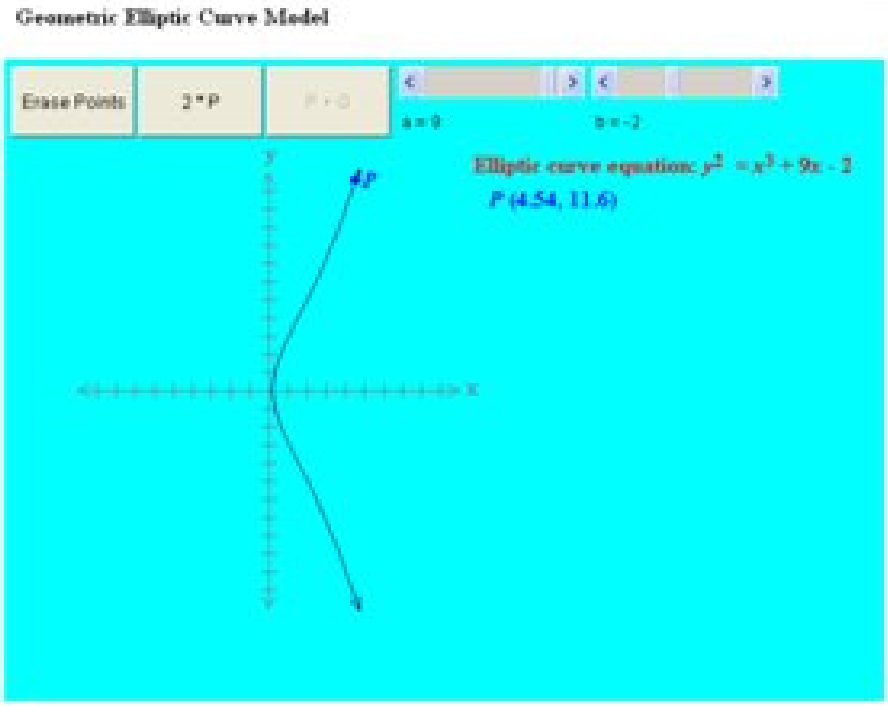


Figure 3.7

$y^2=x^3+ax+b$ with a=10,b=-10.

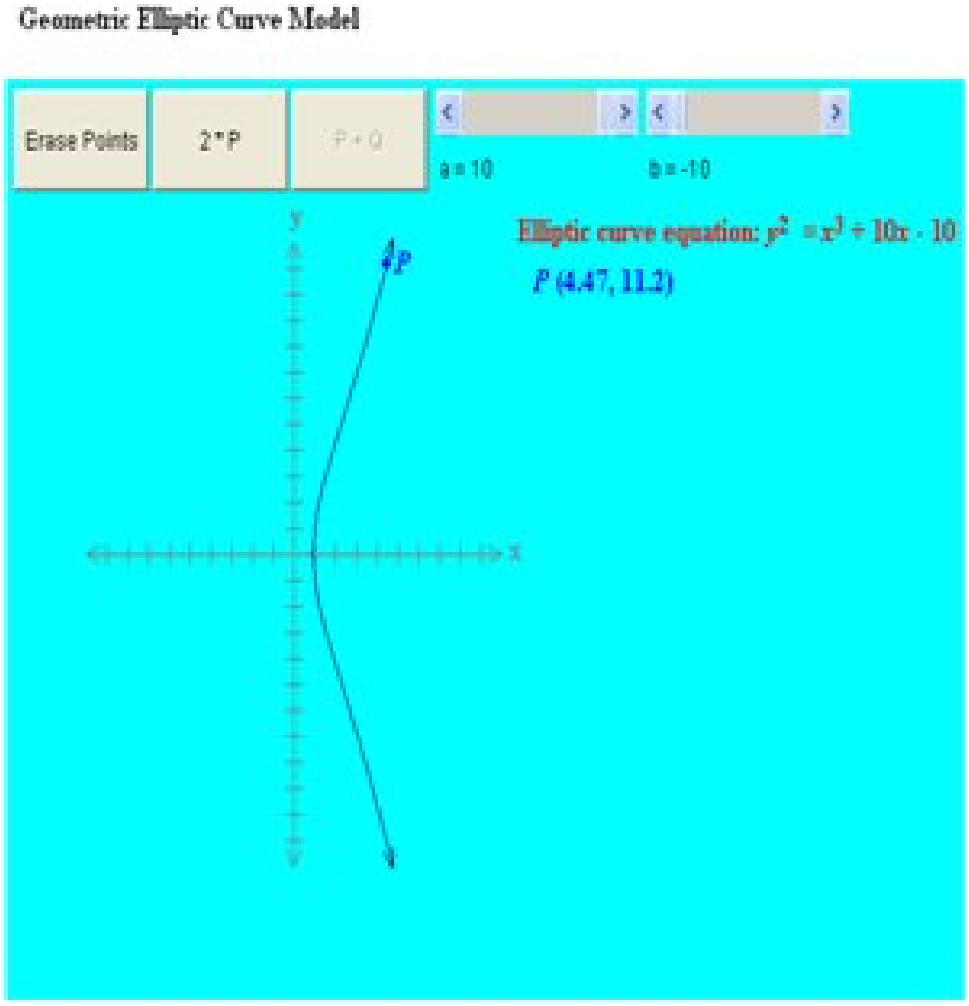


Figure 3.8

$y^2=x^3+ax+b$ with a=-4,b=9.

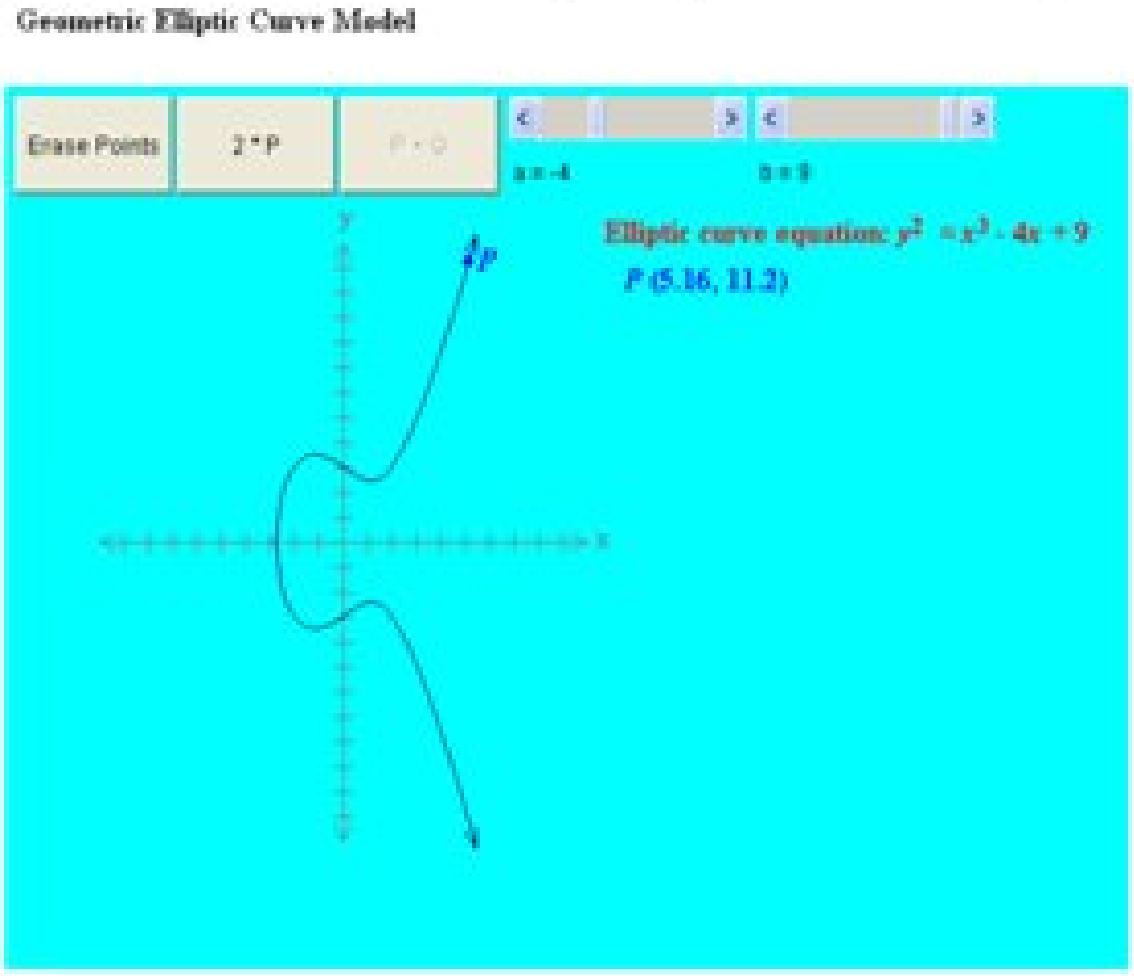


Figure 3.9

$y^2=x^3+ax+b$ with a=-8,b=8.

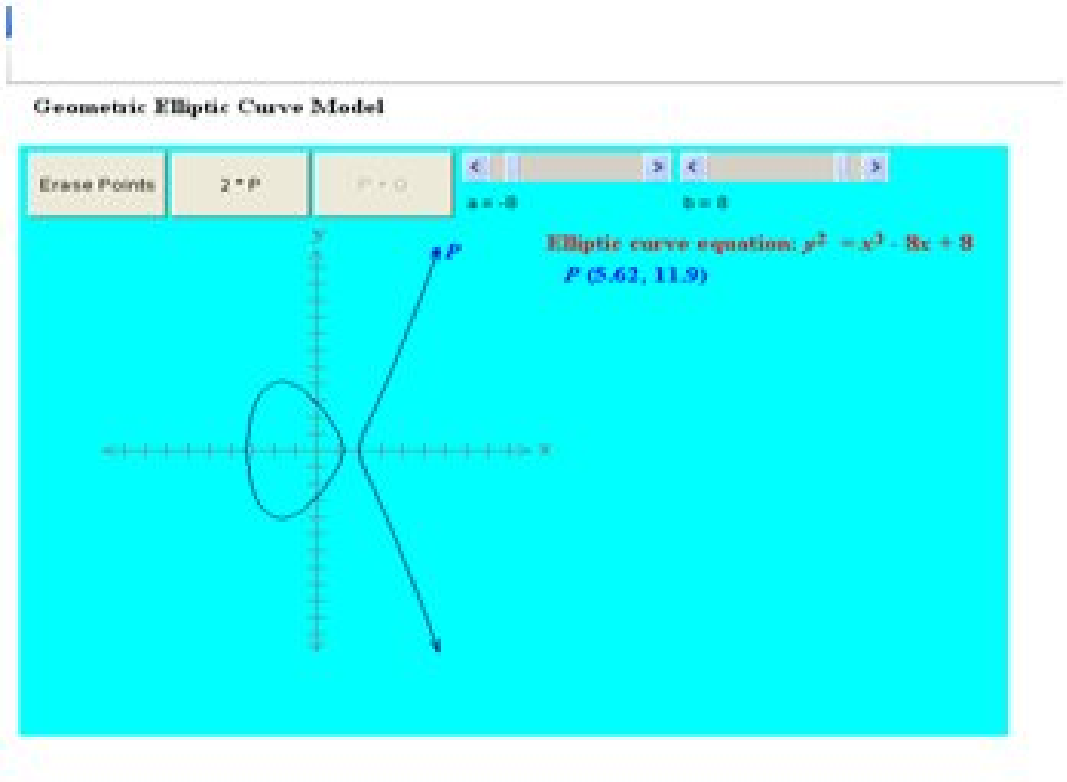


Figure 3.10

$y^2=x^3+ax+b$ with a=-7,b=8.

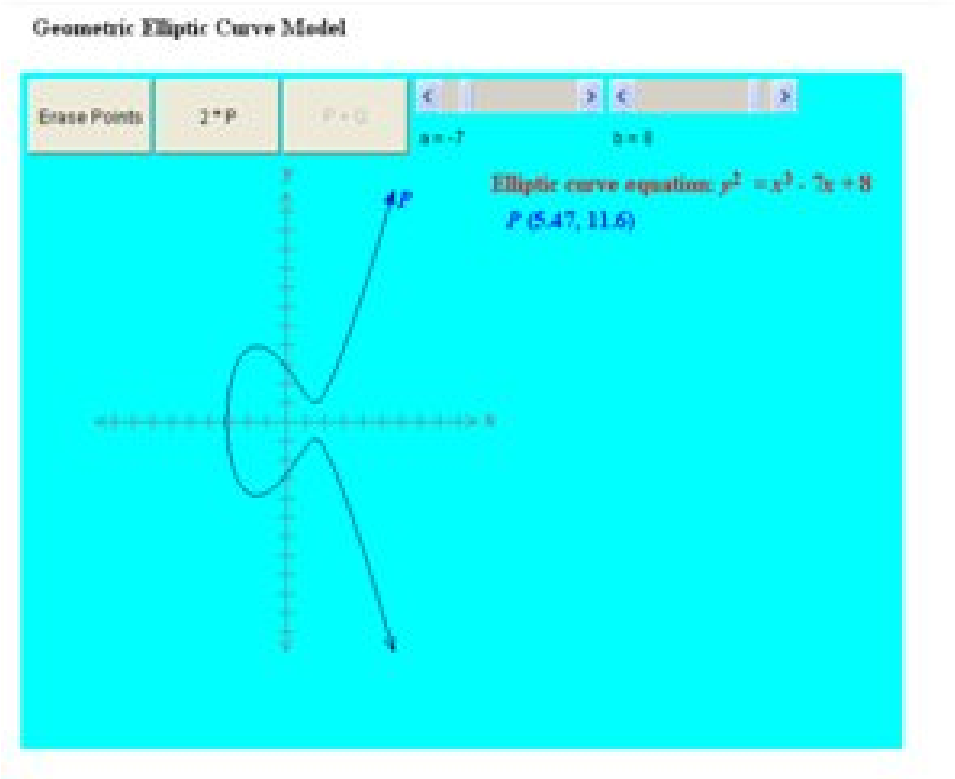
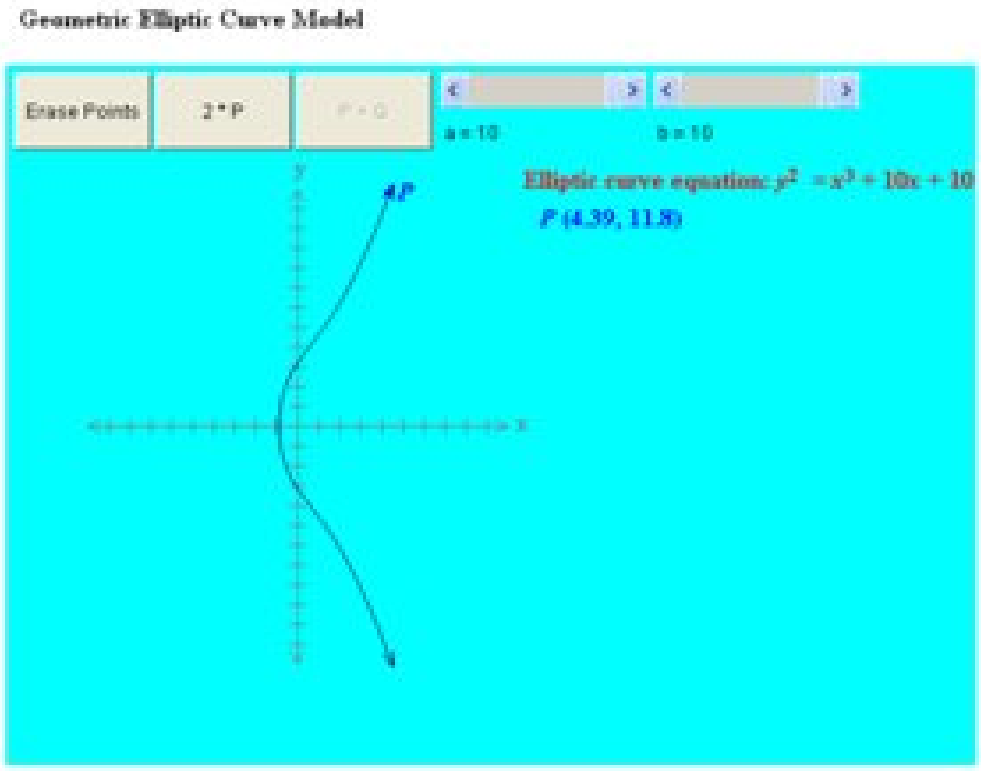


Figure 3.11

$y^2=x^3+ax+b$ with a=10,b=10.



3.3 Elliptic Curve Groups over Finite fields (Fp):

3.3.1. Introduction :

All elliptic curve operations mentioned earlier are based on real numbers. However, operations over the real numbers are inaccurate and slow, whereas cryptographic operations need to be accurate and fast. Therefore, the curve cryptography can be defined over finite fields to operate EC efficiently and accurately. A finite field is a set of a finite number of elements. Cryptographic applications require fast and precise arithmetic; thus elliptic curve groups over the finite fields of F_p and F_2m are used in practice.

Recall that the field Fp uses the numbers from 0 to p - 1, and computations end by taking the remainder on division by p. The number of points on $E(F\ p)$ is denoted by $\#E(F\ p)$. The Hasse Theorem states that:

$p+1-2\sqrt{p} \leq \#E(F\ p) \leq p+1+2\sqrt{p}$.

For example, in F_{23} the field is composed of integers from 0 to 22, and any operation within this field will result in an integer also between 0 and 22.

An elliptic curve with the underlying field of Fp can formed by choosing the variables a and b within the field of F_p. The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation modulo p (where x and y are numbers in F_p).

For example: $y^2 \bmod p = x^3 + ax + b \bmod p$ has an underlying field of Fp if a and b are in Fp.

If $x^3 + ax + b$ contains no repeating factors (or, equivalently, if $4a^3 + 27b^2 \bmod p$ is not 0), then the elliptic curve can be used to form a group. An elliptic curve group over Fp consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity. There are finitely many points on such an elliptic curve.

3.3.2 Example of an Elliptic Curve Group over Fp:

As a very small example, consider an elliptic curve over the field F_{23}. With a = 1 and b = 0, the elliptic curve equation is $y^2 = x^3 + x$. The point (9,5) satisfies this equation since $y^2 \bmod p = x^3 + x \bmod p$

25 mod 23 = 729 + 9 mod 23

25 mod 23 = 738 mod 23

2 = 2

The 23 points which satisfy this equation are:

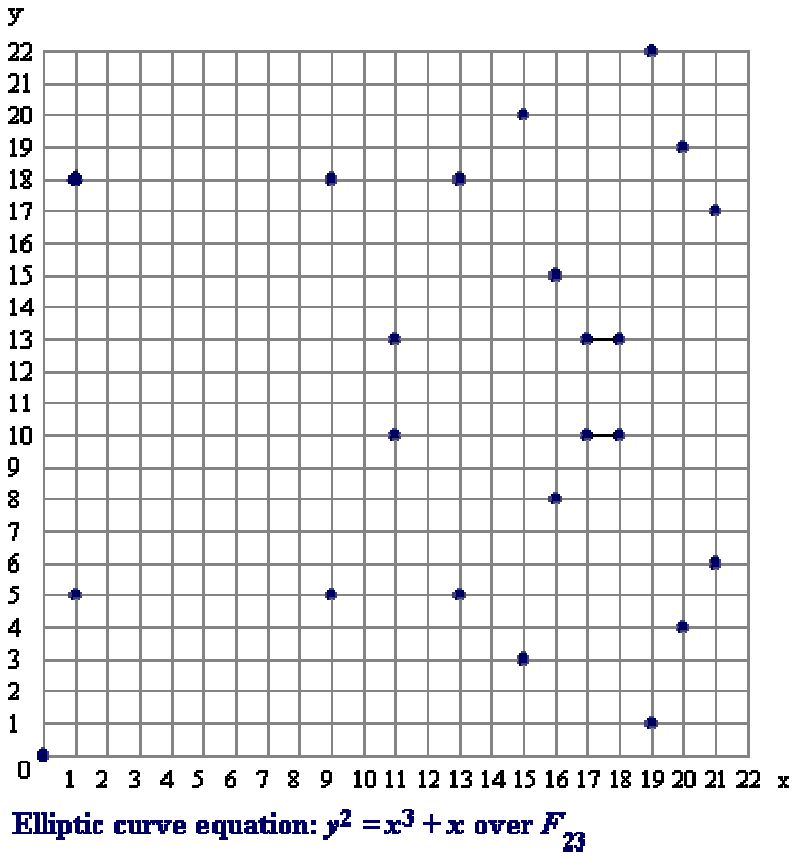
(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5)

(13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10)

(18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)

These points may be graphed as below:

Figure 3.3.2



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

Note that there is two points for every x value. Even though the graph seems random, there is

still symmetry about y = 11.5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. Over the field of F_{23}, the negative components in the y-values are taken modulo 23, resulting in a positive number as a difference from 23. Here $-P = (x_P, (-y_P \text{ Mod } 23))$

3.3.2.1 Arithmetic in Elliptic Curve Group over F_p

Point addition:

Note that these rules are exactly the same as those for elliptic curve groups over real numbers, with the exception that computations are performed modulo p.

There are several major differences between elliptic curve groups over F_p and over real numbers. Elliptic curve groups over F_p have a finite number of points, which is a desirable property for cryptographic purposes. Since these curves consist of a few discrete points, it is not clear how to "connect the dots" to make their graph look like a curve. It is not clear how geometric relationships can be applied. As a result, the geometry used in elliptic curve groups over real numbers cannot be used for elliptic curve groups over F_p. However, the algebraic rules for the arithmetic can be adapted for elliptic curves over F_p. Unlike elliptic curves over real numbers, computations over the field of F_p involve no round off error - an essential property required for a cryptosystem.

The rules for addition over Ep(a,b): Correspond to the algebraic technique described for elliptic curve defined over real numbers. For all points $P,Q \in E_p(a,b)$;

1.P+O=P.

2.If $P=(x_p,y_p)$, then $P+(x_p,-y_p)=O$. The point $(x_p,-yp)$ is the negative of P, denoted as –P. For example , in $E_{23}(1,1)$, for P=(13,7), we have –P=(13,-7).But -7 mod 23=16.Therefore –P=(13,16), which is also in $E_{23}(1,1)$

3.if $P=(x_P,y_P)$ and $Q=(x_Q,y_Q0$ with $P \neq -Q$, then $R=P+Q=(x_R,y_R)$ is determined by the following rules:

$X_R=(\lambda^2-x_P-x_Q) \text{ mod } p$, $Y_R=(\lambda(x_P-x_R)-y_P) \text{ mod } p$

Where

$\lambda=(\frac{y_{Q-y_P}}{x_{Q-x_P}}) \text{ mod } p \text{ if } P \neq Q$

$(\frac{3x_P{}^2+a}{2y_P})$ mod p if P=Q

3.3.2.2. Multiplication is defined as repeated addition; for example, 4P=P+P+P+P.

For example let P=(3,10) and Q=(9,7) in $E_{23}(1,1)$.Then

$\lambda=(\frac{7-10}{9-3})$ mod 23=$(\frac{-3}{6})$ mod 23=$(\frac{-1}{2})$ mod 23=11

xR=(112-3-9) mod 23=109 mod 23=17

y_R=(11(3-17)-10) mod 23=-164 mod 23=20

so P+Q=(17,20).To find 2P

$\lambda\frac{=(3(32)+1}{2x10})$ mod 23=$(\frac{5}{20})$ mod23=$(\frac{1}{4})$ mod 23=6

Figure 3.3.2

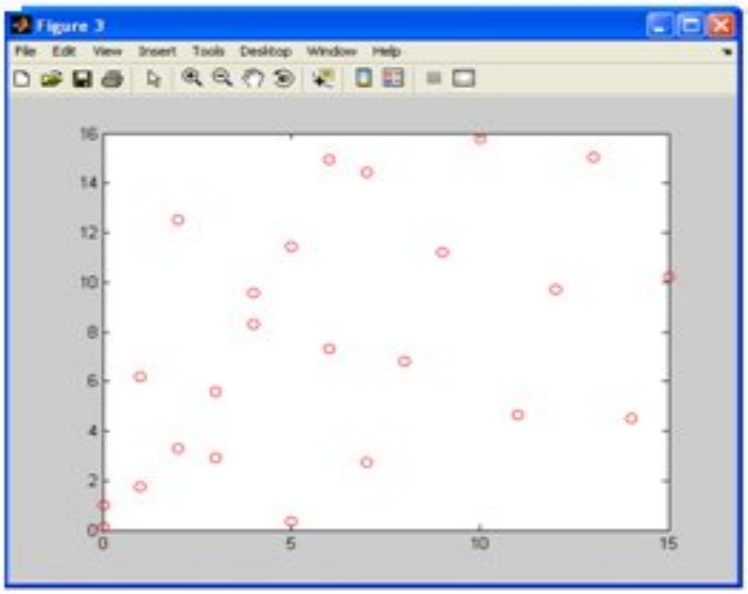
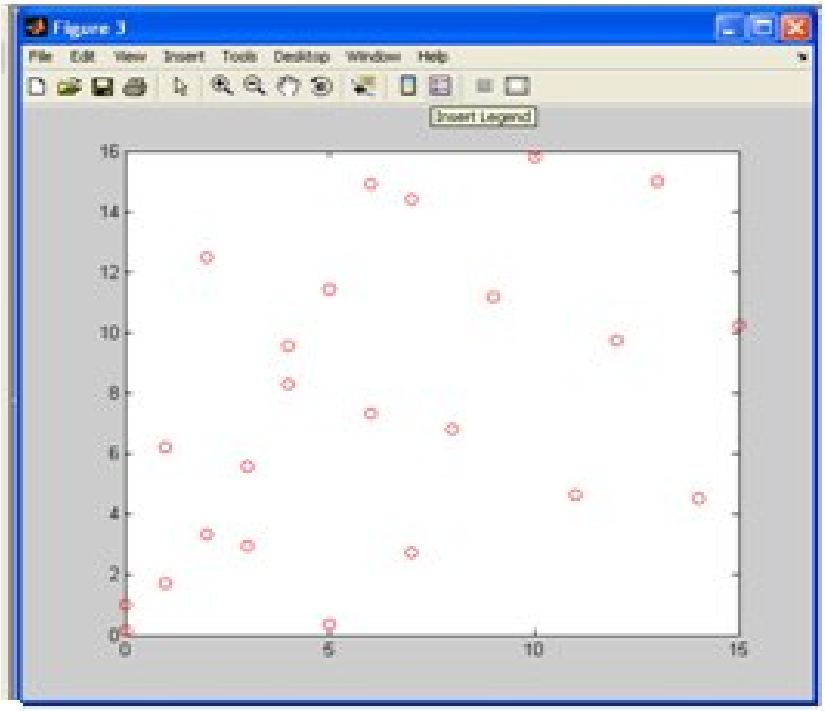


Figure 3.3.2.1

$y^2=x^3+ax+b$ with finite field over mod 23.



3.3.3. Elliptic Curve Groups over Binary field GF(2^n):

The number of points on E(F_2^m)() is denoted by #E(F_2^m). The Hasse Theorem states that:

$2^m+1-2\sqrt{2^m} \leq \#E(F_2^m) \leq 2^m+1+2\sqrt{2^m}$:

There are finitely many points on a curve over F_2^m .

Elements of the field F_2^m are m-bit strings. The rules for arithmetic in F_2m can be defined by either polynomial representation or by optimal normal basis representation. Since F_2m operates on bit strings, computers can perform arithmetic in this field very efficiently.

An elliptic curve with the underlying field F_2^m is formed by choosing the elements a and b within F_2m (the only condition is that b is not 0). As a result of the field F_2m having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation:

$y^2 + xy = x^3 + ax^2 + b$

The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over F_2m (where x and y are elements of F_2m). An elliptic curve group over F_2m consists of the points on the corresponding elliptic curve, together with a point at infinity, O. There are finitely many points on such an elliptic curve.

An Example of an Elliptic Curve Group over $F2^m$:

As a very small example, consider the field $F_2$4, defined by using polynomial representation with the irreducible polynomial $f(x) = x^4 + x + 1$.

The element g = (0010) is a generator for the field . The powers of g are:

g^0 = (0001) g^1 = (0010) g^2 = (0100) g^3 = (1000) g^4 = (0011) g^5 = (0110)

g^6 = (1100) g^7 = (1011) g^8 = (0101) g^9 = (1010) g^{10} = (0111) g^{11} = (1110)

g^{12} = (1111) g^{13} =(1101) g^{14} =(1001) g^{15} = (0001)

In a true cryptographic application, the parameter m must be large enough to preclude the efficient generation of such a table otherwise the cryptosystem can be broken. In today's practice, m = 160 is a suitable choice. The table allows the use of generator notation (g^e) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without reference to the irreducible polynomial

$f(x) = x^4 + x + 1$.

Consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. Here $a = g^4$ and $b = g^0 = 1$. The point (g^5, g^3) satisfies this equation over F_2^m :

$y^2 + xy = x^3 + g^4x^2 + 1$

$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$

$g^6 + g^8 = g^{15} + g^{14} + 1$

$(1100) + (0101) = (0001) + (1001) + (0001)$

$(1001) = (1001)$

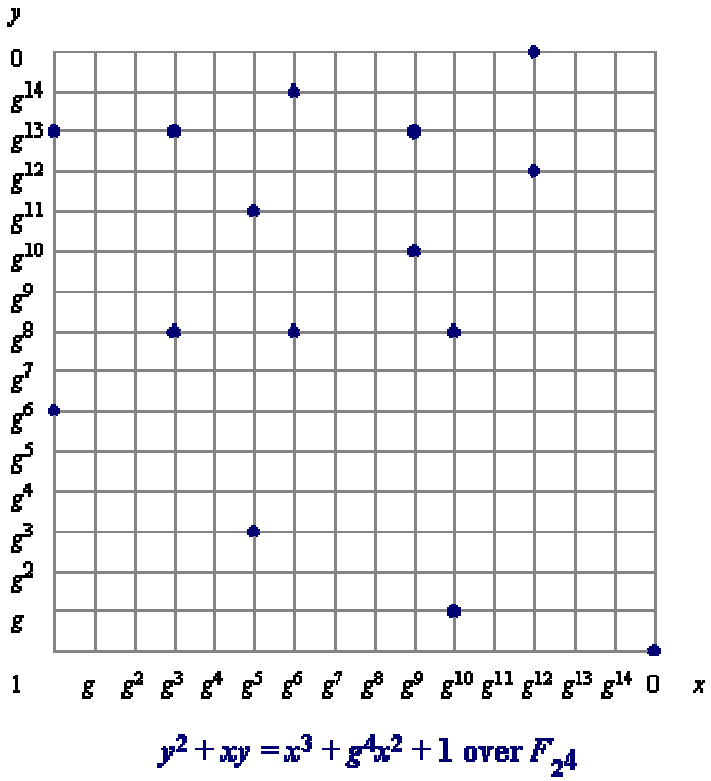
The fifteen points which satisfy this equation are:

$(1, g^{13})$ (g^3, g^{13}) (g^5, g^{11}) (g^6, g^{14}) (g^9, g^{13}) (g^{10}, g^8) (g^{12}, g^{12})

$(1, g^6)$ (g^3, g^8) (g^5, g^3) (g^6, g^8) (g^9, g^{10}) (g^{10}, g) $(g^{12}, 0)$ $(0, 1)$

These points are graphed below:

figure 3.3.3



Elliptic curve groups over F_2m have a finite number of points, and their arithmetic involves no round off error. This combined with the binary nature of the field, F_2m arithmetic can be performed very efficiently by a computer.

The following algebraic rules are applied for arithmetic over F_2m :

3.3.3.1 **Point addition (Adding distinct points P and Q)** :

The negative of the point P = (xP, yP) is the point -P = (xP, xP + yP). If P and Q are distinct points such that P is not -Q, then

P + Q = R where

s = (yP - yQ) / (xP + xQ)

$xR = s^2 + s + xP + xQ + a$ and yR = s(xP + xR) + xR + yP As with elliptic curve groups over real numbers, P + (-P) = O, the point at infinity. Furthermore, P + O = P for all points P in the elliptic

curve group.

3.3.3.2 Point doubling :

If xP = 0, then 2P = O

Provided that xP is not 0,

2P = R where

s = xP + yP / xP

$xR = s^2 + s + a$ and $yR = xP^2 + (s + 1) * xR$

Recall that a is one of the parameters chosen with the elliptic curve and that s is the slope of the line through P and Q

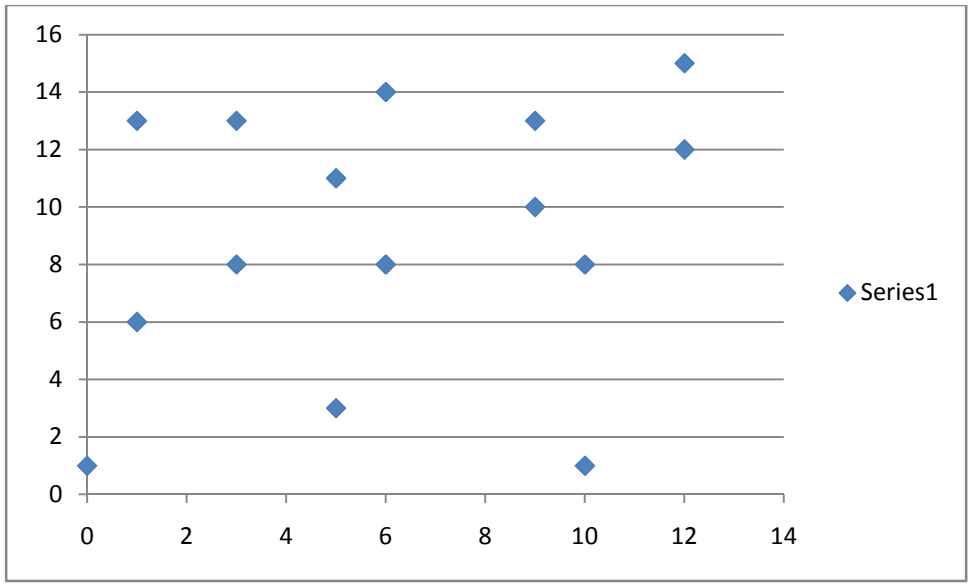
Elliptic curves over binary fields:

Let $y^2+xy=x^3+ax^2+b$ let $a=g^4$, b=1 the points and the graph is given by:

Table:3.1

x	Y
0	1
1	6
1	13
3	8
3	13
5	3
5	11
6	8
6	14
9	10
9	13
10	1
10	8
12	12
12	15

Figure 3.3.3.1

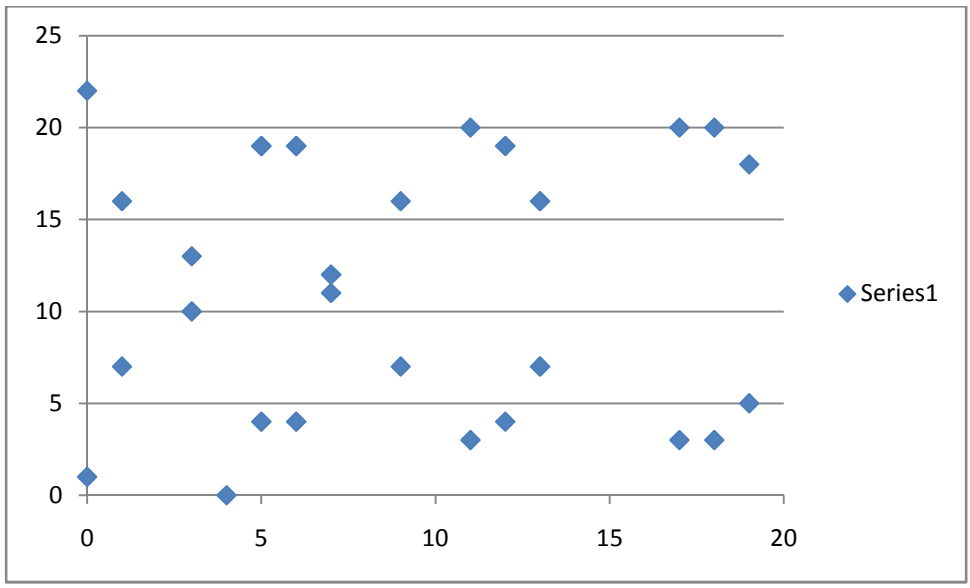


1: The points on the **Elliptic curve** $y^2 = x^3$ **+x+1 here a=1,b=1 and p=23** are given by

0	1	17	20
0	22	18	3
1	7	18	20
1	16	19	5
3	10	19	18
3	13		
4	0		
5	4		
5	19		
6	4		
6	19		
7	11		
7	12		
9	7		
9	16		
11	3		
11	20		
12	4		
12	19		
13	7		
13	16		
17	3		

Table:3.2

Figure 3.3.3.2

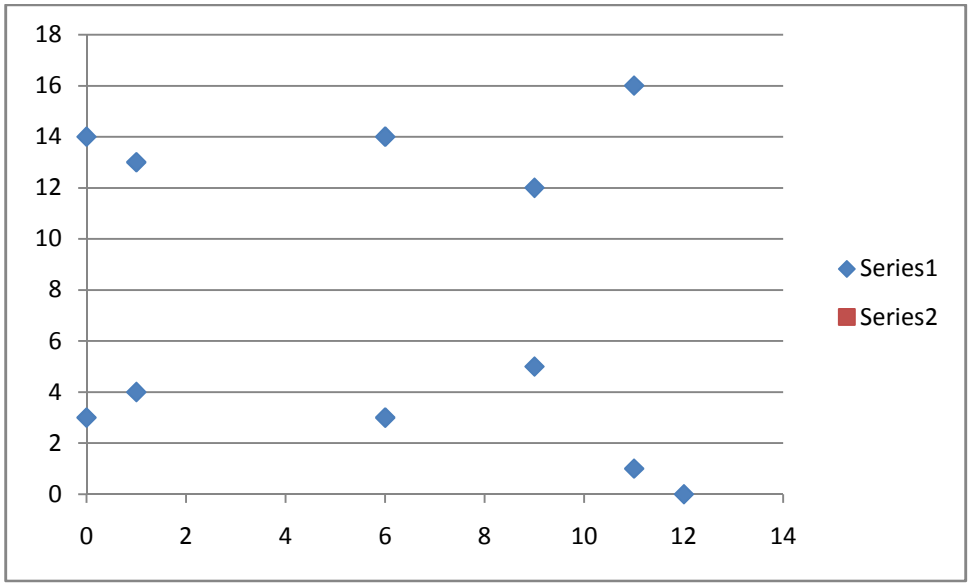


Similarly consider the **Elliptic curve** $y^2 = x^3$ **+10x+5 here a=3,b=5 and p=17** the points are given by

0	3
0	14
1	4
1	13
6	3
6	14
9	12
9	5
11	1
11	16
12	0

Table: 3.3 the graph is given by

Figure 3.3..3.3



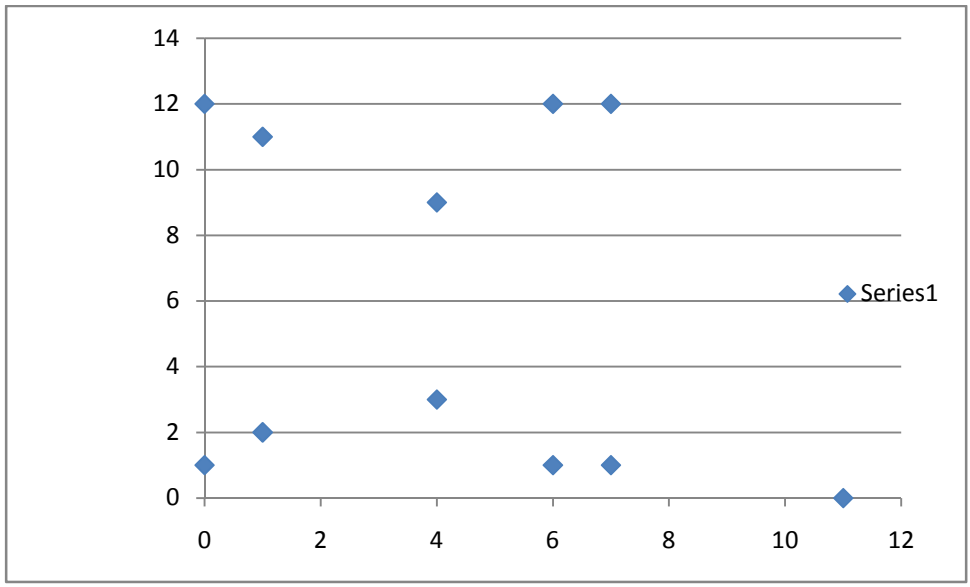
Let the **Elliptic curve $y^2 = x^3$ +3x+1 here a=3, b=1 and p=13**and the points are given by

Table: 3.4

0	1
0	12
1	2
1	11
4	3
4	9
6	1
6	12
7	1
7	12
11	0

The graph is given by:

figure 3.3.3.3.4



3.3.3.3 Construction of finite field of order 2^8 :

Construction of finite field of order 2^8 GF (2^8) with the irreducible polynomial(x) $=x^8+x^4+x^2+x+1$.Let a be a point in this polynomial then $a^8=a^4+a^3+a^2+1$.

As α is a primitive element of GF(2^8),every element x of GF(2^8) may be expressed as $a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5+a_6\alpha^6+a_7\alpha^7$ $a_i \in GF(2^8)$,$0 \leq i \leq 7$.It is represented as 8-tuple $(a_0,a_1,a_2,a_3,a_4,a_5,a_6, a_7)$.By this terminology we have

$\alpha^0=(1,0,0,0,0,0,0,0)$,$\alpha^1=(0,1,0,0,0,0,0,0)\alpha^2=(0,0,1,0,0,0)$,$\alpha^3=(0,0,0,1,0,0,0,0)$,$\alpha^4=(0,0,0,0,1,0)$

$\alpha^5=(0,0,0,0,0,10,0,)$ $\alpha^6=(0,0,0,0,0,0,1,0)$,$\alpha^7=(0,0,0,0,0,0,0,1)$

And $\alpha^8=\alpha^4+\alpha^3+\alpha^2+1=(10,1,1,1,0,0,0,0)$,we get $\alpha^9=\alpha^5+\alpha^4+\alpha^3+\alpha=(0,1,0,1,1,1,0,0)$The other powers of α are computed similarly with the following table.

Table for order GF(2^8):

Table:3.5

i	a^i	42	10101101	85	01101011	128	10100001	171	11001101	214	10011111
0	10000000	43	11101110	86	10001101	129	11101000	172	11011110	215	11110111
1	01000000	44	01110111	87	11111110	130	01110100	173	01101111	216	11000011
2	00100000	45	10000011	88	01111111	131	00111010	174	10001111	217	11011001
3	00010000	46	11111001	89	10000111	132	00011101	175	11111111	218	11010100
4	00001000	47	11000100	90	11111011	133	10110110	176	11000111	219	01101010
5	00000100	48	01100010	91	11000101	134	01011011	177	11011011	220	00110101
6	00000010	49	00110001	92	11011010	135	10010101	178	11010101	221	10100010
7	00000001	50	10100000	93	01101101	136	11110010	179	11010010	222	01010001
8	10111000	51	01010000	94	10001110	137	01111001	180	01101001	223	10010000
9	01011100	52	00101000	95	01000111	138	10000100	181	10001100	224	01001000
10	00101110	53	00010100	96	10011011	139	01000010	182	01000110	225	00100100
11	00010111	54	00001010	97	11110101	140	00100001	183	00100011	226	00010010
12	10110011	55	00000101	98	11000010	141	10101000	184	10101001	227	00001001
13	11100001	56	10111010	99	01100001	142	01010100	185	11101100	228	10111100
14	11001000	57	01011101	100	10001000	143	00101010	186	01110110	229	01011110
15	01100100	58	10010110	101	01000100	144	00010101	187	00111011	230	00101111
16	00110010	59	01001011	102	00100010	145	10110010	188	10100101	231	10101111
17	00011001	60	10011101	103	00010001	146	1011001	189	11101010	232	11101111
18	10110100	61	11110110	104	10110000	147	10010100	190	01110101	233	11001111
19	01011010	62	01111011	105	01011000	148	01001010	191	10000010	234	11011111
20	00101101	63	10000101	106	00101100	149	00100101	192	01000001	235	11010111
21	10101110	64	11111010	107	00010110	150	10101010	193	10011000	236	11010011
22	01010111	65	01111101	108	00001011	151	01010101	194	01001100	237	11010001
23	10010011	66	10000110	109	10111101	152	10010010	195	00100110	238	11010000
24	11110001	67	01000011	110	11100110	153	01001001	196	00010011	239	01101000
25	11000000	68	10011001	111	01110011	154	10011100	197	10110001	240	00110100
26	01100000	69	11110100	112	10000001	155	01001110	198	11100000	241	00011010
27	00110000	70	01111010	113	11111000	156	00100111	199	01110000	242	00001101
28	00011000	71	00111101	114	01111100	157	10101011	200	00111000	243	10111110
29	00001100	72	10100110	115	00111110	158	11101101	201	00011100	244	01011111
30	00000110	73	01010011	116	00011111	159	11001110	202	00001110	245	10010111
31	00000011	74	10010001	117	10110111	160	01100111	203	00000111	246	11110011
32	10111001	75	11110000	118	11100011	161	10001011	204	10111011	247	11000001
33	11100100	76	01111000	119	11001001	162	11111101	205	11100101	248	11011000
34	01110010	77	00111100	120	11011100	163	11000110	206	11001010	249	01101100
35	00111001	78	00011110	121	01101110	164	01100011	207	01100101	250	00110110
36	10100100	79	00001111	122	00110111	165	10001001	208	10001010	251	00011011
37	01010010	80	10111111	123	10100011	166	11111100	209	01000101	252	10110101
38	00101001	81	11100111	124	11101001	167	01111110	210	10011010	253	11100010
39	10101100	82	11001011	125	11001100	168	00111111	211	01001101	254	01110001
40	01010110	83	11011101	126	01100110	169	10100111	212	10011110	255	10000000
41	00101011	84	11010110	127	00110011	170	11101011	213	01001111		

A finite field of order 2^4it is also a subfield of order 2^8

Table:3.6

i	a^i
0	00000000
17	10011000
34	01001110
51	00001010
68	10011001
85	11010110
102	01000100
119	10010011
136	01001111
153	10010010
170	11010111
187	11011100
204	11011101
221	01000101
238	00001011
255	00000001

Multiplication table is given by here for the curve $y^2+xy=x^3+ax^2+b$ let $a=g^4$, $b=1$

	0	1	g	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}	g^{12}	g^{13}	g^{14}	g^{15}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1
g	0	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g
g_2	0	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2
g_3	0	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3
g_4	0	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1
g_5	0	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g
g_6	0	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2
g_7	0	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1
g_8	0	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1
g_9	0	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	G	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g
g_{10}	0	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1
g_{11}	0	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g
g_{12}	0	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1
g_{13}	0	g^3+g^2+1	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1
g_{14}	0	g^3+1	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1
g_{15}	0	1	g	g^2	g^3	g+1	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1

Similarly the multiplication table for the GF(2^8) with the irreducible polynomial

Consider the Elliptic curve $E_2^8(a,b)$

$Y^2+xy=x^3+ax^2+b$

Let a=1,b=1 $4a^3+27b^2\neq 0$

Hence $E_2^8(1,1)$ exists.

$Y^2+xy=x^3+g^{17}x^2+1$ . . . .(I)

Put x=0 $y^2=1$

$Y=\pm 1$

i.e. (0,1) is a point on the curve (I)

$Y^2+xy=x^3+ax^2+b$

$Y^2=x^3+ax^2+b-xy$

$Y^2=x^3+x^2+xy+1$

_____

Put $x=a^{17}$

$Y^2=a^{51}+a^{34}+a^{17}y+1$

$(00001010)+(01001110)+(a^{17}y)+(00000000)$

$=(01000101)+a^{17}y$

$a^{102}+a^{17}y$

$y^2=a^{102}+ya$

_____-

$a^{238}y^2=(a^{85}+y)$

$L.H.S=a^{238}a^{34}=a^{17}$

$R=a^{34}$

$a^{238}a^{68}=a^{85}+a^{34}$

$=a^{51}$

$x^{-1}y^2=x^2+x+x^{-1})+y$

$a^{238}y^2=(a^{34}+a^{119})+y \ =a^{170}+y$

$Y^2=a^{187}+a^{17}y$

$Y^2=a^{187}+a^{17}y$

$y^2+xy=x^3+a^{51}x^2+1$

$y^2=x^3+a^{51}x^2+xy+1$

$y^2=a^{51}+a^{51}a^{34}+a^{17}y+1$

$=a^{51}(1+a^{34})+a^{17}y+1$

$=a^{51}.a^{136}+a^{17}y+1$

$=a^{204}+a1^{7}y$

$a^{34}=x^3+a^{51}x^2+a^{17}x+1$

$a^{34}+1=x^2(x+a^{51})+(a^{17}x+1)$

$(x+1)(x^2+x+1)+a^{17}x(a^{34}x+1)$

$Xy+y^2=x^3+Ax^2+B$

$Xy+y^2=x^{51}+Ax^{34}+B$

Put B=1

$a^{17}y+y^2=a^{51}+Ax^{34}+1=(00001010)+Aa^{34}+1$

put $A=a^{51}$ $xy=(00001010)+a^{85}+1$

$(00001010)+(11010110)+(00000001)$

$=(11011101)=a^{204}$

$a^{51}+a^{153}=a^{17}$

$y^2+a^{17}y+a^{204}=0$

$y^2+(a^{51}+a^{13})+a^{51}a^{103}=0$

$(y+a^{5(})(y+a^{153})=0$

Put $x=a^{68}$

$X^3+a^{51}x^2+1=a^{204}+a^{51}a^{136}+1$

$=a^{204}+a^{187}+1$

$Y^2+xy=0$ $y^2+a^{68}y=0$

Global public key elements:

$E_2^8(a^{51},1)$ Elliptic curve with parameters $P(a^{51},1)$,$Q=2^8$.

Let G=point on the Elliptic curve whose order is large let (a^{17},a^{51}) $y^2+xy=x^3+a^{51}x^2+1$.

P$((x_p,y_p)$ then **R=2P**,$a=a^{51}$

P=Q $x_R=\lambda^2+\lambda+a$

$Y_R=x_P^2+(\lambda+1)x_R$

$\lambda=a^{17}+a^{51}/a^{17}=a^{17}+a^{34}$

$x_R=(a^{17}+a^{34})^2+(a^{17}+a^{34})+a^{51}$

$(a^{17}+a^{34})(a^{17}+a^{34}+1)+a^{51}$

$=a^{85}(a^{85}+1)+a^{51}$

$a^{170}+a^{85}+a^{51}$

$=a^{238.}$

$Y_R=a^{34}+(a^{17}+a^{34}+1)a238$

$=a^{34}+(a^{85}+1)a^{238}$

$=a^{34}+a^{323}+a^{238}$

$=a^{34}+a^{68}+a^{238}$

$=a^{34}+a^{153}$

$=a^{1877}$

2P$=(a^{238},a^{187})$.

3P=P+2P $(a^{17},a^{51})+(a^{238},a^{187})$

P≠Q

$X_R=\lambda^2+\lambda+x_P+x_Q+a$

$Y_R=\lambda(x_P+x_R)+x_R+y_P$

$=a^{187}+a^{51}/a^{238}+a^{17}$

$a^{85}/a^{119} \quad =a^{221}$

$x_R=a^{442}+a^{221}+a^{17}+a^{238}+a^{51}$

$=a^{187}+^{221}+a^{17}+a^{238}+a^{51}$

$a^{51}+a^{51}=0$

$y_R=a^{221}(a^{17}+0)+0+a^{17}$

$a^{238}+a^{17}=a^{119}$

3P$=(0,a^{119})$

4P=2P+2P

$=(a^{238},a^{187})+(a^{238},a^{187})$

$=\lambda=x_P+y_P/x_P=a^{238}+a^{187}/a^{238}=a^{238}+a^{204}=a^{85}$

$X_R=\lambda^2+\lambda+a=a^{51}$

$Y_R=x_P{}^2+(\lambda+1)x_R$

$a^{221}+a^{136}+a^{51}=0$

i.e $4P=(a^{51},0)$

5P=4P+P

P$\neq \boldsymbol{Q}$

$X_R=\lambda^2+\lambda+x_P+x_Q+a$

$Y_R=\lambda(x_P+x_R)+x_R+y_P$

$X_R=a^{306}+a^{153}+a^{51}+a^{17}+a^{51}=a^{17}+a^{17}=0$

$Y_R=a^{153}(a^{51}+0)+0+0=a^{136}$

5P$=(0,a^{136})$

6P=5P+P$=(0,a^{136})+(a^{17}+a^{51})=(\infty,\infty)$ The points on the curve are

P$=(a^{17},a^{51})$

2P=(a^{238},a^{187})

3P=(0,a^{119})

4P=(a^{51},0)

5P=(0,a^{136})

6P=(∞,∞)

Points are

P=(a^{17},a^{51})

2P=(a^{238},a^{187})

3P=(0,a^{119})

4P=(a^{51},0)

5P=(0,a^{136})

6P=(∞,∞)

3.3.3.4 Cryptosystem of order 2^8 :

$E_q(a,b)$ elliptic curve with parameters a and q where q is a prime or an integer of the form 2^m

G point on elliptic curve whose order is large value n let G=(a^{17},a^{51}) n=6

User A key generation: Select private n_A ∋ n_a<n

i.e n_A=2

calculate public key $P_A=n_AXG$

$2(a^{17},a^{51})$

$=(a^{238},a^{187})$

User B key generation:

Select private key n_B n_B<n

i.e n_B=1

calculate public key P_B i.e $P_B=n_BXG=1(a^{17},a^{51})$

calculation of secret key by user A

$$K=n_A X P_B=2(a^{17},a^{51})$$

$$=(a^{238},a^{187})$$

Calculation of secret key by user B:

$$K=n_B X P_A$$

$$=1(a^{238},a^{187})$$

$$=(a^{238},a^{187})$$

The two calculations in this produce the same result, because

$n_A X P_B=n_A X(n_B XG)=n_B X(n_A XG)=n_B XP_A$

$n_A XP_B=n_B XP_A.$

$E_2^8(a^{34},a^{187})$ elliptic curve with parameters $P(a^{34},a^{187})$ G is point on the elliptic curve whose order is very large

Let (a^{34},a^{187})

$Y^2+xy=x^3+a^{51}x^2+1$

$L.H.S=A^{374}+A^{221}$

$=a^{85}$

$R.H.S= a^{102}+a^{51+68}+1$

$=a^{85}$

L.H.S=R.H.S

P=Q

$P(x_P,y_P)$ then R=2P

$X_R=\lambda^2+\lambda+a$

$Y_R=x_P^2+(\lambda+1)$

$\lambda=a^{187}$

$X_R=a^{221}$

$Y_R=a^{34}$

$2P=(a^{221},a^{34})$

3P=2P+P= $a^{221},a^{34})+(a^{34},a^{187})$

P≠Q here

$X_R=\lambda^2+\lambda+x_P+x_Q+a$, $Y_R=\lambda(x_P+x_R)+x_R+y_P$

$\lambda=a^{170}$

$x_R=0$

$y_R=1$

3P=(0,1)

4P=2P+2P

$(a^{221},a^{34})+(a^{221},a^{34})$

$\lambda=a^{187}$

$x_R=a^{221}$

$y_R=a^{238}$

4P=(a^{221},a^{238})

5P=4P+P=$(a^{221},a^{238})+(a^{34},a^{187})$

$\lambda=a^{187}$

$x_R=a^{34}$

$y_R=a^{153}$

5P=(a^{34},a^{153})

6P=2(3P)=3P+3P=(0,1)+(0,1)

$\lambda=\infty$

$x_R=\infty$

$y_R=\infty$

Similarly another cryptosystem is given with the following points on the curve

$Y^2+xy=x^3+ax^2+b$

$a=a^{51}$

P=(a^{34},a^{187})

2P=(a^{221},a^{34})

3P=(0,1)

4P=(a^{221},a^{238})

5P=(a^{34},a^{153})

6P=(∞,∞)

Cryptosystem:

Let n=6

G=(a^{34},a^{187})

User A key generation: select private key $n_A \ni n_A<n$

i.e $n_{A=4}$

calculate public key $P_A=n_AXG=4(a^{34},a^{187})$

$=(a^{221},a^{238})$

User B key generation:

Select private key $n_B \ni n_B<n$

$n_B<n$

i.e $n_B=5$

calculate public key P_Bi.e $P_B=n_BXG=5(a^{34},a^{187})=(a^{34},a^{153})$

calculate of secret key by user A:

$k=n_AXP_B=4(a^{34},a^{187})$

$=(a^{221},a^{34})$

Calculation of secret key by user B:

$K=n_BXP_A=5(a^{221},a^{238})$

$=(a^{221},a^{34})$

The two calculations in this produce the same result, because

$n_AX\ P_B=n_AX(n_BXG)=n_BX(n_AXG)=n_BXP_A$

$n_AXP_B=n_BXP_A$.

Conclusion third chapter ECC:

In this chapter, an introduction of ECC operations over binary field, prime field and their mathematical operations is explained. With clear examples, how the field operation level work over both fields (Binary, Prime) are shown. Then, higher level operations (ECC operations) are discussed. The process of adding point to another point and point doubling in order to produce a new point is explained .We explained the construction of finite field of order2^8 .This chapter gives the cryptosystem over the binary field of order 2^8

CHAPTER 4

Elliptic curve group and discrete logarithmic problem: