Elliptic Curve based Cryptographic Encryption Schemes

Arvind[1] and Mohd Sarik Idrisi[2]

[1]Associate Professor, Hansraj College, Email-arvind_ashu12@rediffmail.com
[2]Research Scholar, Department of Mathematics, Miranda House, Email-sarikidrisi@gmail.com

Abstract

Cryptography is a very important emergent branch of mathematics in 20th century. By using cryptography, we can securely transfer data from one party to another party maintaining data integrity, confidentiality, authentication and proper access. Public key cryptography is a very important type of Cryptography. Using RSA, ElGamal and Elliptic Curve Cryptography(ECC), we can securely transfer data. ECC scheme requires less computational complexity and gives similar security by using smaller key as we get in Symmetric and RSA schemes method with larger key. The security of ECC totally depend on the Elliptic Curve Discrete Logarithm Problem(ECDLP).

Keywords: ECC, ECDLP, Brute-force, Weierstrass.

Introduction

Cryptography is a very important branch of mathematics which provide secure channel to share information to one person to another person in the presence of malicious third person. Two important parts of any cryptography scheme is **Encryption** and **Decryption**. The original message is said to be **plaintext** and codded message is known as **ciphertext**(scrambled text).

Encryption(**enciphering**) transform input message into ciphertext and Decryption(**deciphering** inverse of enciphering) transform ciphertext into input message using given algorithm and secret key. A Cryptographic system is also known as **Cipher.**

Encryption $C=E(K,P)$,

Decryption $P=D(K,C)$ and K is a secret key.

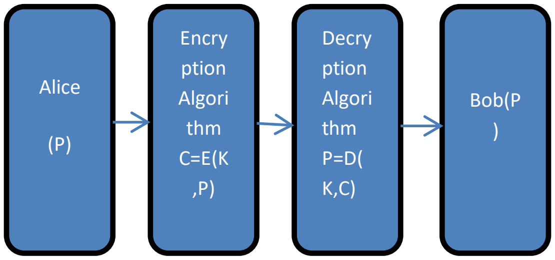

Figure-1.1: Simple Model of Symmetric Encryption

Clearly, $E(D(m,K),K) = D(E(m,K)) = m$, where m is a plaintext.

This is the simple method to see how encryption and decryption work. How will you ensure that Bob gets the same plaintext as the one sent by Alice . Let Bob receive $P1$, then we see

$$P1 = D(E(P,K),K) = P.$$

Cryptographic scheme divided into two types. Symmetric-key Cryptography and Asymmetric-Key Cryptography. In symmetric-key cryptography, the same key is used in encryption and decryption. DES, AES-128 [5] are some examples of symmetric-key cryptography. If different keys used in enciphering and deciphering, then this is asymmetric key cryptography. RSA, ElGamal, Diffie-Hellman and Elliptic Curve Cryptography(ECC) [5] etc are example of Asymmetric Cryptography.

Asymmetric -key cryptography is also known as Public-key Cryptography. Now, the question is how will we choose best algorithm for data transfer? Suppose that an attacker intercepted the ciphertext, but he cannot determine any properties of the plaintext or key, then we can use this algorithm for our message transmission. Apart from this, cryptography provides data integrity, confidentiality, user authentication, and Non-repudiation.

In the diagram

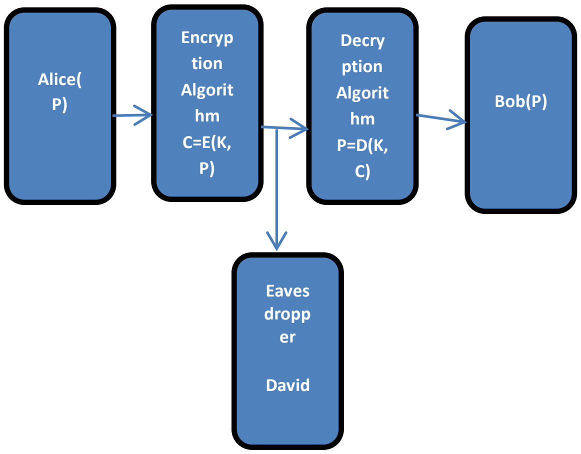

Figure -1.2: Attack on Symmetric Encryption

From the above flow chart we see , Alice sends a message (plaintext) to Bob then an Eavesdropper David somehow accesses the cipher text and tries to get the plaintext. If he did not know the algorithm and key pace(possible number of keys), then he got the message(plaintext) but this depends on the size of key space. But if David objective is not to attack on encryption system to recover just plaintext, because he want to find the key. Presently, there are two such methods exists in cryptography - **Cryptanalysis** and **Brute-force attack**.

In Brute-force attack, the attacker check each possible key of key space on the ciphertext until he got the piece of meaningful plaintext. Brute-force is applicable when the key space of encryption system is small. But this methods is impractical, if the key space is very large . For example in DES with a key length of 56 bits, then there are approximately $2^{56} \approx 7.2 \times 10^{16}$ keys. If the eavesdropper tries to search a key, then on average he will have to try half keys, a single machine which calculating DES encryption per microsecond would take more than a thousands years to break the DES Cryptographic System. Therefore, they have discover second method- Cryptanalysis, in this method eavesdropper do study about the algorithm, key type(size) and general characteristics of the plaintext used in algorithm. Using all these information they can obtain plaintext or the key being used in encryption.

Now by [**2**], the Table -1 compares the key length(size) of different cryptographic scheme.

Table -1 shows that , RSA and ECC both offer similar security with the different key sizes, ECC gives the same Cryptographic strength with smaller key size. Because in RSA, the computation involved in encryption(or decryption) are complex(at least 1024 bits) which make the system slower. In ECC encryption scheme, it involve less computational complexity but it provide similar security(as from RSA encryption scheme). That's why at present time Elliptic Curve Cryptography is a very secure and efficient method to encrypt data in Modern Cryptography.

Table -1: Comparable Key Size (in bits)

Comparable Key size(in bits)		
Symmetric	ECC	DH/DSA/RSA
80	163	1024
112	233	2048
128	283	3072
192	409	7680
256	571	15360

Elliptic Curve Cryptography (ECC)

Any curve of the form

$$E : y^2 = x^3 + ax + b \qquad (1)$$

is said to be an **Elliptic Curve,** where *a, b* are constants. This equation is also known as the **Weierstrass equation** for the elliptic curve. In general a, b, x and y belong to field ***Q****(rational numbers)* , ***R****(real numbers),* ***C****(Complex number),* finite field $F_q(=Z_q)$ for a prime number p or finite field F_q, where $q = p^k$ with $k \geq 1$. Let K be an arbitrary field such that $a,\ b \in K$, then we say E is defined on K.

If $E \subseteq L$, then we defined

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + ax + b\}.$$

Where ∞ denote a point at infinity.

Example 2.1: Let $y^2 = x^3 + 2x + 3$ be an elliptic curve over Z_5 (finite field). Then

$$E(Z_5) = \{\infty,\ (0,2),\ (0,3),\ (2,1),\ (2,4),\ (4,1),\ (4,4)\}$$

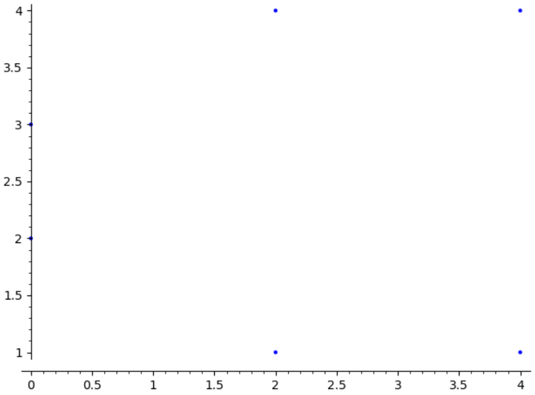

Figure-2.1: $y^2 = x^3 + 2x + 3$ over Z_5

Example 2.2: Let $y^2 = x^3 + 2x + 4$ be the elliptic curve over the real number ***R***. Then the plot of this curve is

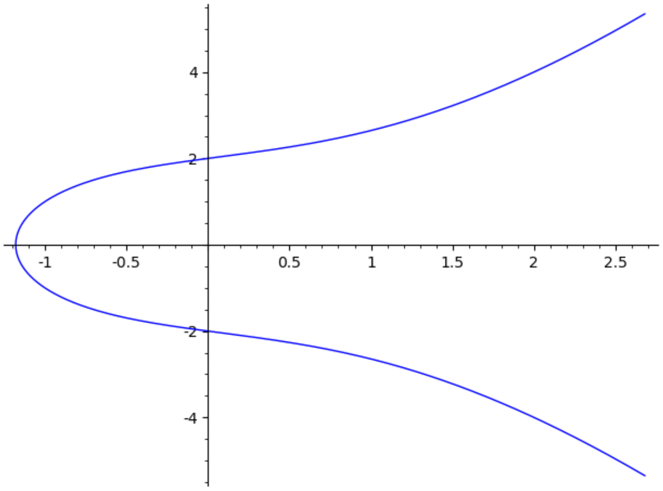

Figure-2.2:

$y^2 = x^3 + 2x + 4$

Similarly , the graphs of the curves(elliptic curve) $y^2 = x^3 - x$ and $y^2 = x^3 + x$ are given below

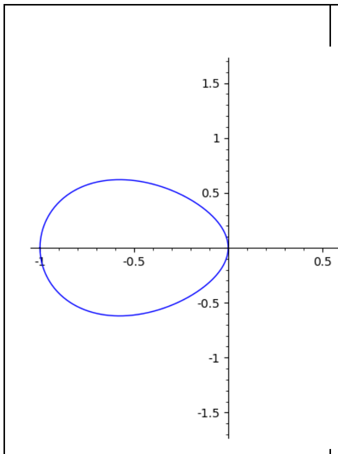

Figure-2.3: $y^2 = x^3 - x$

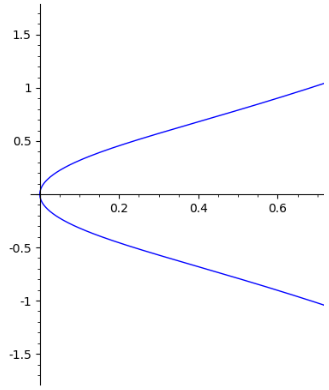

Figure-2.4: $y^2 = x^3 + x$

Clearly, we see that $y^2 = x^3 - x$ has three distinct roots where as $y^2 = x^3 + x$ has only one real root.

More general form of Weierstrass equation is

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6.$$

(2)

If the characteristic of field on which general elliptic curve defined is not 2 and 3, then (2) always be transformed into the equation

$$y^2 = x^3 + a^{'}x + b^{'} \qquad (3)$$

Singular: Let $E: y^2 = x^3 + ax + b$ be an elliptic curve. Then the discriminant of the elliptic curve E is given by the expression $-16(4a^3 + 27b^2)$. Elliptic Curve E is **non-singular** if and only if $-16(4a^3 + 27b^2) \neq 0$ [8, **Theorem 2.4**]. Any curve E which is not a non-singular is called **singular**.

j **-invariant :** Let $E: y^2 = x^3 + ax + b$ be an elliptic curve defined over a field K with characteristic of K is not 2 or 3. Then the value of j **-invariant** of any elliptic curve is given by the formula

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Theorem 2.4([**7, Theorem 2.19**]): Let $y_1^2 = x_1^3 + a_1x_1 + b_1$ and $y_2^2 = x_2^3 + a_2x_2 + b_2$ be two elliptic curves with j **-invariant** j_1 and j_2, respectively. If $j_1 = j_2$, then there exist $\mu \neq 0$ in $\overline{K}$ (=algebraic closure of K) such that

$a_2 = \mu^4 a_1$, $b_2 = \mu^6 b_1$.

The transformation

$x_2 = \mu^2 x_1$, $y_2 = \mu^3 y_1$

takes one equation to the other.

If the characteristics of the field is 2, then (2) convert to the following form

1. If $a_1 \neq 0$, then the equation (2) convert into the following form

$$y^2 + xy = x^3 + a^{'}_2x^2 + a^{'}_6$$

This curve is **non-singular** if and only if $a^{'}_6 \neq 0$.

2. If $a_1 = 0$, then the general Weierstrass equation (2) convert into the following form

$$y^2 + a^{'}_3y = x^3 + a^{'}_4x^2 + a^{'}_6$$

This curve is **non-singular** if and only if $a^{'}_3 \neq 0$.

Let E be elliptic curve whose graph is shown below. Let P and Q be two points lie on the elliptic curve, where $P = (x_1, y_1)$ and

$Q=(x_2,y_2)$. Now we define sum of two points P and Q on E as follows:

First we draw a line $L(x)$ between two points P and Q which cut the curve again at the point R. The point R is reflected with respect to x-axis, we get some point lie on the other side of the curve (see Figure-2.5) , say *-R*, the point *-R* is nothing but *P+Q*. We also have a direct formula to calculate $P+Q=(x_3,y_3)$. It is called the Group Law on the elliptic curve E.

Group Law [**7, Section 2.2**]:

1. If $x_1 \neq x_2$, then

$$x_3=m^2-x_1-x_2 \quad , \quad y_3=m(x_1-x_3)-y_1 \quad ,$$

where $m=\dfrac{y_2-y_1}{x_2-x_1}$.

2. If $x_1=x_2$ but $y_1 \neq y_2$, then $P+Q=\infty$.

3. If $P=Q$ and $y_1 \neq 0$, then $x_3=m^2-2x_1$, $y_3=m(x_1-x_3)-y_1$, where *m* is the slope of the tangent passing through point *P* and it can be calculated as $m=\dfrac{3x_1^2}{2y_1}$.

4. If $P=Q$ and $y_1=0$, then $P+Q=\infty$. Moreover, define $P+\infty=P$ for all points on E.

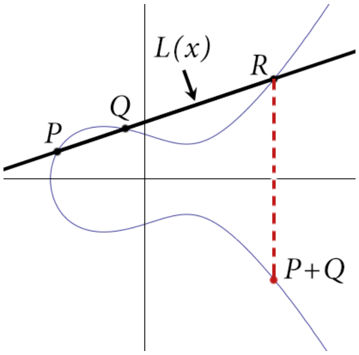

Figure-2.5: Addition of *P* and *Q* on *E*

We see that if two points P and Q both lies on the elliptic curve, then $P+Q$ will also lie on the curve. This implies that addition satisfies the closure property . Now , the following theorem show that set of all points on E including ∞ form a group,

Theorem 2.5([**7, Theorem 2.1**]): The addition of points on the elliptic curve E satisfies the following properties:

1. Commutativity: $P_1+P_2=P_2+P_1$ for all P_1, P_2 on E.

2. Existence of Identity: $P+\infty=P$ for all points P on E.

3. Existence of Inverse: Given P on E, there exist $P^{'}$ on E with $P+P^{'}=\infty$. This point $P^{'}$ will usually be denoted $-P$.

4. Associativity: $(P_1+P_2)+P_3 = P_1+(P_2+P_3)$ for all P_1, P_2, P_3 on E.

Therefore, the points on E from an additive abelian group with ∞ as the identity element.

If $P=(x,y)$, then $-P=(x,-y)$.

Example 2.6: Consider the curve E: $y^2=x^3-x$ over the set of rational number **Q.** Take P =(1,0) and Q =(-1,0), R =(0,0). Since P not equal to Q, then by Group law ,

$P+Q$ =(0,0) , since m =0,

$P+R$ =(-1,0)

$Q+R$ =(1,0)

Also , we see that $2P=\infty$, $2Q=\infty$ and $2R=\infty$.

Example 2.7: Consider an curve $y^2=x^3+1$ over the field $F_{13}(=Z_{13})$

$E(F_{13})=\{\infty,(0,1),(0,12),(2,3),(2,10),(4,0),(5,3),(5,10),(6,3),(6,10),(10,0),(12,0)\}$

Then, if we take P=(5,10)=(x_1, y_1), then

$2P = P + P$=(0,12)=(x_2, y_2),

since $m = \dfrac{3x_1^2}{2y_1} = 7$

$3P$=2$P + P$=(4,0), since $m = \dfrac{y_2 - y_1}{x_2 - x_1}$=10

Similarly, $4P$=(0,1), $5P$=(5,3) and $6P = \infty$. Its graph is shown in figure 2.6.

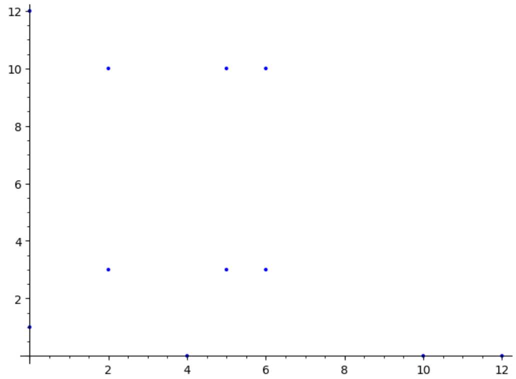

Figure-2.6: $y^2 = x^3 + 1$

Torsion Point : Let E be an elliptic curve defined over a field K. Consider a point on E and a positive integer n such that $nP = \infty$ but $mP \neq \infty$ for $m < n$. Then P is called a n-torsion point. Clearly, a point P is n-torsion if and only if order of P divides n. The set of all n-torsion points denoted by $E[n]$. Clearly, $E[n]$ is the subgroup of $E(K)$.

If we replace K by any finite field F_q, where $q = p^k$, $k \geq 1$. Then the number of elements in $E(Fq)$ is denoted by $\# E(Fq)$.

Theorem 2.8([7, **Theorem 3.2**]): Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0, then

$$E[n] \cong Z_n \oplus Z_n.$$

If the characteristic of K is p>0 and $p \mid n$, write $n = p^s n'$ with p does not divides n'. Then

$$E[n] \cong Z_{n'} \oplus Z_{n'} \text{ or } E[n] \cong Z_n \oplus Z_{n'}$$

Let K be a field of characteristic p. Then E is called ordinary if $E[p] \cong Z_p$. If $E[p] \cong 0$, then E is called **supersingular**. Also, **singular** and **supersingular** are totally different elliptic curves.

Example 2.9: Let E be the elliptic curve $y^2 = x^3 + x + 1$ over F_7. Now we want to find all points on E. Since F_7={0, 1, 2, 3, 4, 5, 6}.

First we pick x in F_7 and calculate $x^3 + x + 1$(mod 5), then its square root gives y. So the point (x, y) on E.

Table-2: Set of all points on the E

x	$x^3 + x + 1$	y	(x, y)
0	1		(0,1),(0,6)
1	3	--	--
2	4	2,5	(2,2),(2,5)
3	3	--	--
4	6	--	--
5	1	--	--
6	6	--	--
∞			∞

So, we see that , $\# E(F_7)$=5. But since $E(F_7)$ is a group, so $E(F_7) \cong Z_5$.

Theorem 2.10([7, **Theorem 4.1**]): Let E be an elliptic curve over the finite field F_q. Then

$E(F_q) \cong Z_n$ or $Z_{n_1} \oplus Z_{n_2}$

For some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

Hasse Theorem 2.11 ([**7, Theorem 4.2**]):

Let E be an elliptic curve over the finite field F_q. Then order of $E(F_q)$ satisfies

$$|\, q+1-\#E(F_q)\,| \leq 2\sqrt{q}$$

Hasse theorem gives the bound of the order of the group $E(F_q)$.

Let E be the curve $y^2 = x^3 + 7x + 1$ over F_{101}. Then by, Hasse theorem

$$|102-\#E(F_{101})| \leq 2\sqrt{101}$$

So, $102 - 2\sqrt{101} \leq \#E(F_{101}) \leq 102 + 2\sqrt{101}$. Therefore, the total number of element in the group $E(F_{101})$ bound between 82 and 122.

Theorem 2.11([7, **Theorem 4.14**]): Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over F_q. Then

$$\#E(F_q) = q + 1 + \sum_{x \in F_q} \left(\frac{x^3 + ax + b}{F_q} \right)$$

where

$$\left(\frac{x}{F_q} \right) = \begin{cases} +1, \text{ if } \ t^2 = x \text{ has a solution } t \in F_q^{\times} \\ -1, \text{ if } \ t^2 = x \text{ has no solution } t \in F_q \\ \ \ 0, \text{ if } \ x = 0. \end{cases}$$

Example 2.12: Let E be the curve $y^2 = x^3 + 2x + 1$ over F_7. Then

$$\#E(F_q) = q + 1 + \sum_{x \in F_q} \left(\frac{x^3 + ax + b}{F_q} \right)$$

$$\#E(F_7) = 7 + 1 + \sum_{x=0}^{6} \left(\frac{x^3 + 2x + 1}{F_7} \right)$$

$$= 8 + \left(\frac{1}{7}\right) + \left(\frac{4}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{3}{7}\right) + \left(\frac{3}{7}\right) + \left(\frac{5}{7}\right)$$

=8+1+1-1-1-1-1-1

=5

Therefore, $\#E(F_7)$=5.

In 1985, Schoof [4] developed a algorithm to calculate the total number of points on the E (Elliptic Curve) over the field F_q. It need at most c(constant) times $\log^8 q$ bit operation unlike baby step $q^{1/4}$.

If P in $E(F_q)$, then the order of P is the number k such that $kP = \infty$ but $k_1 P \neq \infty$, where $k_1 < k$. For example, if $P = (1,5) \in E(F_7)$, then $5P = \infty$. Let E be a elliptic curve over F_q, where $q = p^k$, where $k \geq 1$ and P in $E(F_q)$. How to calculate the order of P. **Baby Step, Giant Step**[7, **Section** 4.3.4] method is used to calculate the order of P. Now given the whole algorithm:

1. Compute $Q = (q+1)P$.

2. Select an integer such that $m > q^{1/4}$. Find and store the points jP for j = 0, 1, 2,… m,

Calculate the points $Q+k(2mP)$ for k =- m , -(m -1),…, m until got a match $Q+k(2mP)=\pm jP$ with a points stored element.

3. Then $MP=\infty$, where $M=q+1+2mk\mp j$.

4. Reduce M in factor. Suppose $p_1, p_2, \dots p_r$ be the prime factors of M .

5. Calculate $(M/p_i)P$ for all i =1,2,.. r . If $(M/p_i)P=\infty$ for some i, replace M by M/p_i and return to (5). If $(M/p_i)P\neq\infty$ for all i then M the is the order of the point P .

Example 2.13: Let E be an elliptic curve $y^2=x^3-10x+21$ over F_{557} and point P =(2,3) lie on E . Find the order of P . We apply **Baby Step, Giant Step** to calculate the order of P ,

1. $Q=558P$ = (418, 33).

2. Suppose $m=5$, where $m>557^{1/4}$. Now compute list of jP is

∞ , (2,3), (58,164), (44,294), (56,339), (132,364)

3. Compute $Q+k(2mP)$, where k =- m , -(m -1),.., m

k =-5, Q -50* P =(517,52)

k =-4, Q -40* P =(267,225)

.

.

k =1, Q +10* P = (2,3) = P

This implies j =1.

4. So M = 557+1+10-1 = 567 = 3^4.7. But 567 P = ∞. Compute (M /3) P =(189)* P = ∞ and 63* P =(38,535), 27* P =(136,360). So order of P is 189.

So using this method, order can be calculated of any points on E over F_q. But What about its converse part, that is if P and Q both lies on E and Q obtained by P . Then how to find k such that $Q=kP$. Now, this arise the Discrete Logarithmic Problem.

Application of the Elliptic Curve Cryptography (ECC) and the Discrete Logarithm Problem(DLP)

This section describe some good application of the Elliptic Curve Cryptography(ECC).

Diffie-Hellman Key Exchange [6, Section 16.5.2]

Suppose that Cathy and Dan want to share some information to each other such that no third person get a clue about their communication. For this, they want to exchange a key. For this, both agree on some point P on Elliptic Curve

$$E: y^2=x^3+ax+b(\text{mod}\, p) \qquad (4)$$

Suppose that they select p = 7211, a = 1 and P = (3,5). Using (1), we get b = 7206. Let Cathy and Dan randomly choose numbers A and B respectively. Assume that A = 12 and B = 23. They keep confidential the number A and B but publish AP and BP in public domain. Then

$$AP=(1794,6375) \text{ and } BP=(3861,1242)$$

After this Cathy send AP to Dan and Dan send BP to Cathy. Now Cathy multiply A to BP to get the key(k_1), that is

$A(BP)=(1472,2098)=k_1$ (say). Similarly, Dan multiply B to AP get the key (k_2), that is $B(AP)=(1472,2098)=k_2$ (say). We notice $k_1=k_2$, that is, both are getting the same secret key. So we see, using ECC Cathy and Dan share the key(same secret key) for the further communication.

Elliptic Curve Cryptography(ECC) Simulating ElGamal[1,**Section 10.5**]

In this method, first we construct the public and private (secret) key and then we apply Elgamal encryption scheme on the plaintext (secret message). Bob select, let

$$E: y^2 = x^3+ax+b$$

be any elliptic curve on F_p (finite field) , where p is any prime number.

Now, Bob select a point e_1 on E and a integer d. Now , he compute e_2=de_1=e_1+e_1+...+e_1 (d times). He make E, e_1 and e_1 public as a public key and he keeps d as his private key. Alice select a plain text message m and convert its a point P on E. She calculate C_1=re_1 and C_2 = $P+re_2$. Bob receive a pair (C_1,C_2), after obtaining this pair, he calculate P_1 by the given formula:

$$P_1 = C_2 - d\ C_1$$

$$= P + re_2 - d(re_1)$$

$$= P$$

Bob obtain the P, after this he obtain the m.

Factoring with Elliptic Curves [**6, Section 16.3**]

Let us consider a number n, where $n=pq$, p and q both are prime numbers. Now , we wish to factor n in terms of p and q. First , we choose any arbitrary elliptic curve on mod n . Now, the question how we choose the elliptic curve. In this problem, first we choose a point P and a coefficient a. Now using the elliptic curve,

$$E: y^2 = x^3+ax+b(\text{mod}\,n) \qquad (5)$$

Find the value of b by assuming P lies over the curve E. This is more convenient than to choose a and b and then find P. For more clear explanation, we take a example, let n=2773. Now we want to factorize n. Take P =(1,3) and a =4. Clearly, we get b =4. So the required Elliptic curve is

$$E: y^2=x^3+4x+4$$

Since P = (1,3). We see that $2P$ = (1771,705), because P = (x,y) (say). Then, x =1, and y =3. we know from the elliptic curve theory

$$2P = P+P = (m^2-2x, m(x-m^2+x)-y) \quad ,$$

where $m=\dfrac{3x^2+4}{2y}$

So m=7/6, but gcd(6,2773) = 1 and 6^{-1}(mod 2773) = 2311. Thus, $2P$ = (1771,705). Similarly,

$$3P = 2P+P = (x_1,y_1)+(x,y)$$

$$=(\quad m^2-x-x_1 \quad , \quad m(x_1-m^2+x_1+x)-y_1),\ m=\frac{y_1-y}{x_1-x}.$$

Then m =702/1770, but gcd(1770,2773) = 59, so we can not find 1770^{-1}(mod 2773). But our main purpose is to find the factors of 2773, and we have gcd(1770,2773) = 59. That is , we have calculate the factor 59, which implies 2773 = 59*47.

We regarded E as a pair of two elliptic curves on mod 59 and mod 47. Since P = (1,3). Clearly, $3P = \infty$ (mod 59) and $4P = \infty$ (mod 47). Hence when tried to compute $3P$ and $4P$, we see slope is infinite on mod 59 and finite on mod 47. So now taking gcd we get the factor 59.

If $n = pq$, then we can not separate p and q as long as behave identically. But if you can find some thing that makes them behave slightly differently, then these number can be calculated. In earlier example we see the multiple of P reached ∞ faster than mod 47. Since in general the primes p and q should act. Fairly independently of each other , one would expect that for most curves E (mod pq) and points P , the multiples of P would reach ∞ mod p and mod q at differently times. This will cause the gcd to find either p and q.

Elliptic curve cryptography is also being used to generate Pseudorandom number generation (PRNG)[**5, Section 10.5**] and ElGamal Digital Signatures[**6, Section 16.5.3**].

In 2020, Utku Gulen and Seluck Baktir [**9**] used elliptic curve cryptography(ECC) on the MSP430 microcontroller, which is used in WSNs (Wireless Sensor Networks).

The Discrete Logarithm Problem(DLP)-

Supppose that p is a prime. Let a, b be two integers that are non-zero under mod p. The numbers a and b related as $a^k = b$. To find k is the simple example of Discrete Logarithm Problem.

Let G be a group(Abstract Algebra) with multiplicative operation and let a, b in G. Consider $a^k = b$, the discrete logarithm problem to find k.

We know that $E(F_q)$ is a group and P, Q be two points on curve and we are trying to find *k*, such that $kP = Q$.

The Elliptic Curve Cryptography scheme's security is depend on the complexity to solve Discrete Logarithm Problem(DLP). Since there are many scheme, like Index calculus Algorithm, Baby step Giant step Algorithm, Pollards Rho Algorithm and Pohling Hellman Algorithm, using this we can attack on the Discrete Logarithm Problem(DLP). See the following table [**3**].

Table-3: Attacks and Expected time

Attacks	Expected Time
Baby Step Giant step Method	O($\sqrt{n}$)
Pollard Method	O($\sqrt{\frac{n\pi}{2}}$)
Index Calculus Method	$L_q[\frac{1}{2}, C]$
Pohling Hellman Method	O($\sqrt{n}$)

The cryptographic strength of elliptic Curve encryption depends on the how difficult to solve solution of the discrete logarithmic problem for a cryptanalyst to calculate the value of random number k from kP and P.

References

1. A. Forouzan, Behrouz(2007). *Cryprography and Network Security*, Special Indian Edition. Tata

McGraw-Hill.

2. Patil, Sneha & Devmane, Vidyullata(2018). A review on Elliptic Curve Cryptography and variant. *International Research Journal of Engineering and Technology(IRJET), 05(05), 3065-3068.*

3. Pote, Santoshi & Katti, Jayashree(2015). Attacks on Elliptic Curve Cryptography Discrete Logarithm Problem(EC-DLP). *International Journal of innovative Research in Electrical, Electronics, Instrumentation and Control Engineering,* DOI 10.17148/IJIREEICE.2015.3428.

4. Schoof, R. Elliptic curves over finite fields and the computation of square root mod *p. Math.Comp., 44(170): 483-494,1985. 0*

5. Stalling, William(2014). *Cryptography and Network Security: Principle and Practice, Sixth Edition.* Pearson Press.

6. Trappe, Wade & C.Washington, Lawrence(2006). *Introduction to Cryptography with Coding Theory*. Pearon Educational International.

7. C. Washington, Lawrence(2008). *Elliptic Curves Number Theory and Cryptography*. University of Maryland (USA); Chapman & Hall/CRC.

8. Menezes, Alfred(1993). *Elliptic Curve Public Key Cryptosystems;* Auburn University. Springer Science+Business Media, LLC.

9. Gulen, Uktu & Baktir, Seluck(2020). *Article* Elliptic curve Cryptography for Wireless Using the Number Theoretic Transform. *Sensor* ***2020****, 20, 1507;* doi:10.3390/s20051507.