A STUDY ON CRYPTOGRAPHY AND ELLIPTIC CURVE CRYPTOGRAPHY

JIGNASA- A Student Study Project

Subject: Mathematics

Government Degree College,

Rangasaipet, Warangal

Warangal – District

Submitted by:

T. Rohith Chand, BSc. (MPCs), III year

G. Shailaja, BSc. (MPC), III year

K. Srilekha, BSc. (MPC), III year

Ruheena, BSc. (MPCs), II year

P. Vigneshwari, BSc. (MPCs), II year

Under the supervision of:

Smt. R. Rudrani,
Asst. Prof of Mathematics,
Government Degree College,
Rangasaipet, Warangal,

DECLARATION

We do hereby declare that the work presented in this study project is an original one and has been carried out by us in the Department of Mathematics, GOVERNMENT DEGREE COLLEGE, RANGASAIPET, WARANGAL and has not been submitted either in part or in full for the award of any Degree or Diploma of any University earlier.

Date:

PLACE:

DEPARTMENT OF MATHEMATICS
GOVERNMENT DEGREE COLLEGE, RANGASAIPET
DISTRICT:WARANGAL

CERTIFICATE

This is to certify that the **JIGNASA-Students Study Project** is an original one and has been carried out by the students of **GOVERNMENT DEGREE COLLEGE, RANGASAIPET, DISTRICT: WARANGAL** It was carried out under my supervision. It is a bonafide work done by them and has not been submitted elsewhere for the award of any Degree or Diploma. This study project is of the standard expected and I strongly recommend that it may be sent for evaluation.

Date: R.RUDRANI

Place: **Study Project Supervisor**

CONTENTS

1. Aims and objectives **5**

2. Methodology **5**

3. Analysis of Data **5**

4. Findings **21**

5. Suggestions **27**

6. Conclusion **28**

7. References **31**

1. AIMS AND OBJECTIVES:

- To learn and understand the concepts of cryptography and elliptic curve cryptography also to present an overview of elliptical curve cryptography.
- To focus on the importance and advantages of elliptic curve cryptography (ECC) over other public-key cryptosystems.
- To deal with the working of ECC by using the arithmetic of elliptic curves.
- To find reasons why ECC is a powerful cryptographic approach and discover the role and need of ECC in today’s world.

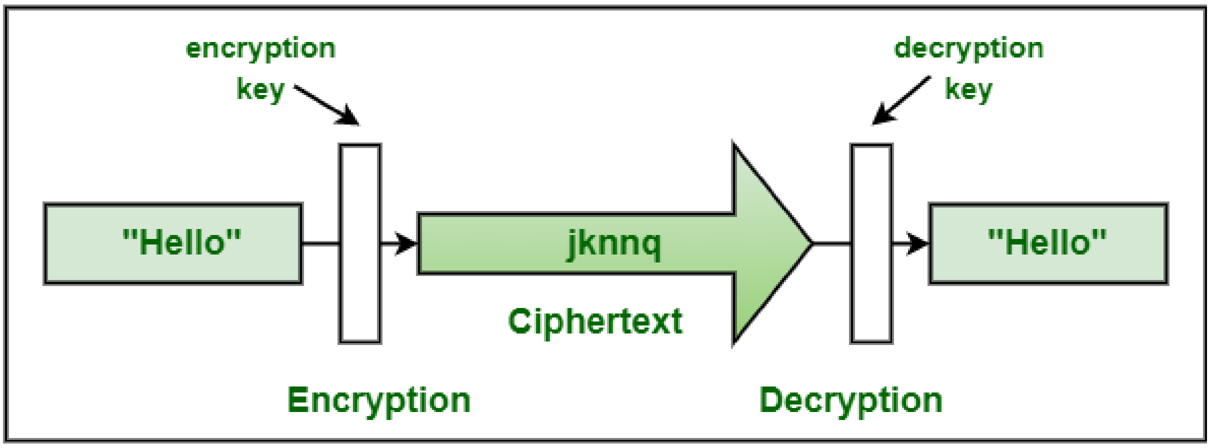
2. METHODOLOGY:

We have gathered information from various Open Educational Resources and referred few books related to cryptography, like Cryptography and Network Security by William Stallings. Researched the concepts of Elliptic Curve Cryptography, and understood that there are various things to be encountered before gaining knowledge on ECC and all the data that has been analyzed and presented in this project.

3. ANALYSIS OF DATA:

Cryptography is the science of using mathematics to hide data behind encryption. It involves storing secret information with a key that people must have in order to access the raw data. Cryptography has been in practice for thousands of years where ability to send messages in secret has been influential throughout the history. There is another influence in history which is cryptanalysis, the technique of uncovering encrypted messages without knowing the decryption key.

Cryptography is always changing, However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext the original message which is encrypted into ciphertext, a process called encryption, then back again known as decryption.



one key element of this change is the inclusion and progression of mathematics. From simpler arithmetic such as addition and multiplication to the use of more advanced techniques such as matrix operations, modular arithmetic, and discrete logarithms, a wide variety of mathematics is incorporated into cryptography. For instance, A specific field of mathematics that is essential to cryptography is number theory. While various ciphers use number theory like Public key ciphers are essential in modern-day security for the internet and credit card transactions.

There are many different ciphers, In this project we will primarily discussing on shift ciphers

3.1 Overview of terms encryption and decryption through the shift ciphers:

3.1.1 Introduction:

One of the earliest substitution ciphers was the Caesar shift cipher, used by Julius Caesar. Caesar would replace the original letters of the message with the letters that are three letters down in the alphabet.

A description of how the cipher works follows: Suppose the plaintext “Math” is to be encrypted using the Caesar cipher. Following table gives the corresponding ciphertext alphabet.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	N	o	p	q	r	s	t	u	v	w	x	y	z
Cipher text	d	e	f	g	h	i	j	k	l	m	n	o	p	Q	r	s	t	u	v	w	x	y	z	a	b	c

Note that M is mapped to p; A is mapped to d; T is mapped to w and H is mapped to k. Thus, "Math" is encrypted to pdwk

3.1.2 Encryption:

The shift cipher is a special type of monoalphabetic substitution cipher, in which a single cipher alphabet is used throughout the entire encryption process. In shift ciphers, the number that each letter of the plaintext is shifted by is called the key, which we will refer to as k. In the Caesar cipher the key, k, is 3. In shift ciphers each plaintext letter corresponds to a number as follows:

a	b	c	d	e	f	g	h	i	J	k	l	m	n	o	p	q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

r	s	t	u	v	w	x	y	z
17	18	19	20	21	22	23	24	25

Let m denote the numerical value of the plaintext letter, and c denote the numerical value of the ciphertext letter. The plaintext is converted letter by letter to the ciphertext, c, by the following encryption function:

$c \equiv m + k(mod\ 26),$ where $k \in Z_{26}$

For example, the encryption algorithm for a Caesar cipher is c ≡ m + 3 (mod 26), and we encrypt "math" as follows:

plaintext	M	A	T	H
m	12	0	19	7
$c \equiv m + k(mod\ 26)$	$12 + 3 \equiv 15$	$0 + 3 \equiv 3$	$19 + 3 \equiv 22$	$7 + 3 \equiv 10$
ciphertext	p	d	w	k

Thus the ciphertext pdwk is achieved.

3.1.3 Decryption:

In a shift cipher, the decryption function is determined by solving the encryption function for m in terms of c; that is, $m \equiv c - k \equiv c + (26 - k)\ (mod\ 26)$, where the decryption key is $d = 26 - k \in Z_{26.}$ Given the ciphertext from the previous example, the first step of decryption is to convert the ciphertext to its numerical value, c, Then the function

$m \equiv c - k \equiv c + (26 - k)\ \ (mod\ 26)$, is used to obtain the plaintext as shown in the table below.

ciphertext	p	d	w	k
c	15	3	22	10
$m \equiv c - k(mod\ 26)$	$15 - 3 \equiv 12$	$3 - 3 \equiv 0$	$22 - 19 \equiv 3$	$10 - 3 \equiv 7$
plaintext	M	A	T	H

The problem with the security of the cipher is that it can be solved by either frequency analysis or a brute force attack. Frequency analysis is using the frequency that each ciphertext letter appears and comparing that to the frequency that English letters are used in words and sentences. The most common letters, in order, are E, T, A, O, I, N, and S. A frequency table for all letters can be found in. A brute force attack is trying all different 25 keys until the correct one is found. This was time-consuming in the time period of Julius Caesar, but with technology now, it can be accomplished in seconds.

3.2 Evolution of Cryptography:

A human being from ages had two inherent needs that are to communicate and to share information and most importantly to communicate selectively. These two needs gave rise to the art of coding the messages such that only intended people could have access to information and no other unauthorized people could extract any information, even if the scrambled messages fell in their hands.

The evolution of cryptography and the roots of the existence of cryptography were found in Roman and Egyptian civilizations and the first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyphs. This followed code was one of the secrets known only to the scribes who used to transmit messages on behalf of the kings.

Cryptography has been in practice for thousands of years, and many different ciphers and cryptosystems have been used throughout history. Present technology’s continual advancements will eventually make these cryptosystems insecure and obsolete. This is why the exploration of the history, evolution, and mathematical concepts behind cryptography is so important. More research needs to be done to further the security and evolution of these cryptosystems in order to protect the welfare of what the cryptosystems are protecting.

We have made incremental improvements over the years yet, Cryptography did not gain a public face until the World Wide Web was invented in 1989, The World Wide Web is an electronic protocol that allows people to communicate mail, information, and commerce through a digital medium. This new method of information exchange has caused a tremendous need for information security. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient.

At the end of World War I, Arthur Scherbius invented the Enigma, an electro-mechanical machine that was used for encryption and decryption of secret messages. The Enigma had several rotors and gear that allowed up to 10^{114} possible configurations. Because of the numerous configurations, the Enigma was virtually unbreakable with brute force methods. The first commercially available versions were available in the 1920's.

The Enigma machine was a mechanical tool used by the Germans in World War II to scramble messages and prevent the enemy from understanding them. Enigma was based on revolving wheels, or rotors, that were wired together and connected to a typewriter keyboard.

Every time a user presses a key, an electrical current would run through the rotors connecting the key to the light. Then the rotor would rotate into a new position if a user could press the same key over, and over again, and each time would create a different connection to a new light. This was a brilliant scheme that took several governments and millions of man-hours for several years to solve. With the evolution taking place, several government organizations, and even military units have used cryptography to guard their secrets against others. Speaking of now, the arrival of computers and the Internet has brought effective cryptography within the reach of common people.

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.

3.3 Modern Cryptography and its objectives:

Nowadays, the networks have gone global and information has taken the digital form of bits and bytes. Critical information now gets stored, processed, and transmitted in digital form on computer systems and open communication channels. Since information plays such a vital role, adversaries are targeting the computer systems and open communication channels to either steal sensitive information or disrupt the critical information system. Modern cryptography provides a robust set of techniques to ensure that the mean intentions of the adversary are disillusioned while ensuring the legitimate users get access to information.

Cryptography is ultimately used to secure important data on the hard disk or any medium where it concerns itself with the following four objectives:

1. **Confidentiality:** The information cannot be understood by anyone for whom it was unintended thereby ensuring that no one can read the message except the intended receiver.
2. **Integrity:** Assuring the received message has not been altered in any way from the original one.
3. **Authentication:** Where the sender and receiver can confirm each other's identity and the origin/destination of the information.
4. **Non-repudiation:** A mechanism to prove that the sender sent the message.

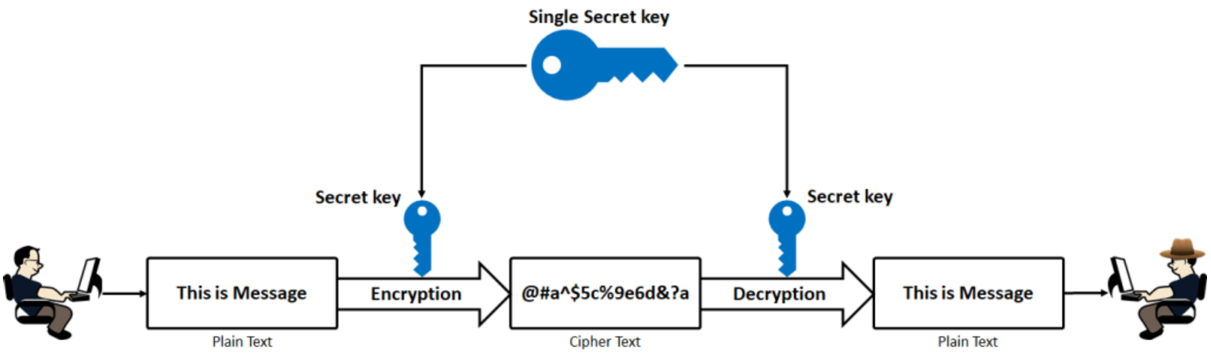
3.4 Types of Cryptography:

Based on the key encryption algorithm, cryptography is primarily classified as:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

3.4.1 Symmetric Key Cryptography:

Symmetric key cryptography is also called Private key Cryptography. In this approach, both the sender and receiver will share a single, common key that is used to encrypt and decrypt the message.



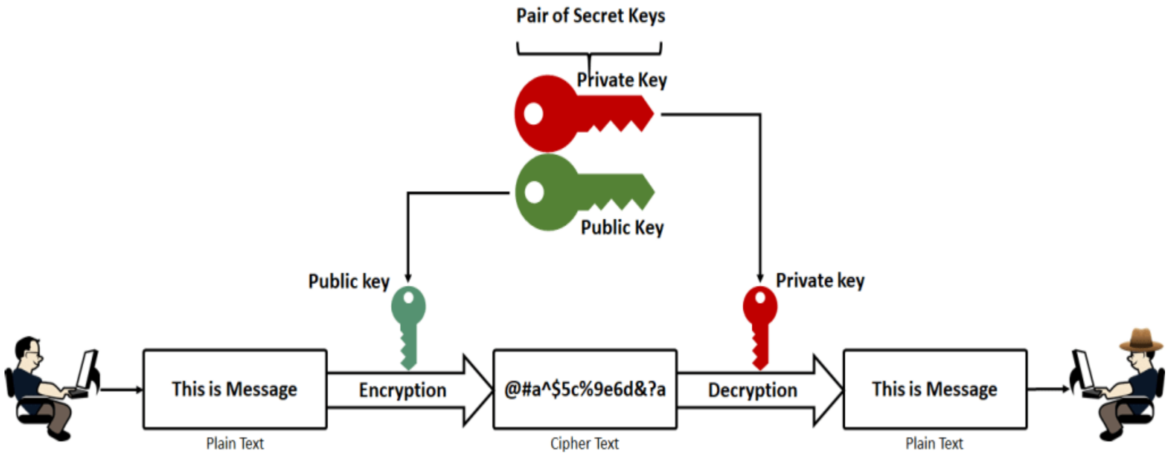
In Symmetric Key Cryptography Sender will encrypt the data with a secret key. Then the receiver will use the same key to decrypt the received data.

AES (AES stands for Advanced Encryption Standard, DES(DES stands for Data Encryption Standard), RC4, RC5, and RC6 (RC stands for Rivest Cipher)are some examples of symmetric key Cryptography.

Here in the case of Symmetric-key systems, they are simpler and faster but the main drawback is that the two parties must somehow exchange the key securely and keep it secure after that.

3.4.2 Asymmetric Key Cryptography:

Asymmetric Key Cryptography is called Public-key cryptography. In this approach, the Receiver will use Private Key to Decrypt and Sender will use Public Key Encrypt.



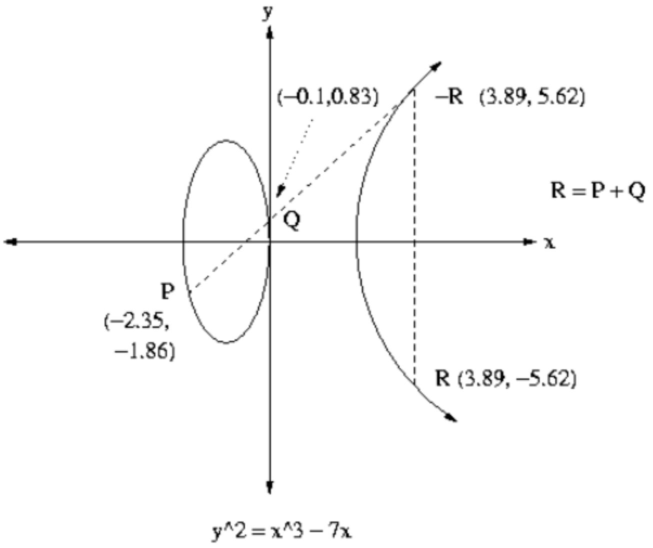
In Asymmetric Key Cryptography Sender will encrypt the data with a public key. Then the receiver will use the private key to decrypt the received data. Some most used Asymmetric Key Cryptography is Elliptic curve techniques, RSA and DSA.

3.4.3 Public Key and Private key Comparison

	Private Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Key distribution	Must be out-of-bond	The public key can be used to distribute other keys
Speed	Fast	Slowness of execution
Secure	Access can be gained through software-based attacks	Digital signature authentication and increased security

3.5 Elliptic Curve Cryptography, its Algebra and Geometry:

Elliptic Curve Cryptography (ECC) has technically already been invented but is considered to be a future technique of cryptography because its advantages and disadvantages are not yet fully understood. ECC is an approach to encryption that utilizes the complex nature of elliptic curves in finite fields. ECC typically uses the same types of algorithms like that of Diffie-Hellman Key Exchange and RSA Encryption. The difference is that the numbers used are chosen from a finite field defined within an elliptic curve expression.



The above figure shows an example of an elliptic curve. This example could be used in conjunction with an RSA type algorithm in which two primes, "P" and "Q", are chosen. When the primes are chosen using a predefined elliptic curve in a finite field, the key sizes can be much smaller and still yield the same amount of security. This allows the time it takes to perform the encryption and decryption to be drastically reduced, thus allowing a higher amount of data to be passed with equal security. Just as other methods of encryption have, ECC must also be tested and proven secure before it gets accepted for commercial, governmental, and private use.

3.5.1 What is an Elliptic Curve?

Elliptic curves appear in many diverse areas of mathematics, ranging from number theory to complex analysis, and from cryptography to mathematical physics.

Elliptic curves as algebraic/geometric entities have been studied extensively for the past 150 years, and from these studies has emerged a rich and deep theory. Elliptic Curve Cryptography (ECC) is a public key cryptosystem just like RSA, where every user has a public key and a private key.

Elliptic Curves are just another way to map the data into another form. The power of the scheme comes from the fact that it is very hard to do the unmapping without the knowledge of the key. Elliptic curves are used as an extension to other current cryptosystems like Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.

An elliptic curve is a smooth, projective, algebraic curve on which there is a specified point $\mathcal{O}$. An elliptic curve is defined over a field *K* and describes points in K^2, the Cartesian product of *K* with itself. If the field's characteristic is different from 2 and 3, then the curve can be described as a plane algebraic curve which, after a linear change of variables, consists of solutions (*x*,*y*) for:

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

for some coefficients *A* and B in *K*.

The curve is required to be non-singular, which means that the curve has no cusps or self-intersections. (This is equivalent to the condition the discriminate is non zero that is, being square-free in *x*.)

It is always understood that the curve is sitting in the projective plane, with the point $\mathcal{O}$ being the unique point at infinity.

An elliptic curve is an abelian variety – that is, it has a group law defined algebraically, with respect to which it is an abelian group – and $\mathcal{O}$ serves as the identity element.

The group law is constructed geometrically also.

3.5.2 Points on Elliptic Curves

Elliptic curves can have points with coordinates in any field, such as Fp, Q, R, or C.

Elliptic curves with points in Fp are finite abelian groups.

An Elliptic Curve is a curve given by an equation of the form

$\boldsymbol{y^2 = x^3 + Ax + B}$

There is also a requirement that the discriminate

$\boldsymbol{\Delta = 4A^3 + 27B^2\ is\ nonzero}$

$\boldsymbol{E = \{(x, y): y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}}$

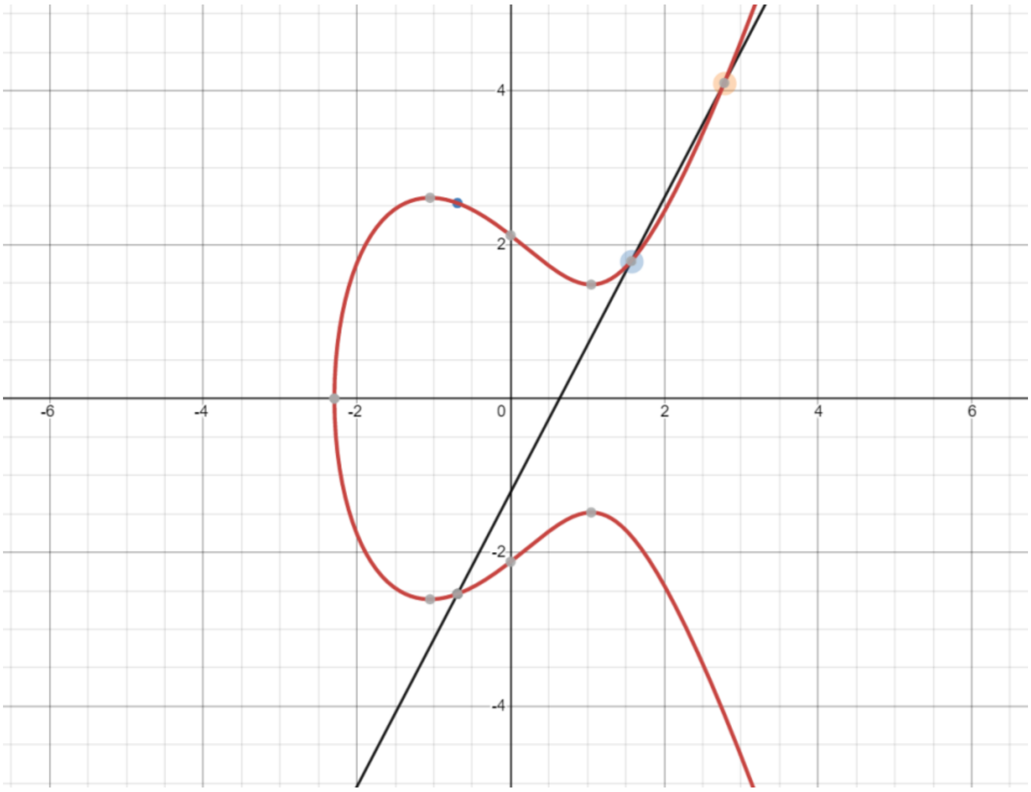
Where x, y, A, and B are field elements.

Each choice of the numbers A and B yields a different elliptic curve.

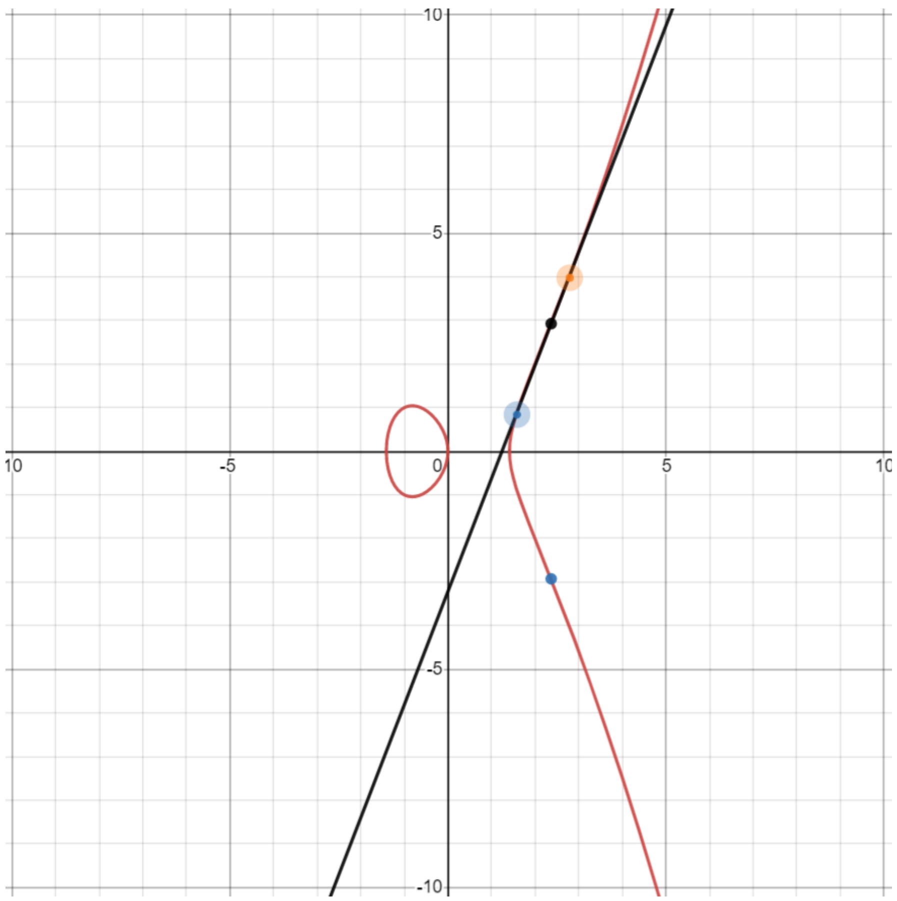
For example, A = -3.3 and B = 4.5 give the elliptic curve with equation

$$\boldsymbol{y^2 = x^3 - 3.3x + 4.5}$$

The graph of this curve is shown below:



Some Other Example:$\boldsymbol{y^2 = x^3 - 2x}$



3.5.3 The Algebra of Elliptic Curves:

Addition algorithm for $P_1 = (x_1, y_1)$and $P_2 = (x_2, y_2)$

on the elliptic curve

$\mathbf{E : \ y^2 = x^3 + Ax + B}$

- **If** $\boldsymbol{P_1 \neq P_2}$ **and** $\boldsymbol{x_1 = x_2}$**, then** $\boldsymbol{P_1 + P_2 \ = \mathcal{O}}$

- **If** $\boldsymbol{P_1 = P_2}$ **and** $\boldsymbol{y_1 = 0}$**, then** $\boldsymbol{P_1 + P_2 \ = 2P_1 = \mathcal{O}}$

- **If** $\boldsymbol{P_1 \neq P_2}$ **and** $\boldsymbol{(x_1 \neq x_2)}$,

$$\mathbf{let}\ \boldsymbol{\lambda = \frac{y_2 - y_1}{x_2 - x_1}}\ \boldsymbol{and\ v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}}$$

- **If $P_1 = P_2$ and $(y_1 \neq 0)$,**

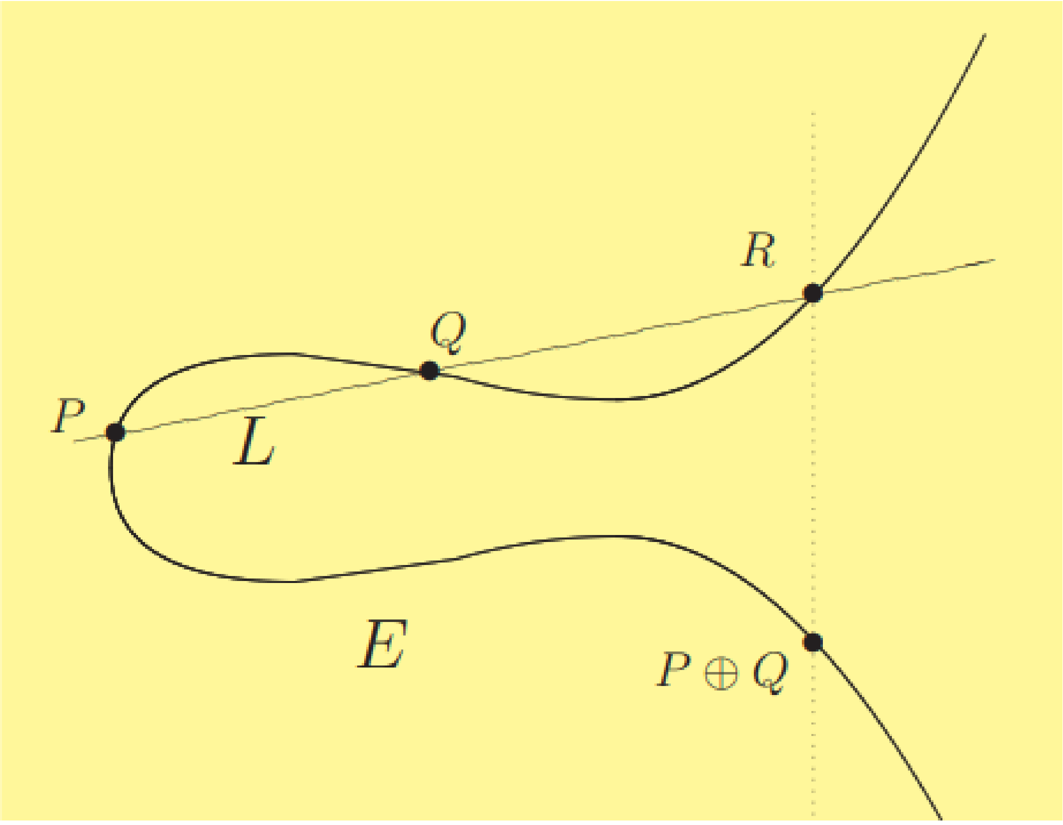
$$\text{let } \lambda = \frac{3x_1^{\,2} + A}{2y_1} \textit{ and } v = \frac{-x_1^{\,3} + Ax_2 + 2B}{2y_1}$$

Then

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - v)$$

3.5.4 The Geometry of Elliptic Curves:

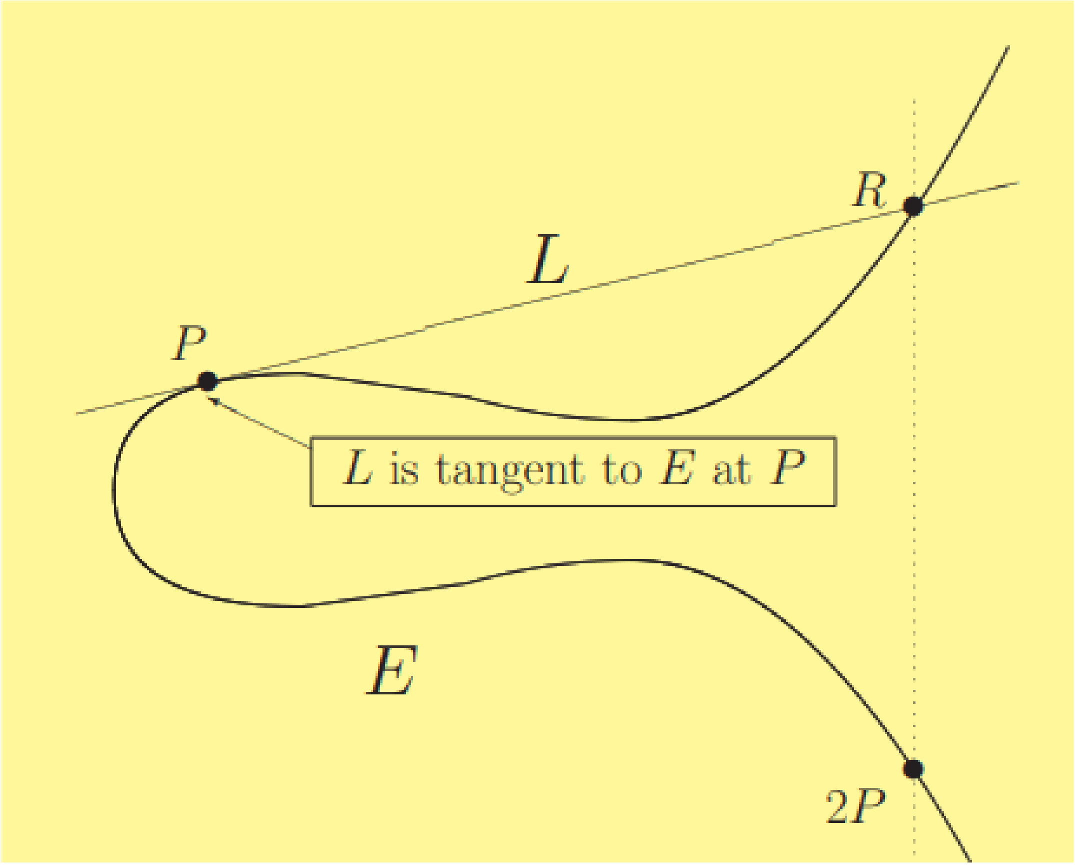
Case 1: Adding 2 Points on an Elliptic Curve



If P and Q are two points on the curve, then we can uniquely describe a third point, P + Q, in the following way. First, draw the line that intersects P and Q.

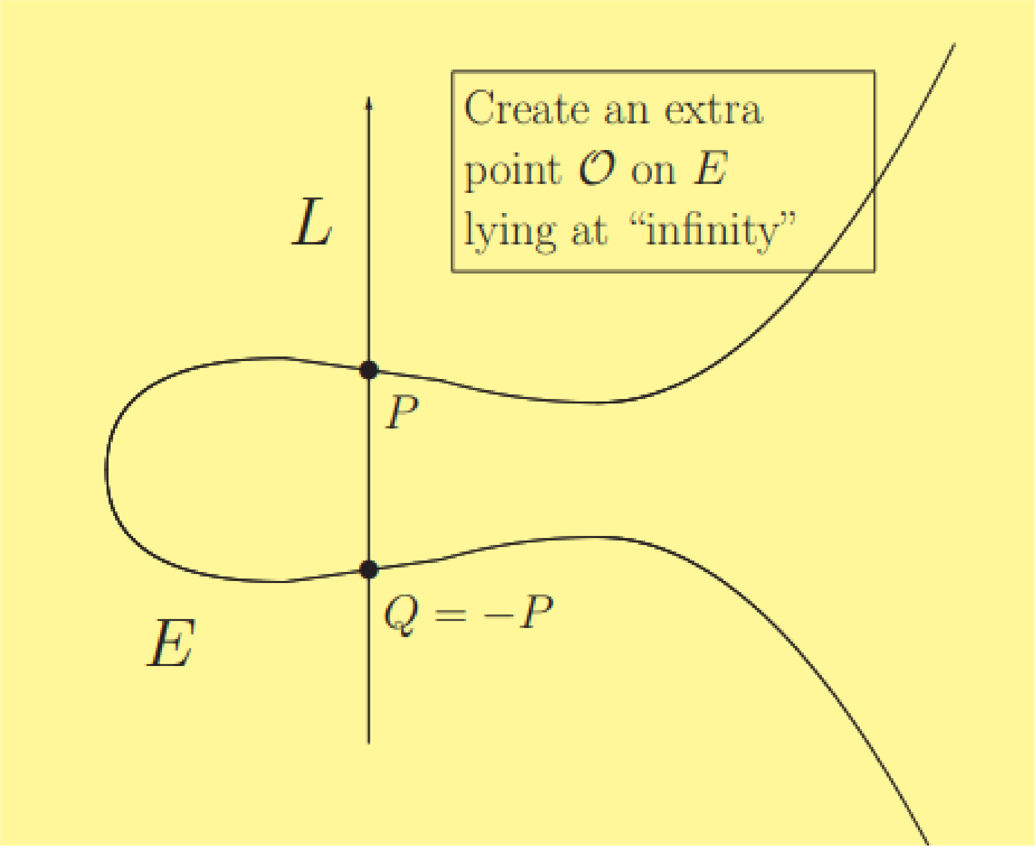
This will generally intersect the cubic at a third point, R. We then take P + Q to be −R, the point opposite R.

Case 2: Adding a point to itself on an Elliptic Curve



If P = Q we only have one point, thus we can't define the line between them. In this case, we use the tangent line to the curve at this point as our line.

Case 3: Vertical line and an extra point "At Infinity"


Create an extra point $\mathcal{O}$ on E lying at "infinity"
L
P
$Q = -P$
E

if P and Q are opposites of each other, we define P + Q = $\mathcal{O}$

3.5.5 Finding Integer Points on the Curve:

To use these curves in cryptography, we have to limit their range; after all, it simply isn't practical to have numbers near infinity on a 16/32/64-bit microcontroller. So the vertical and horizontal range is capped at a very large prime number, p. The modulus operator is used to keep the results within that range. Then, all integer solutions to the equation that describes the curve are found.

Let's look at the points on the curve $y^2 = x^3 + x + 6\ (mod\ 11)$

x	$x^3 + x + 6$ (mod 11)	y	y^2(mod 11)
0	$0^3 + 0 + 6 = 6$	0	0
1	$1^3 + 1 + 6 = 8$	1	1
2	$2^3 + 2 + 6 = 5$	2	4
3	$3^3 + 3 + 6 = 3$	3	9
4	$4^3 + 4 + 6 = 8$	4	5
5	$5^3 + 5 + 6 = 4$	5	3
6	$6^3 + 6 + 6 = 8$	6	3
7	$7^2 + 7 + 6 = 4$	7	5
8	$8^2 + 8 + 6 = 9$	8	9
9	$9^2 + 9 + 6 = 7$	9	4
10	$10^2 + 10 + 6 = 4$	10	1

$E_{11}(1,6)$ consists of the following points {(2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9), $\mathcal{O}$ }

Likewise in this example, we have used the prime number 37 and the equation will be as follows

The Curve $E: y^2 = x^3 - 5x + 8\ (mod\ 37)$

E (F37) consists of the following 45 points modulo 37

$\{\ (1, \pm 2), (5, \pm 21), (6, \pm 3), (8, \pm 6), (9 \pm 27), (10, \pm 25), (11, \pm 27),$

$(12, \pm 23), (16, \pm 19), (17 \pm 27), (19 \pm 1), (20, \pm 8), (21 \pm 5), (22, \pm 1),$

$(26, \pm 8), (28 \pm 8), (30, \pm 25), (31, \pm 9), (33, \pm 1), (34, \pm 25), (36, \pm 26), \mathcal{O}\ \}$

4. FINDINGS:

4.1 The idea behind Asymmetric Cryptography

Whitefield Diffie and Martin Hellman published a paper named “New Directions in Cryptography” back in 1976 which introduced the idea of public-key cryptography for this very fundamental contribution indeed the modern secure internet as we know it would not have been possible without the idea of public-key cryptography. At that time cryptographic algorithms had a problem with key transportation where the secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Whereas every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

This problem is addressed by introducing two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called the public key, and the decryption key is kept secret and called the private key. The keys are generated in such a way that it is impossible to derive the private key from the public key. The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, there is no need for exchanging keys, thus eliminating the key distribution problem and increasing security too

Asymmetric key cryptosystems / public-key cryptosystems include RSA, elliptic curve cryptography (ECC), Diffie-Hellman, ElGamal, McEliece, NTRU and others) use a pair of mathematically linked keys: a public key (encryption key) and a private key (decryption key).

The RSA public-key cryptosystem is based on the mathematical concept of modular exponentiation (numbers raised to a power by modulus), along with some mathematical constructions and the integer factorization problem (which is considered to be computationally infeasible for large enough keys).

Modular Arithmetic

$$p \bmod m = n \text{ or } \mathrm{mod}(p,m) = n$$

The modulus operator determines the remainder left after the division, the modular arithmetic performed on a no say ‘p’ involves arithmetic in the range from 0 to p-1. If in any operation the number falls out of this range then the result is wrapped around to fall in the range 0 to p-1. And for that mod operator is used.

Exponentiation is the process of multiplying a number by itself a given number of times. The products of exponentiation become large quickly (2^64=18,446,744,073,709,551,616) which can consume available memory quickly. Fortunately, the process can be broken up into small problems that better fit into the memory of a microprocessor. The modulus operator takes care of overruns.

2^64=2^16•2^16•2^16•2^16

Diffie & Hellman realized that it was possible to combine the ideas of modular arithmetic and exponentiation to create a shared secret on two different systems. Both the sender and receiver participate in generating the secret and sharing public data freely.

4.2 Working of Elliptic Curve Cryptography

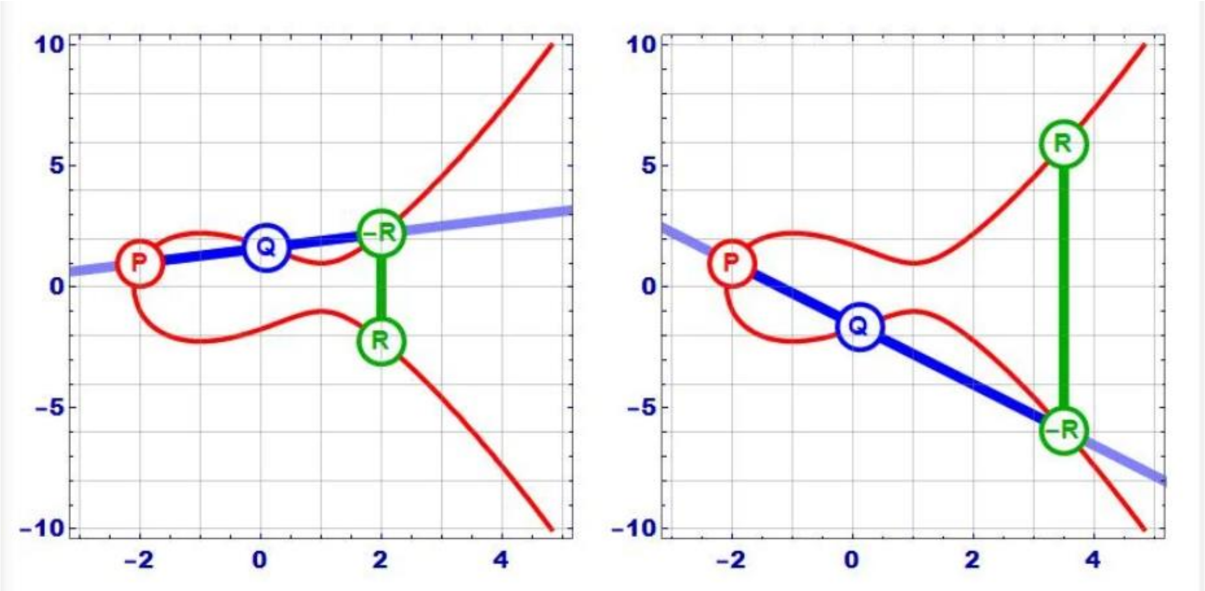
For instance; let’s consider Alice and Bob two parties who need to exchange the secret key

1. Both Alice and Bob agree upon starting point P point on the elliptic curve publicly defined $y^2 = x^3 + Ax + B$
2. Alice selects his private key ‘α’ and computes αP shares this with bob
3. Bob selects his private key ‘β’ and computes βP shares with Alice
4. Alice receives βP and computes βPα by multiplying with his private key
5. Bob receives αP and computes αPβ by multiplying with his private key
6. It is obvious that $\beta P\alpha = \alpha P\beta$
   hence both Alice and Bob have the same key which serves as the private key for further encryption and decryption.

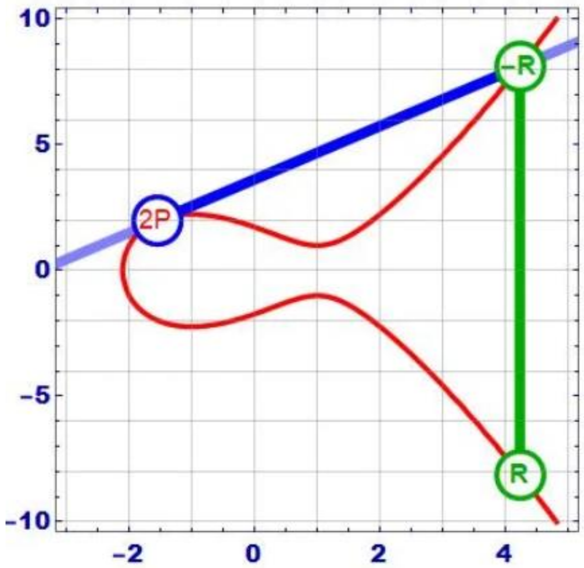
The reason that we use elliptic curves for the key exchange is that they allow longer keys to be generated with fewer bits of data exchanged between computers. This method of cryptography was discovered independently by Neal Koblitz and Victor S. Miller.

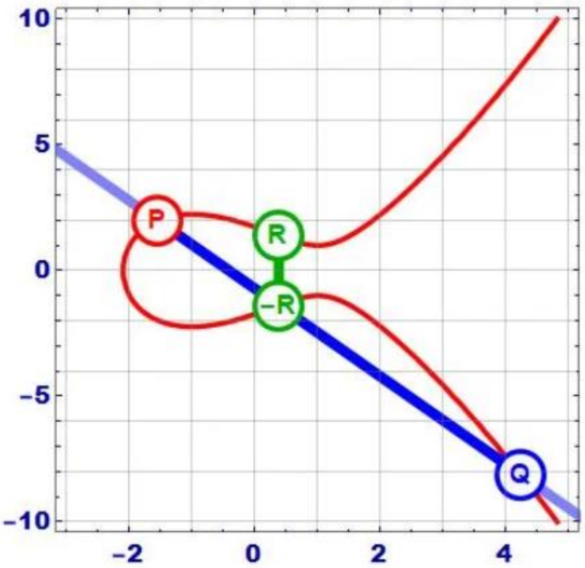
Elliptic curves have a few necessary peculiarities when it comes to addition. Two points on the curve (P, Q) will intercept the curve at a third point on the curve. When that point is reflected across the horizontal axis, it becomes the point (R). So $P \oplus Q = R$.

***Note:** The character ⊕ is used as a mathematical point addition operator, not the binary **XOR** operator.



The line that connects P and Q intersects the curve at a third point, and when that point is reflected across the horizontal axis, it becomes the point R. This reflection is necessary for the times where P and Q are at the same point on the curve (P=Q). In those cases, the generated line is tangent to the curve by definition. Without the reflection, it would not be possible to add P to itself multiple times, since P⊕P (2P) would generate the same point as $P \oplus P \oplus P\ (3P, 4P, nP)$, etc...





A point that is added to itself (2P) generates a tangent line that intercepts the curve at a new point that when reflected across the horizontal access becomes the point R.

Two points (P, Q) that lie on the curve will intercept the curve in a third point, that when reflected across the horizontal access becomes point R

This, of course, wouldn’t be an ideal mathematical condition. By reflecting below the line, P⊕P=R, and the point P⊕R=P⊕P⊕P=3P ends up generating a new point (-S) somewhere else on the curve. That new point, when added to P, then generates a new point, and so on. Without the reflection, none of this would happen.

The following graphic shows the result of successive addition of P to itself ($P \oplus P, P \oplus 2P, P \oplus 3P, P \oplus 4P,$ etc…).

The curve and original point P is a shared value everybody knows and agreed to use, the final point nP is your public key, safe to share with anyone. How many steps do you jump will be the value n is your private key.

The idea behind all of this is that one point on the curve added to itself multiple times will generate other points on the curve. Any two points can be used to identify a third point on the curve. An exception is provided for when P(x,y=0), and the tangent line goes to infinity.

4.3 Importance and Security aspects of ECC

The most important and most used public-key cryptosystems are RSA and ECC. Elliptic curve cryptography (ECC) is the recommended and most preferable modern public-key cryptosystem, especially with the modern highly optimized and secure curves (like Curve25519 and Curve448), because of smaller keys, shorter signatures and better performance.

- Smaller keys, ciphertexts and signatures.
- Very fast key generation.
- Fast signatures.
- Moderately fast encryption and decryption.
- Signatures can be computed in two stages, allowing latency much lower than inverse throughput.
- Good protocols for authenticated key exchange
- Special curves with bilinear pairings allow new-fangled crypto.
- Binary curves are fast in hardware.

These are the advantages of ECC.

Though it has disadvantages like having

- Complicated and tricky to implement and particularly the standard curves.
- Signing with a broken random number generator compromises the key.
- Still has some patent problems, especially for binary curves.
- Newer algorithms could theoretically have unknown weaknesses.

4.3.1 Security Aspects:

- Attacks on the group of elliptic curves are weaker than available factoring algorithms attacks
- The complexity of these methods is approximately $\sqrt{p}$.
- An elliptic curve using a prime p with 160 bit, roughly 2160 points, provides security of 2^{80}steps on average that are required by an attacker and

- Similarly, an elliptic curve using a prime p with 256 bit, provides security of 2^{128}steps on average.

4.4 Applications of Cryptography and ECC

Elliptic Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully studied. ECC allows performing encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as with other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.

4.4.1 Cryptography and Elliptic curve cryptography are widely used in many areas;

- Cryptography is being used everywhere by billions of people. Mostly we use Security mainly in Securing Email Communications, Protecting data, Encrypting Databases and even Securing a Website.
- The most common use of cryptography is to encrypt and decrypt email and other plain-text messages. Each person with an email address has a pair of keys associated with that email address, and these keys are required to encrypt or decrypt an email.
- Electronic money (digital cash) includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.
- WhatsApp uses the ‘signal’ protocol for encryption, which uses a combination of asymmetric and symmetric key cryptographic algorithms. The symmetric key algorithms ensure confidentiality and integrity whereas the asymmetric key cryptographic algorithms help in achieving the other security goals namely authentication and non-repudiation. (WhatsApp uses the Curve25519 based algorithm)
- Instagram uses SSL/TLS over port 443 to encrypt requests from Instagram servers and will send you data over the same encrypted data stream. This prevents malicious parties from eavesdropping on the conversation between the user and Instagram.
- Elliptic curves are especially important in number theory, and constitute a major area of current research; for example, they were used in Andrew Wiles's proof of Fermat's Last Theorem.

- Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. Elliptic curves are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic curve factorization.
- ECC is most popularly used in smart cards. Smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms.
- PDAs(Personal Digital assistants) have more computing power compared to most the other mobile devices, like cell phones or pagers. PDAs are considered to be a very popular choice for implementing public-key cryptosystems. But ECC is an idol choice for PDAs because they still grieve from the limited bandwidth.
- For implementing the ECC, Constrained devices have been considered to be the most suitable platforms. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC.
- Also includes electronic commerce, chip-based payment cards, digital currencies, computer passwords, cyber security, and military communications

5. SUGGESTIONS

The major fields of mathematics like number theory, field theory, and coding theory play an important role in cryptology. A thorough understanding of cryptography is required to develop better ways to protect valuable information and we believe that this project will enlighten many students to pursue a career in cyber security we do hope that our project helps to motivate students to open up their curious doors towards the research in ECC .

The Clay Mathematics Institute of Cambridge, Massachusetts (CMI) has named seven "Millennium Prize Problems," selected by focusing on important classic questions in mathematics that have remained unsolved over the years one of the problems includes the Riemann hypothesis, where Kumar Eswaran’s claim of solving the equation has been in the news since 2016. of cryptography is required to develop better ways to protect valuable information as technology becomes faster and more efficient.

Most cryptography systems require mathematics to solve computational problems, else makes it hard to deduce the key to encrypted text.

ANUARY FEBRUARY MARCH APRIL MAY JUN JULY AUGUST SEPTEMBERINR

The coming technology, Metaverse will be the next big thing of the digital age, and also it has the potential to change everyday life. As the Metaverse demands to deliver permission less identity, financial services, and high-speed exchange. Data will have to be stored and served to millions if not billions of people. The answer to these problems lies in the technology of Cryptocurrency. And, the backbone of the upcoming technology underlies the concept and tools of cryptography and ECC.

6. CONCLUSION

In this project, we have covered an overview of the Evolution of Cryptography, Types of Cryptography, Elliptic Curve Cryptography and its Geometry, and Elliptic Curves and their operations. We have discussed the use of Elliptic Curves in public-key cryptography. Further, we have mentioned several topics along with applications and covered many more areas of cryptography and ECC. We urge to say that Elliptic Curve Cryptography can be the other version of RSA which is much cheaper and is based on cubic equations as ECC uses fewer bits than RSA.

1. Comparing Key Sizes for Equivalent Security

Symmetric scheme (key size in bits)	ECC-based scheme (size of *n* in bits)	RSA/DSA (modular size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Elliptic curve cryptosystems with a 160-bit key offer about the same security as RSA and discrete logarithm based systems with a 1024-bit key. Elliptic Curve Cryptography's main advantage is that the implementation allows for a significant reduction in key size as the ECC key of 160 bits is equivalent to the RSA key of 1024 bits and similarly 256 bits equivalent to the RSA key of 3072 bits which means limited memory and computational power.

ECC also allows resource-constrained systems like smartphones, embedded computers, and cryptocurrency networks to use 10% of the storage space and bandwidth required by RSA. As a result, the lengths of the public key and private key are much shorter in elliptic curve cryptosystems.

2. Significance of ECC in terms of speed and power

Nick Sullivan, *A (Realatively Easy to Understand) Primer on Elliptic Curve Cryptography* where he mentions that "We can compute how much energy is needed to break a cryptographic algorithm and compare that with how much water that energy could boil... By this measure, braking a 228-bit RSA key requires less energy than it takes to boil a teaspoon of water. Comparatively breaking a 228-bit elliptic curve key requires enough energy to boil all the water on earth. For this level of security with RSA, you'd need a key with 2,380 bits".

So, We use ECC in cryptographic key algorithm like Bitcoin and Etherium as it can potentially save 90% of the resources used by a similar RSA system. It seems that each year we see more systems moving from RSA to a more modern elliptic curve approach.

3. Role and necessity in today's world:

We can also apply ECC in wireless communication devices, smartcards, Web services and any application where security is needed but lacks the power, storage and computational power that is necessary for the current cryptosystems and we do believe that doing research in largescale can result in more widespread applications.

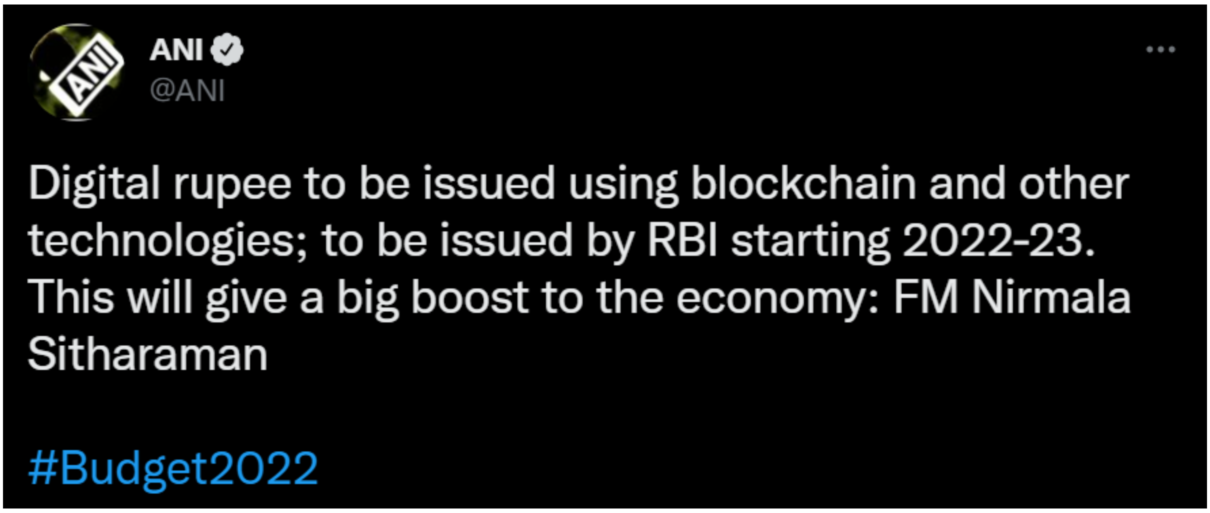
There has been a historical pattern that shows the country with the strongest encryption has been a leader in military power. By studying cryptography and encryption, a country could strengthen its defences and have the necessary means to survive in a hostile world.

An understanding of encryption can also help individuals with securing private data and information. Even though it is severely unethical, our communication with one another is constantly being monitored. Those who monitor our communication can include governments, internet service providers, hackers, identity thieves, and more.

By learning to use cryptography for secure communication, we can safeguard ourselves from being compromised by those who could steal our information.

4. Need a new form of encryption

The government has proposed to issue a digital rupee managed by the RBI, Finance Minister Nirmala Sitharaman announced in the Union Budget 2022. Introduction of a Digital currency by the government will lead to cheaper currency management where it need a new formencryption and security standards



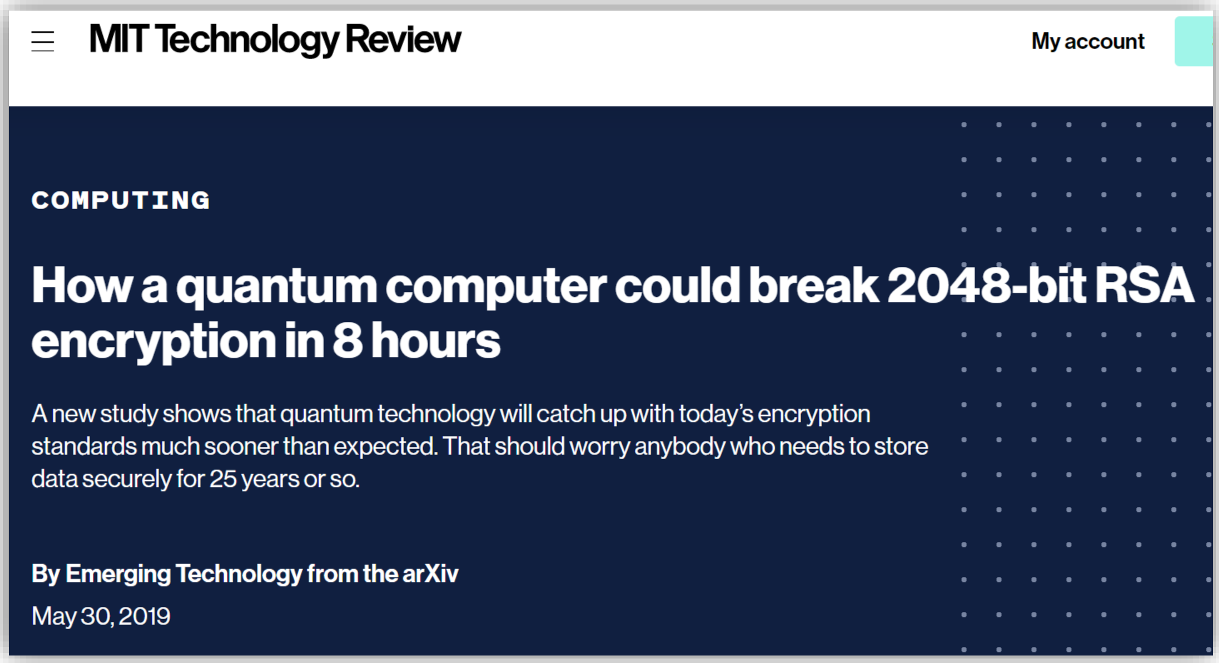
ANI

@ANI

Digital rupee to be issued using blockchain and other technologies; to be issued by RBI starting 2022-23. This will give a big boost to the economy: FM Nirmala Sitharaman

#Budget2022

Further, we would like to know a study on Quantum security because most of the cryptography that is currently used in several areas (many of the data infrastructures) including the daily basis on the internet can be fatally broken by sufficiently powerful quantum computers.



COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

By Emerging Technology from the arXiv

May 30, 2019

Yet this is not necessarily a threat in the next few years but, Building a currency of the future means that it should be built to withstand the attacks of a quantum computer.

7. REFERENCES

1. Introduction to Cryptography: With Coding Theory Book by Lawrence C. Washington and Wade Trappe
2. Cryptography and Network Security: Principles and Practice, Book by William Stallings
3. https://avihttps://digitalvarys.com/what-is-cryptography-and-its-types/
4. https://en.wikipedia.org/wiki/Elliptic_cuprve_cryptographyhttps://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve
5. networks.com/glossary/elliptic-curve-crytography/
6. https://www.desmos.com/calculator/ialhd71we3
7. https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm
8. https://www.indiatvnews.com/business/news-what-is-cryptocurrency-types-investment-price-ban-in-india-746789
9. https://hackaday.com/2019/07/04/understanding-elliptic-curve-cryptography-and-embedded-security/
10. How Elliptic Curve Cryptography Works - Technical Articles (allaboutcircuits.com)

11. The Diffie-Hellman Exchange in Embedded Cryptography - Technical Articles (allaboutcircuits.com)
12. https://abelprize.no/sites/default/files/2021-04/pressrelease_en_2016_A.Wiles_.pdf
13. https://www.claymath.org/millennium-problems/millennium-prize-problems
14. https://blogmathmusingsbyrohanjha.blogspot.com/2020/06/how-to-make-cool-million-dollars-by.html
15. https://www.ox.ac.uk/news/2016-03-15-fermats-last-theorem-proof-secures-mathematics-top-prize-sir-andrew-wiles
16. https://www.desmos.com/calculator/ialhd71we3
17. https://avinetworks.com/glossary/elliptic-curve-cryptography/
18. https://www.ox.ac.uk/news/2016-03-15-fermats-last-theorem-proof-secures-mathematics-top-prize-sir-andrew-wiles
19. https://blogmathmusingsbyrohanjha.blogspot.com/2020/06/how-to-make-cool-million-dollars-by.html
20. https://www.claymath.org/millennium-problems/millennium-prize-problems
21. https://www.allaboutcircuits.com/technical-articles/the-diffie-hellman-exchange-in-embedded-cryptography/
22. https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/

https://hackaday.com/2019/07/04/understanding-elliptic-curve-cryptography-and-embedded-security/

23. https://www.indiatvnews.com/business/news-what-is-cryptocurrency-types-investment-price-ban-in-india-746789
24. https://www.tutorialspoint.com/cryptography/origin_of_cryptography.html
25. https://cybersecurityventures.com/cybercrime-infographic/
26. https://www.pgurus.com/india-to-approve-crypto-currencies-like-bitcoin-bill-placed-in-parliament-for-approval