**ANALYSIS AND IMPLEMENTATION OF ELLIPTIC KEY CRYPTOGRAPHY**

**BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE**

**& ENGINEERING(2018-2022)**

**ABSTRACT**

Advancement in the technology has brought major changes in the current systems and thus made these a better version of the previous ones. This project deals with the concept of Elliptical Curve Cryptography to be used as a method of public key exchange system to exchange shared secrets among untrusted nodes. Towards the end the project includes the analysis and the implementation of this method of cryptography. This work discusses the methodology of generating points on elliptic curves in a method such that the internal state of the machine remains unpredictable. It is more efficient than its competitor RSA (Rivest–Shamir–Adleman) as it provides much smaller keys sizes with the same if not better mathematical backbone. The main concern of this work will be around generation of public and private keys using Elliptic Curves. Further this work will discuss mathematical superiority of Elliptic Curves and its use along with Diffie-Hellman Key Exchange to establish shared secret. It is frequently written on the internet that this type of cryptography is a very powerful approach but is understood by very few people which makes the topic very interesting to work on as well.

Keywords: Cryptography, Elliptical Curve Cryptography, Diffie-Hellman algorithm, RSA

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Contents** | **Page No.** | |
| 1. | Introduction | 1 |  |
| 2. | Application | 2 |  |
| 3. | Literature Review | 3 |  |
| 4. | Objectives | 4 |  |
| 5. | Methodology | 4 | – 5 |
| 6. | Designing Phase | 6 | – 17 |
| 7. | Screenshots |  | |
| 8. | References |  | |

|  |  |
| --- | --- |
| Pg 7 | Workflow |
| Pg 8 | Symmetric key and Asymmetric key Encryption |
| Pg 9 | Diffie Hellman key Exchange and RSA |
| Pg 10 | Elliptic Curves |
| Pg 17 | Public key Encryption |
| Pg 20 | Elliptic Curves |
| Pg 21 | Point Addition |
| Pg 22 | Doubling |
| Pg 23 | EC points |
| Pg 24 | User Case Diagram |
|  |  |
|  |  |

**LIST OF FIGURES AND TABLES**

**WORKFLOW**

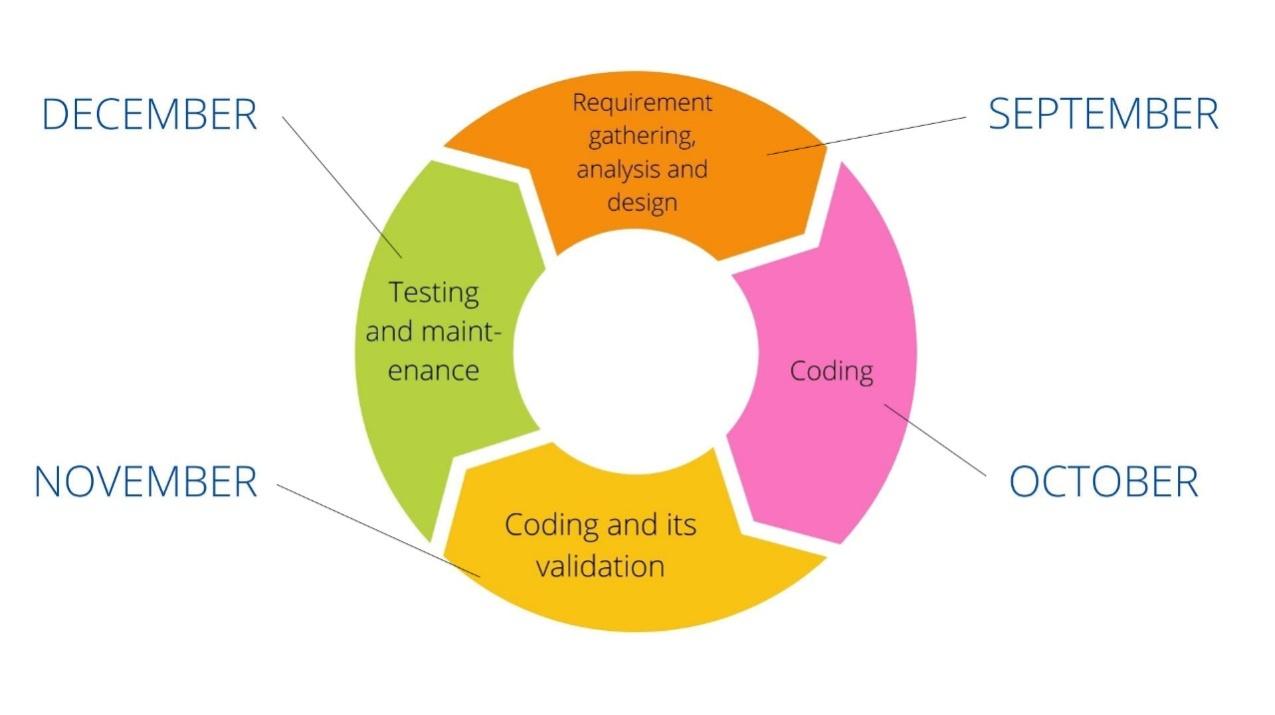
****

Fig 1: Workflow

**INTRODUCTION**

Cryptography is the method of hiding information using mathematically inclined functions to encrypt plain text into cipher text and thus ensures the Confidentiality and Integrity of the data.

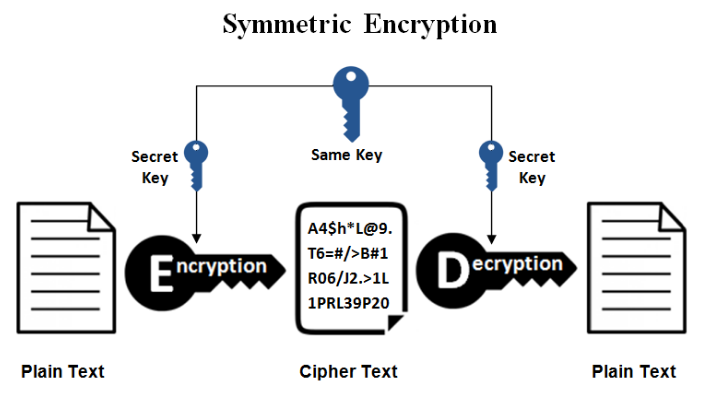


Fig 2: Symmetric Encryption

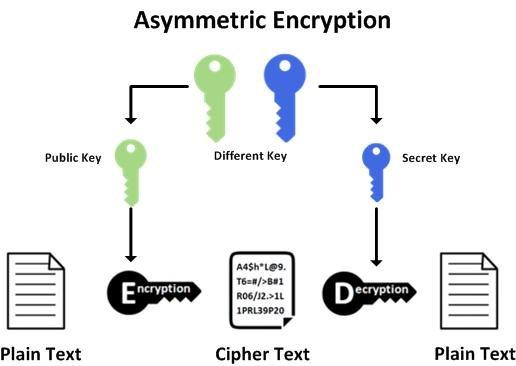


Fig 3: Asymmetric Encryption

There are two types of cryptography:-

* Public key cryptography
* Private key cryptography

Private key cryptography includes a single, common and shared secret key which is used to encrypt as well as decrypt the data as well.

In public key cryptography, the public key is used to encrypt the data while the private key is used to decrypt the data which is shared among the sender and the receiver while the public key is accessible in the public domain.

ECC or Elliptical Curve Cryptography is a public key cryptography method which is used in conjunction with the RSA and the Diffie-Hellman algorithm.

**Diffie-Hellman algorithm:-**

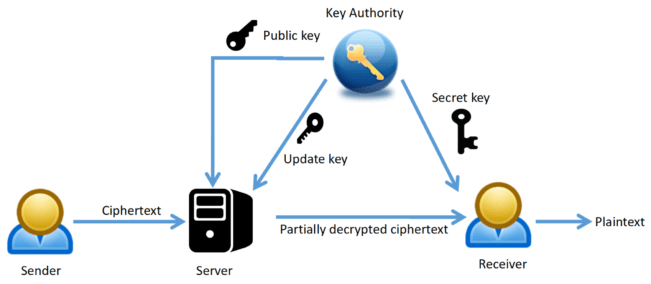


Fig 4: Diffie-Hellman Key Exchange

Whitfield Diffie and Martin Hellman are the inventors of this algorithm in which there is an exchange of keys (cryptographic) over the channels which are public. Exchange here does not mean legitimate exchange but it actually means that the keys are derived jointly. It is an asymmetric encryption method.

**RSA algorithm:-**

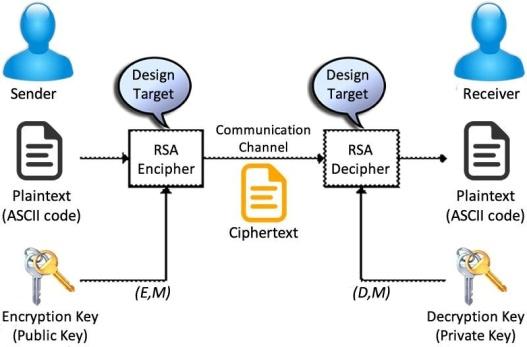


Fig 5: RSA

It is an asymmetric encryption or public key cryptography method where both private and public keys are used in order to encrypt and decrypt the information. The basic idea of this algorithm is to find the factors of composite numbers (large) which is originally very difficult but when the factors are only prime then the term prime factorization is used for the problem. Key generation i.e. both public and private key generation also takes place in this method.

**Elliptical Curve Cryptography:**

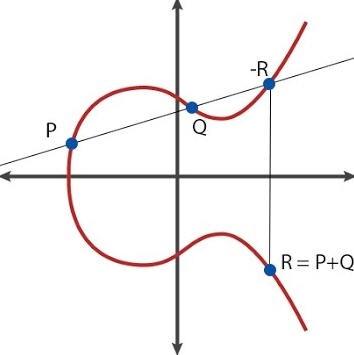


Fig 6: Elliptic Curve

It is based on the theory of Elliptic curve and thus is used to efficiently create smaller and more secure keys. Basically the functions and the properties of an ellipse have been studied since 150 years but the use of the elliptic curve equation in cryptography was introduced by Neal Kobiltz from the University of Washington and by Victor Miller at IBM (separately) in the year 1985. The logic behind this method is the elliptic curve equation which is used instead of the old method for the process of generation as the product prime numbers (very large). The mathematical equation of an elliptic curve is:-

CodeCogsEqn (6).gif

**DIFFERENCE IN RSA AND ECC**

|  |  |
| --- | --- |
| **RSA** | **ECC** |
| Large amount of time require for computation:  For providing higher securities we have to use larger bit keys therefore the amount of time is high for calculation. | Less amount of time require for computation:  In ECC we are having very less bit key size hence the calculation time is very less. |
| Larger storage required:  In order to store the big size keys we are required to use larger storage. | Less storage required:  Small size keys did not require the higher storage. |
| For increasing the security larger bit size key required | Can provide same amount of security at very small bit size key |
| Because of high hardware requirement we can use this in limited field of areas | Not require high specs hardware so can be used at more fields of area.  Exp: smartwatches,smartphones,tablets,etc. |
| For applying this algorithm we require a high performance system and good software for calculations.  Therefore, the price requirement is also high | ECC did not require high hardware software; it can easily work on limited system hardware and software so the price is very less but security is high. |

Here are some differences in key size of ECC and RSA; both are having the same level of security but at different key sizes.

|  |  |
| --- | --- |
| **ECC (SIZE OF KEY IN BITS)** | **RSA (SIZE OF KEY IN BITS)** |
| 112 | 512 |
| 160 | 1024 |
| 224 | 2048 |
| 256 | 3072 |
| 384 | 7680 |
| 512 | 15360 |

**APPLICATIONS OF ELLIPTIC CURVE CRYPTOGRAPHY**

1. **TRADITIONAL APPLICATIONS:-**

Within the past few decades ‘ECC’ has become more and more common on the web. Many mainstream operating system, web browser, server software has some support of ‘ECC’ as well.[3]

* KEY EXCHANGE
* DNSSEC VALIDATION
* SIGNATURE SERVER

1. **MOBILE APPLICATIONS:-**

As the growth of mobile phones increases within the past decade, more people have mobile devices than before. Also, these mobile devices also contain private information of the people and they also have the feature to connect to the internet the attacker there are trying to exploit the security weakness of these devices.[4]

* AUTHENTICATION
* MANET
* INTERNET OF THINGS

1. **MODERN APPLICATION’S:-**

Aside from the Traditional and modern application many researchers have implemented

ECC in less conventional settings.[5]

* SMART GRID
* VEHICULAR COMMUNICATION
* RFID
* IRIS PATTERN RECOGNITION
* E-HEALTH APPLICATION

**SYSTEM REQUIREMENTS**

**Windows Operating System:**

* **Hardware:** 
  + Ram: 1GB and above
  + Hard Disk: from 2 to few Mb’s.
* **Software:**
  + Any Linux system with installed C interpreter and compiler.
  + Or IDE’s like Dev C++ or Turbo C++

**MAC operating system**

* **Software:** Install Apple Developer Tools then you have two choices i.e.Xcode IDE or use gcc.

**LITERATURE REVIEW:**

|  |  |
| --- | --- |
| Harkanson, R., & Kim, Y. (2017, April). Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research (pp. 1-7). | It explains about the structure of the curve and the basic general equation that the elliptic curve uses. It also tells about how to operate between two points. What is the application of the elliptic curve in tradition and modern scenario |
| Brown, E., & Myers, B. T. (2002). Elliptic curves from Mordell to Diophantus and back. *The American mathematical monthly*, *109*(7), 639-649. | This work deals with generation of other roots of the equation out of known roots and this method is what we call the Diophantus Rule which we have exploited in order to generate multiple points of of the known points. |
| Smart, N. P. (1999). The discrete logarithm problem on elliptic curves of trace one. *Journal of cryptology*, *12*(3), 193-196. | This work deals with mathematical superiority of Elliptic Curves over other modulus based key generation methods. |

**PROBLEM STATEMENT**

Current Standards of Public Key Cryptography relies heavily on Diffie-Hellman Key Exchange using RSA standards for Key Generation. RSA provides a computationally strong mathematical function for generating keys around 2000 to 4000 bit which is a **NP-HARD** but it has some serious optimization problems when it comes to continuous key exchange for a long period of time for example in case of a server.

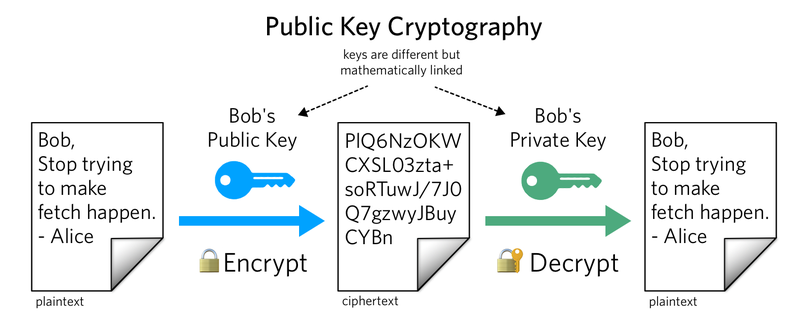
RSA encounters problems such as:

1. RSA is slow in terms of time taken for key generation.
2. RSA requires a significant space for storage.
3. Inefficient for continuous long term usage.
4. Not designed for modern day IOT devices which have limited storage.
5. Only way for RSA to be stronger will be to increase key size which further adds more to the current problem.

**PUBLIC KEY CRYPTOGRAPHY**

It is also known as Asymmetric key cryptography. It is an encryption algorithm that uses the mathematically related but two non-identical keys (**public key and private key**). Unlike the symmetric key algorithm that uses the same key for encryption as well as for decryption. It uses two different keys. The **public key** is for ‘encryption’ and **private key** is for ‘decryption’.

**WORKING OF THE PUBLIC KEY CRYPTOGRAPHY**



**Fig 7: Public key**

Let’s assume that Bob has the message that he wants to share it with Alice. So, Bob will first encrypt his plaintext message into the cipher text using a public key. And the cipher text is sent through the network to Alice. And Alice will decrypt the cipher text into the plaintext using a private key in order to read it.

**ADVANTAGES-:**

1. No need for key exchange.
2. One key cannot be derived from another key.
3. It maintains the authentication and confidentiality at the same time.

**DISADVANTAGES-:**

1. It is slow as compared to symmetric key cryptography.
2. It uses more computer resources/supplies compare to single key encryption

**APPLICATION OF PUBLIC KEY CRYPTOGRAPHY:-**

1. **DIGITAL SIGNATURE:-**

Digital Signature helps us to verify that the message is provided by the trusted user/identity.

**For example:**Digital Signature enable the development of secure automatic updates into the wordpress. Suppose if the attacker gains access to their update server’s more than thirty percent of the internet site will be affected with malwares.

1. Most public key cryptography algorithm used is RSA.

**OBJECTIVES**

Objective of this Project is to generate a private key using Elliptical Curve Cryptography.

The sub-objectives of this project are:

1. Literature of public key cryptography.

2. Analysis of various public key cryptography algorithms.

3. Analysis and implementation of ECC algorithm

**METHODOLOGY OF APPLYING ELLIPTICAL CURVE CRYPTOGRAPHY**

An Elliptic Curve is combination of discrete points plotted on a Galois finite field (GF(2^n)) following the equation:

**y² = x³+ax+b**

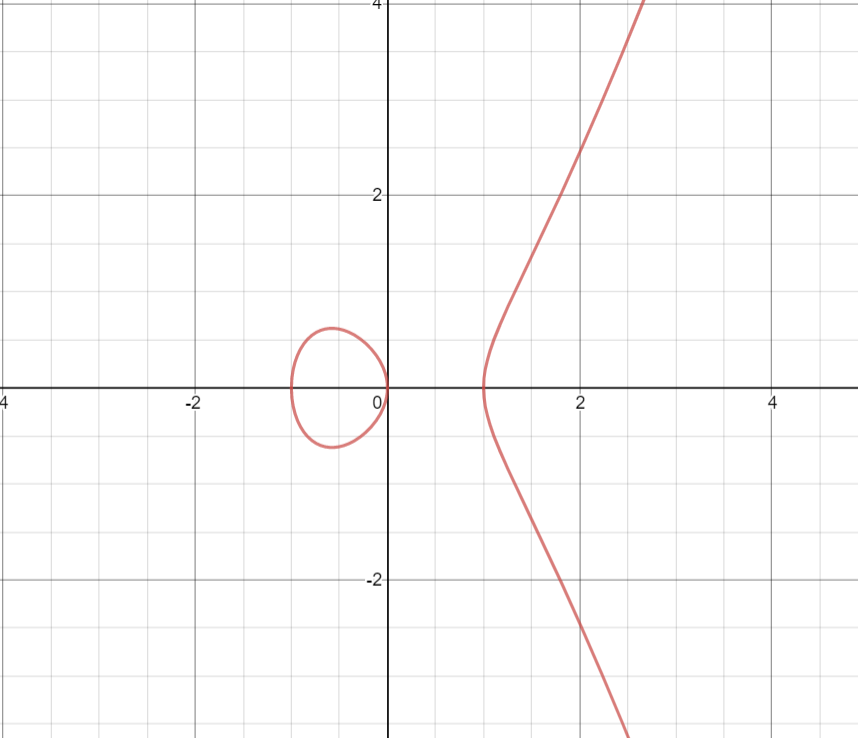


Fig 8: Elliptic Curve of equation y^{2}=x^{3}-x

Elliptic Curve equation is derived from the Generalized Weierstrass Equation i.e:

C:\Users\Divyansh Kamboj\Desktop\Sem 5\Minor 1\weistrass.PNG

**Characteristics of Elliptic Curves:**

1. Non-Singular.e (-16(4b^3 + 27a^2)) != 0
2. Points over finite field
3. Falls under Abelian Group

**Plotting Points on the Elliptic Curves:**

Using **Diophantus rule**[1] of point generation i.e generating the third root from the known 2 roots we will plot the points on a graph which will further be used as our public and private key.

To plot the points using Elliptic Curve equation, we have 2 methodologies:

1. Point Addition
2. Doubling
3. **Point Addition:**

Let us assume a point P on the curve and draw line tangent to the point P. Draw a tangent

to the point P and wherever the tangent intersects the curve is point R.

When we obtain the image of the point R on the other side of the graph, we obtain a point 2P

i.e we are performing:

1. **Chord** from point P to Q intersecting at point R.
2. Mirror of point R which is considered as P+Q.

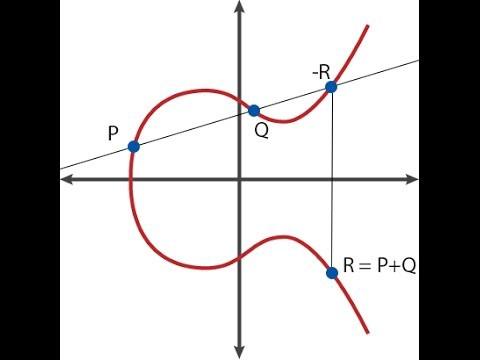


Fig 2: Point Addition Operation

We go on adding the R with P again and again till we reach a pointXp where x and P should be

large integers.

P+R+P+R+…………. = x.P

**Xp = x.P**

**Doubling:**

The doubling operations are performed when the points P and Q are the same.

In that case operations performed are:

1. **A Tangent** is drawn with respect to point P.
2. The point on the curve where the tangent intersects will be R i.e. 2P.

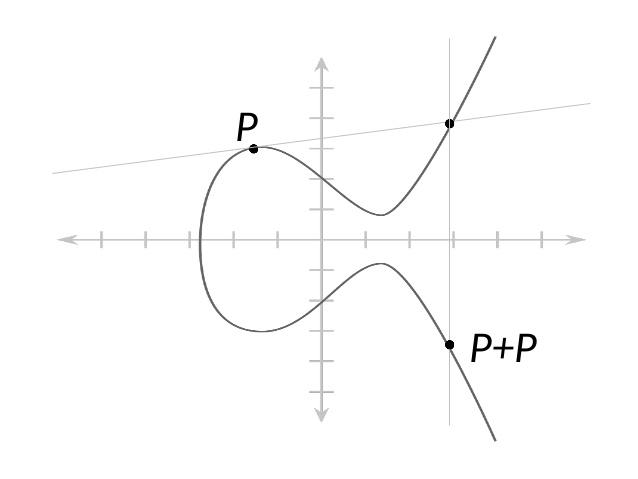


Fig 3: Point Doubling Operation

As shown in the figure, the point P will add to itself again and again till we reach the point Xn such that:

P+P+P+P………….= x.P

**Xn = x.P**

**The x coordinate of the Xn is what will become our PUBLIC KEY. And the Y coordinate of Xn will be used as our Private Key.**

The equation **Xn = x.P** is basis and foundation of what is referred as **Discrete logarithm problem**

**of Elliptic Curves**[2]. The problem states the given value of from the value Xn i.e the Public key,

it is not mathematically possible to find the value of x i.e the number of time point addition or doubling has been performed. Or in other words, provided the initial point and the public key, one cannot determine the internal state of the Elliptic Curve point generator given that the point P and Q are very large numbers i.e 112 bit – 256 bit.

The points on elliptic curve will be scattered as follows:

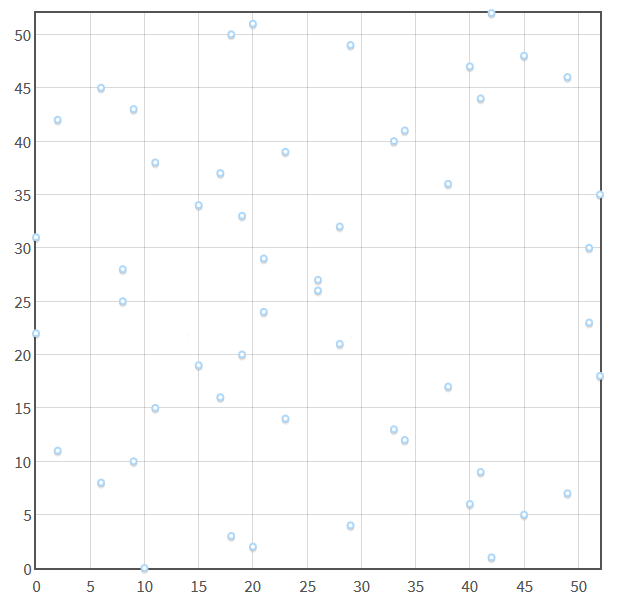
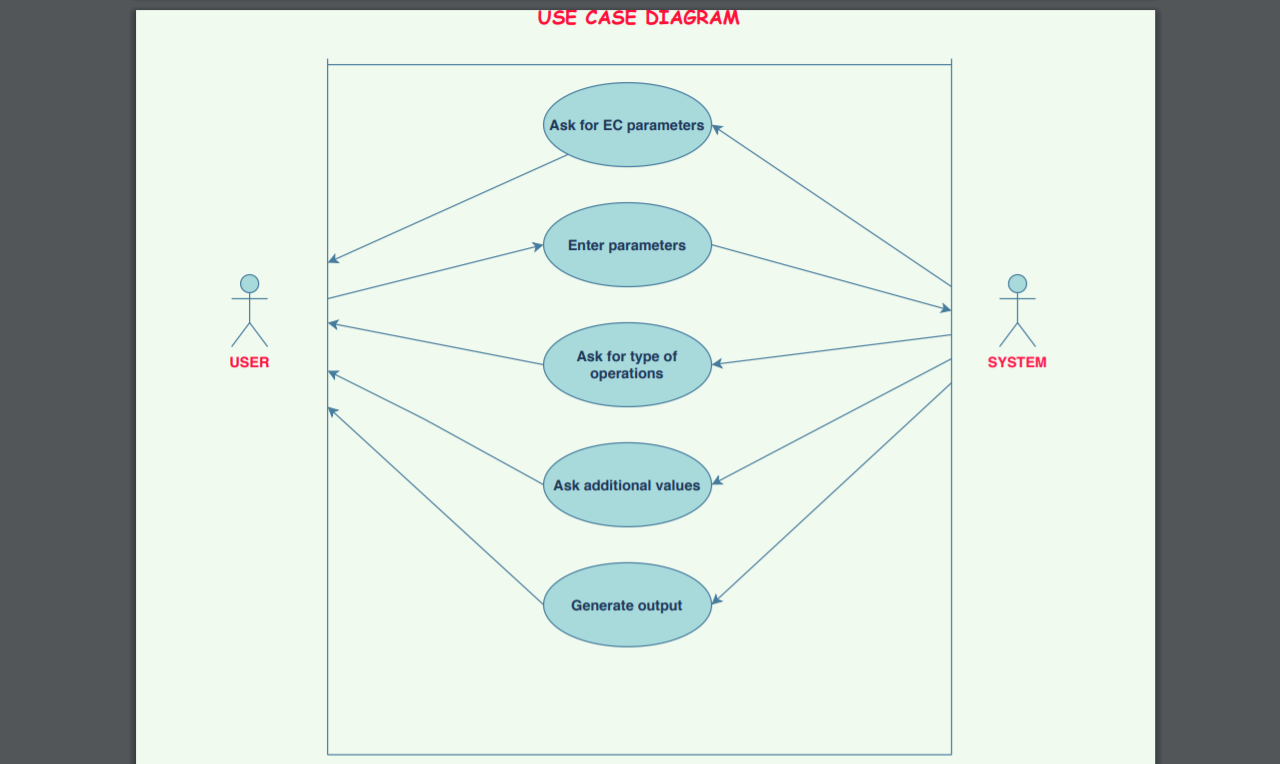


Fig 3: Points scattered over Elliptic Curve

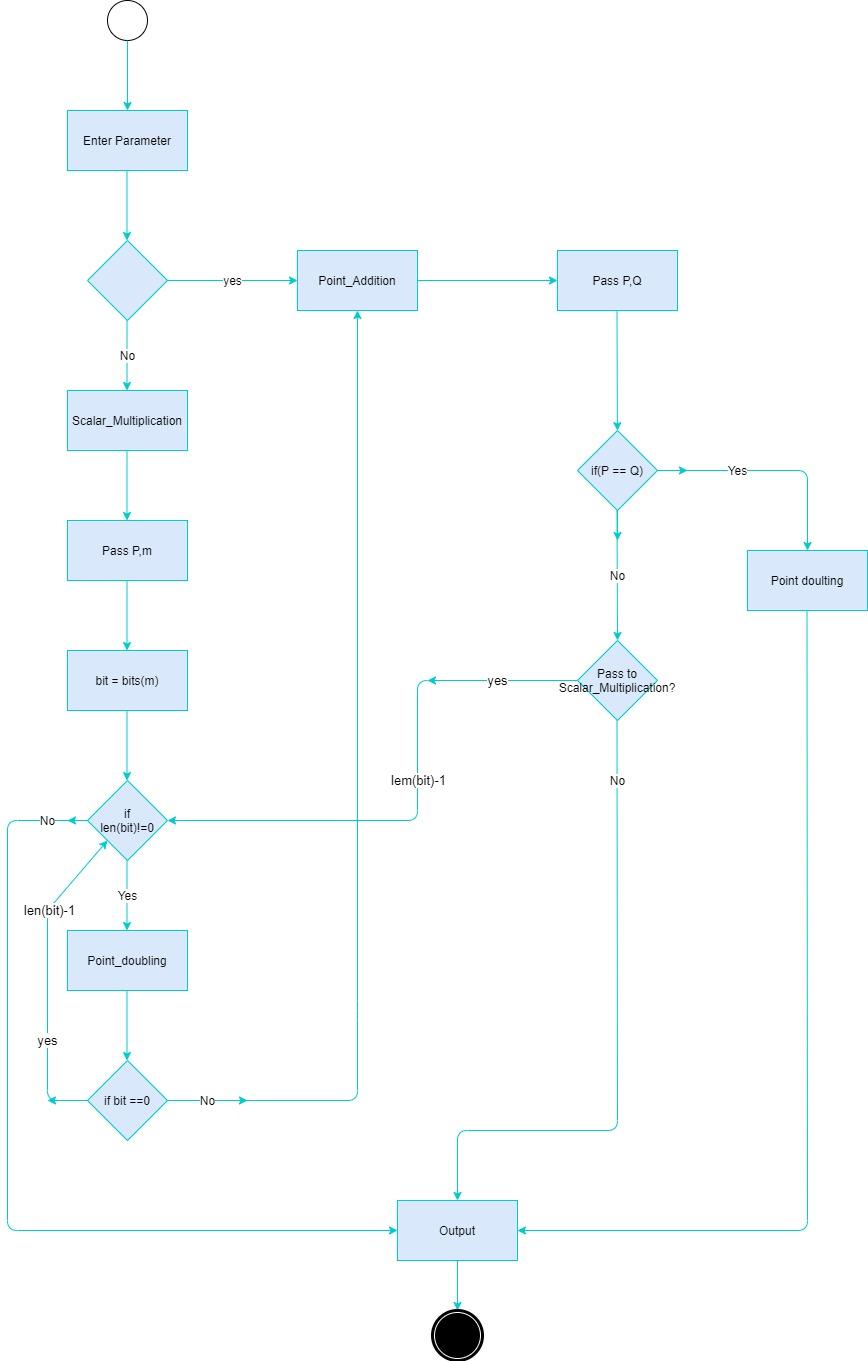
**CHALLENGES:**

1. Choosing a Non-Singular Curve Equation.
2. The initial points P and Q.
3. Conversion of Affine Coordinated to Projective Coordinates.
4. To reduce the number of inverse operations it is too costly to perform.

**USE CASE DIAGRAM**

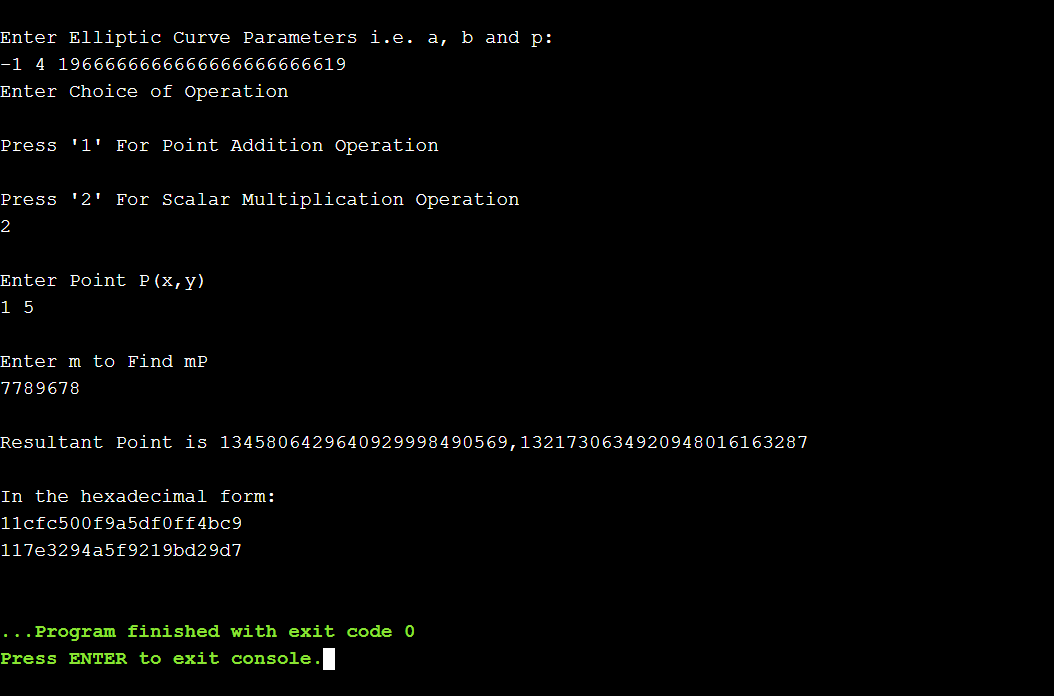
****

**ACTIVITY DIAGRAM**

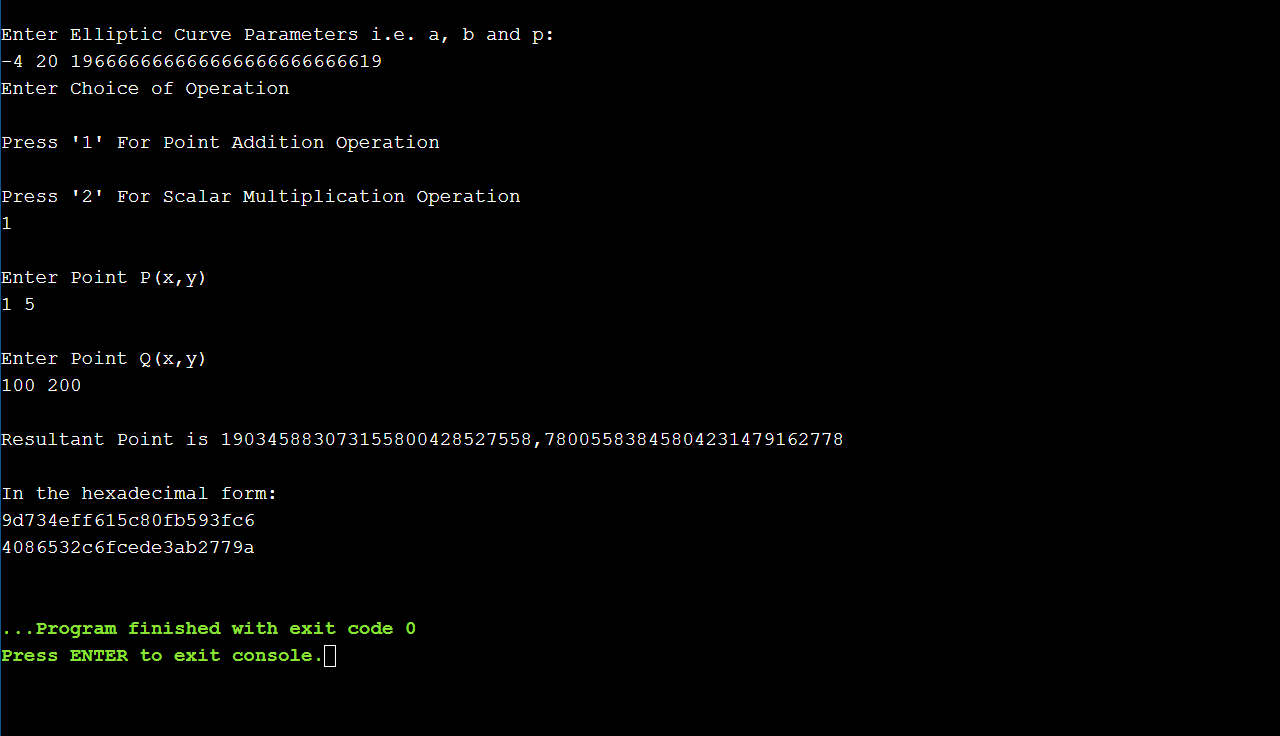
****

**OUTPUT-**

***SCALAR MULTIPLICATION***



***POINT ADDITION***



References:

1. Brown, E., & Myers, B. T. (2002). Elliptic curves from Mordell to Diophantus and back. *The American mathematical monthly*, *109*(7), 639-649.
2. Smart, N. P. (1999). The discrete logarithm problem on elliptic curves of trace one. *Journal of cryptology*, *12*(3), 193-196.
3. Harkanson, R., & Kim, Y. (2017, April). Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research (pp. 1-7).