# CRYPTOGRAPHY

***Submitted To:***

***Dr. Purnendu Pandey***

***Submitted By:***

***Rahul Gupta***

***Ayush Govil***



**SCHOOL OF ENGINEERING &TECHNOLOGY**

**BML MUNJAL UNIVERSITY**

**April 2020**

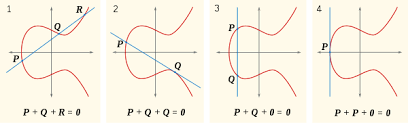
**Abstract**

Elliptic curve cryptography is an algorithm that is used for public key encryption using the properties of an elliptic curve over a finite field. The most important property about elliptic curve which makes it difficult to decrypt is the discrete algorithmic problem to get the private key. The curve has operations which is different from the algebraic operations. These operations are applied on the elliptic curve in the finite field which gives the end point within the curve which will be the encrypted message.

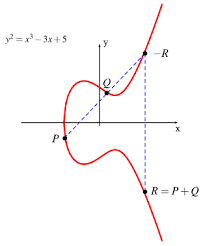
By using these operations a trapdoor function is generated. This trapdoor function makes it very difficult to decrypt the message. It can be decrypted only by the person for whom the message is meant. Deffi Hellman technique allows key exchange between the sender and the receiver. Since the operations in ECC are commutative , a key is shared by the sender on which the receiver performs the operation using his own private key to generate the final key . This final key cannot be obtained by the third party because he has the obtain the private keys which only the sender and receiver has. These private keys are used with the generator point to generate the key. The equation is given as: n=p.G where G is the generation point and p is the private key. Even if the hacker obtains the n value and G, he will not get the private key p because of the discrete logarithmic problem of ECC . ECC also uses shorter key sizes than many other cryptosystems thus making it faster. The paper gives a review of different works done on elliptic curve cryptography which shows how useful this technique is for communication between the systems in a network.

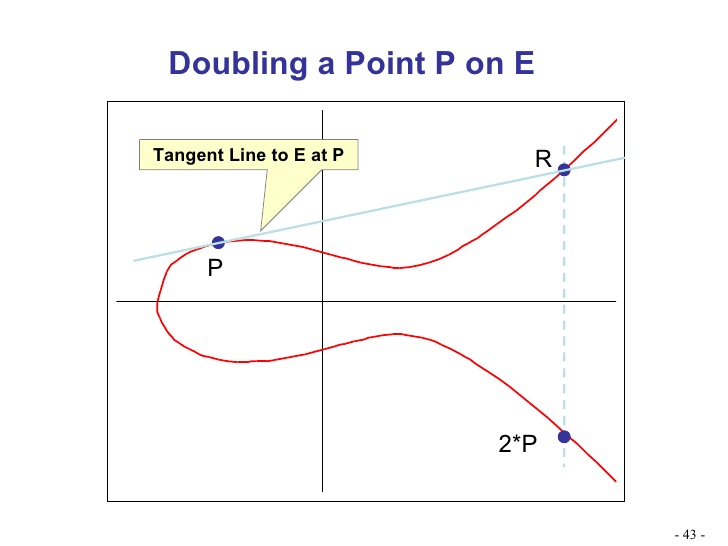
**Introduction**

The Elliptic curve cryptography algorithm is a public key encryption algorithm. We have applied this algorithm in encrypting the key which is used for encrypting the data and the key that is used in Digital Signature. Digital Signature is used to provide three security measures: Integrity, Authenticity and Non-repudiation. In order to prevent the break of these security measures we need to save the key from the third parties. If the key is compromised the digital signature can be generated by them and thus frauds happen. So in order to prevent the break of key we are using Elliptic Curve Cryptography technique with Deffi Hellman key exchange algorithm. The ECC algorithm has a discrete logarithmic problem and the operations in the algorithm are commutative. ECC algorithm in digital signature is used in bitcoins to ensure that the transaction is made between the trusted parties. We have also used the ECC algorithm in encrypting the public key that is meant for encrypting and decrypting data. The operations performed in this algorithm are different from normal arithmetic operations.



In one of the curve we see that P+Q+R=0. We can write it as P+Q=-R. So we get the R point by dropping a perpendicular from the R point that we got . See the diagram below. R is the result that we wanted.



Similarly we can perform point doubling operation and can derive multiplication operation.

We can derive the multiplication operation from the addition operation which is the most important part in encrypting the key. For example:

7P=P+P+P+P+P+P+P

With this multiplication we generate the public key.

**Literature Review**

1. Smart grid system helps in saving and adjusting the power supply to its customers who are connected to the system on the basis of the status and consumption information of the customers. There is a communication channel between the customers and the system which needs to be secured. If not secure the intruders can alter the data which is transmitted from the communication channel which in turn will alter the power supply making unusual changes in the power. Khalid Mahmood (2017) has introduced the use of elliptic curve cryptography that is an efficient way as compared to other algorithms such as RSA and DSA because of its lower key size. He uses ProVerif tool to analyze the security provided by ECC which shows that it is highly secure technique.
2. Laiphrakpam Dolendro Singh(2015) in his paper has proposed a technique to encrypt the text without the classic technique of mapping the characters to other characters. Therefore it removes the use of a lookup table which takes up space. He uses the ASCII values of the text and pairs them with one another which serves as an input to the elliptic curve. The algorithm can encrypt large data by dividing it into smaller size consisting of multiple characters. This technique is designed in such a way that it can encrypt or decrypt any type of script i.e. it is not confined to only English script and can be used for any script. This algorithm needs only the ASCII values of the text and since every text in every language has some ASCII values. This algorithm uses the ASCII values of the text for the encryption .
3. Privacy and security of images is important nowadays as due to the increase of cyber crimes in the present scenario. Ponmani E.(2018) has introduced a secure way to for transmission of the images using Elliptic Curve Cryptography. This technique is applied on the images which are compressed by Discrete Wavelet Transform technique which is the best technique for compression. The private key is generated from

the compressed image which together is sent to the receiver by the sender. This provides Integrity and Confidentiality of the image.

4.K.S.Abitha and Anjalipandey(2015) in their paper proposed a method which provides a secure data transmission technique with the help of AODV algorithm and Ellipitc curve Cryptography. AODV is a routing protocol used for transferring data and is used in mobile networks. It is a protocol supervises the network and decides that which device will send data to which other device or devices. The three modules used in this project are Ad Hoc On-Demand Distance Vector Routing, Packet discovery and Elliptic Curve cryptography which is the essence of this complete secure transmission between the devices.The system uses a shared key and a private key for this technique. This method increases the efficiency of the AODV protocol due to the discrete logarithmic problem of the ECC algorithm that is almost impossible to break.

**Conclusion of Literature Review**

Different works from the researchers provides us the knowledge that Elliptic Curve Cryptography is secure and reliable algorithm which can be used in almost every field. It provides the same level of security that RSA or other old algorithms can provide with shorter key size. The use of ECC by researchers in different fields shows it that it is progressive and can expand to many different sectors such as finance, business, secret agencies due to its discrete logarithmic problem. The world is dependent on data and cyber attacks is more prevalent in the present scenario therefore it becomes very crucial to secure the data to maintain its confidentially, integrity and availability. Governments and secret agencies cannot compromise with their data therefore evolution in cryptography is important. One of the evolution is Elliptic Curve Cryptography.

**Software Used**

Jupyter Notebook: It is an easy to use software that works as an IDE to write python code. Data visualization and analysis can be done on this platform. It contains several inbuilt modules and libraries which allows to write small and readable code.

**Result Analysis**

ECC algorithm has various advantages over other existing cryptographic algorithm. These advantages are described below.

* It has Short Encryption key that value has to be fed from encryption Algorithm and later to be decrypted an encrypted message.
* It is faster & requires less computation power and less time consuming.
* It is more important in wireless devices, where computing power, memory and battery life are limited.
* It increases the size of the encrypted message.

ECC algorithm has some disadvantages also, which can be illustrated as:

* ECC Algorithm is more complex and more difficult to implement.
* Due to complexity of the Algorithm, it increases the implementation errors and by that it reduce the security of the Algorithm.

**Conclusion and Future Scope**

In the given paper we have implemented Elliptic Curve Cryptography in Deffi Hellman Key Exchange and Digital signatures that are used for authenticity, integrity and to prevent repudiation. It is an algorithm which uses less key size to provide the same level of complexity than other advanced algorithms provide such as RSA algorithm. Elliptic curve when applied on Digital signature is called ECDSA algorithm. Researchers are still working on this field with researches emerging in various directions. Presently RSA algorithm is used in many sectors for asymmetric

encryption. With time the technology will get advanced and so will be the cyber attacks. With the introduction of quantum computers, RSA algorithm would be very easy to break and to increase the security, it needs to have large key size. Therefore ECC encryption can be used in place of RSA algorithm which can withstand more powerful attacks.

**References**

1. Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumari, Xiong Li, Arun Kumar Sangaiah(2017). An Elliptic Curve Cryptography based Lightweight Authentication Scheme for Smart Grid Communication. *Future Generation Computer Systems*
2. Singh,D.L. and Singh, K. M(2015). Implementation of Text Encryption using Elliptic Curve Cryptography. *Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)*
3. Ponmani,E., Nandhini,E., Karthika K., Palani,S(2018). Secured Transmission of a compressed image by using ECC. *International Journal of Pure and Applied Mathematics (IJPAM-2018)*