Algorithm for Encryption and Decryption Based on Elliptic Curve Cryptography and Caesar Cipher

Yogesh Anand[1.], Monika Sharma[2]
AIIT, Amity University, Noida (U.P)
yogeshanandprogrammer@gmail.com[1],msharma5@amity.edu[2.]

Abstract-Cryptography is the technique to protect the data from unauthorized access. In this era of Information security various cryptographic algorithms are used. But information technology is not only means to secure information from unauthorized access but with using limited power and limited memory usage.

In this paper we have proposed encryption and decryption algorithm to protect the information with limited power and memory usage using Elliptic Curve Cryptography and Caesar Cipher technique with Dot Net as a Implementation Tool.

Keyword ---Elliptic Curve Cryptography, Ciphertext, Encryption, Decryption

I. INTRODUCTION

A. CRYPTOGRAPHY

Cryptography is the technique used to encrypt and Decrypt the data for security reasons. It is the technique which hides the data in some unknown format so unauthorized person can't access that.

B. ENCRYPTION

It is the technique which is used to convert the data in some different format which is not easy to understand or which changes the sense of the original data.

Example ABCDF -→ after encryption-→QSDAG

C. DECRYPTION

It is the technique which is used to obtained the original data by the encrypted data.

Example QSDAG→after decryption→ABCDF

D. PRIVATE KEY

It is the key which is matched with the public key to decrypt the data .It saves at server side and generally a secret key which isn't share with anyone. It is fast as compare to public key.

There are various techniques used for Encryption and Decryption .like RSA, DES, Cipher text, Plaintext, SHA, and Elliptic Curve Cryptography. But Elliptic Curve Cryptography is one of them which is more secure for finite fields and fast. It was first proposed by Victor Miller and Neil Koblitz in the Year 1985. Elliptic Curve Cryptography over finite fields shows that the Key comparison to RSA is too small. But this is only for finite fields. There has been lots of changes occurred in Elliptic Curve Cryptography.In Elliptic Curve Cryptography we need public key and private key to encrypt the data and then decrypt the data .In both case both Keys are useful. Elliptic bends are not comparable from ovaL[3]. An elliptic bend will be the gathering of focuses in x-y arrangement to fulfill an comparison x^3+a6+a4x+a2 x^2=a1xy+a3y+$y^{2.}$

II. LITRATURE REVIEW

A. Today's time data security is must because we are using everything on Cloud Computing.

Data security is must and we need to create that kind of system which takes low memory, less key size, lesser encryption and higher decryption with limited power and limited bandwidth [1].

B. In auditing the Encryption and system protection since 1970, a paramount pattern has extended. The science included in great cryptography is exceptionally mind blowing and regularly

troublesome, however numerous product applications have a tendency to conceal the points of interest from the client accordingly making cryptography a helpful instrument in giving system and information security Many companies are consolidating information Encryption and information arrangements, taking into account strong cryptographic methods, into their system security key arranging projects. Cryptographic long haul security is required yet is frequently hard to obtain. Cryptography provides as the establishment for most IT security availability, which include Digital signature should be platform independent, such as Windows 2000,7,8; and to provide the security to the bank sites where money matters and provide security (SSL) and(TLS) for authorization and IT protection. The presentation of digital cards that permit access history and records in nations, for example, Germany, contains the data about their people to know information about them.; then again, solid open key, and the option may be too non corporate[2].

C. Elliptic bend cryptography (Elliptic Curve Cryptography) was first presented by Neil Kolbitz and Victor Miller in year 1985. The fundamental reason for elliptic bend cryptography usage for RFID innovation is that there is no sub exponential calculation known to unravel the discrete calculation issue on an fittingly chose elliptic bend[3]. This implies that vitally smaller parameters can be utilized as a part of Elliptic Curve Cryptography than in other focused frameworks, for example, DSA furthermore, RSA yet with comparative security levels. The smaller key sizes with lessened and quick processing's in limited space, transmission capacity sparing and handling power makes Elliptic bend cryptography utilized as a part of different fields such as brilliant cards, portable telephones and so forth.. Agreeing to Zheng and Lionel an elective to RSA, elliptic bend cryptography will be another approach to open key cryptography [4]. The elliptic bend cryptography allows one to choose a mystery number as a private key which is then used to choose a point on a non mystery elliptic bend. A uncommon property of an elliptic bend will be that it powers both sides to figure a mystery key singularly taking into account its private key and other's open key. Elliptic bends are not comparable from oval. An elliptic bend will be the gathering of focuses in x-y arrangement to fulfill an comparison x^3+a6+a4x+a2 x^2=a1xy+a3y+y^2. This comparison will be additionally known as Weierstrass comparison which can be connected on genuine, sound, complex or limited field. Opposite to that Tilborg and Jajodia characterized that elliptic bend cryptography upgrades the investigation what's more, setup of open key cryptographic plans that can be created utilizing elliptic bends [5]. The elliptic bend plan analogs in view of the discrete logarithm issue where the basic bunch will be the accumulation of focuses on an elliptic bend characterized over a limited field. Stavroulakis and Stamp portrayed that elliptic bend cryptography improves utilizing the gathering of focuses on an elliptic bend as the fundamental number framework for open key cryptography . Elliptic bends are logarithmic structures that structure a essential class of cryptographic primitives which depend on a scientific hard issue. The elliptic bend discrete calculations issue will be construct in light of the recalcitrance of inferring an immense scalar after its increases with a given point on an elliptic bend Yalcin Elliptic Curve Cryptography Concurring to Tipton and Krause Elliptic Curve Cryptography execution is suitable for taking after reasons A. Versatility As RFID innovation needs more grounded and more grounded security with enormous keys, Elliptic bend cryptography can proceed with to offer the security with proportionately lesser extra framework assets. By actualizing Elliptic Curve Cryptography, RFID innovation able of offering higher security levels without expanding their costs.

D. B.Schneider transmission times and less memory The elliptic bend discrete logarithm issue calculation quality implies that solid security will be picked up with proportionately declaration sizes and smaller key. The smaller size of key thus implies that little memory is expected to store endorsements and keys and that less information must be passed between the tag and the per user so transmission times are shorter .The data is sending using public key which is randomly generating sends encrypted data from one server to another[2].

III. PROPOSED WORK

A. ENCRYPTION ALGORITHM

Step 1 Let's take a string B.

Step 2 Split this sting B into characters.

Step 3 Give a range for every character like for 'a' it should be 1-10,for 'b' it should be 11-20 etc.

Step 4 For every character a randomly number Will be generated .

Step 5 Replace particular string according to the number.(Every number associated with a string) i.e. if 156 selected then "Axsdw#4" will be used .

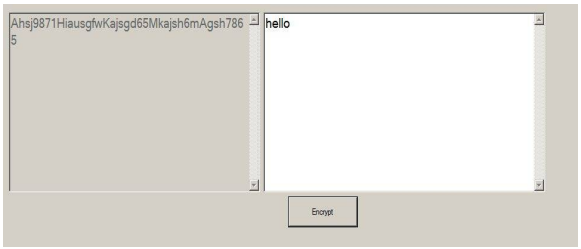

Fig.1 shows Encryption of the data.

We have encrypted "**amity**" keyword 10 times using encryption tool as the results are as follows:

1. Bhji090OJa5643waA10lpq03!qwadf$5asnxrqe342

2. Txc897Ui!jkas677Fgahsg09azsdxcn9asqw12$31

3 Bhji090OJa5643waFgahsg09Aqw123$5asqw12$31

4GhjU789lJa876*90asdqw75!Aqw123$5&^%!GAF

5 hjU789lJa5643wa0op912qwAqw123$5asnxrqe342

6.Poyr34BvKas543&6A10lpq03Aqw123$5adsrwe23 14%

7.XoPr128UKas543&6A10lpq03azxnmdklasnxrqe34 2$

8.Poyr34BvJa876*90asdqw75!Aqw123$5&^%!GAF RS

9. Poyr34Bv!jkas677A10lpq03Aqw123$5asnxrqe342

10.Plkj54CxKas543&6asdqw75!azsdxcn9&^%!GAF RS

Here we have found different results at tym of ency.

B. DECRYPTION ALGORITHM

Step 1: Replace Every String with number that associated with it.

Step 2: Now check the number and replace with appropriate character that belongs within a range.

Step 3: Now Integrated all the characters to form the actual message

Step 4:Show the Integrated Characters.

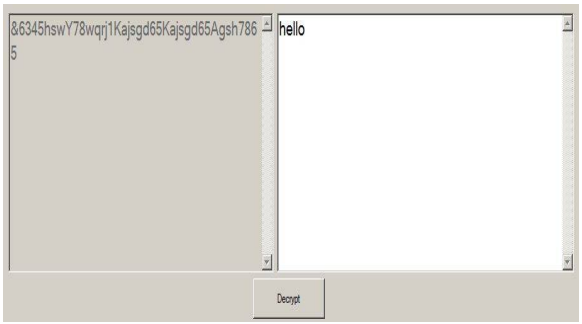

Fig. 2 shows Decryption of the data.

In the above algorithm we have described about encryption & decryption of data differently at the same time using Elliptic Curve Cryptography & Caesar Cipher Text.

Now we have compared our algorithm with Caesar Cipher and found our algorithm is more secure in comparison of Caesar cipher as our algorithm encrypting data differently at every time.

For encryption it is replacing 1 character at a time and that character is same as always but in our algorithm it is different always.

IV. CONCLUSION

Cryptography algorithm which using now a days providing security but with few limitations like saving memory and time. Our main focus is to develop such an algorithm which provides better security with limited power and memory. Elliptic Curve Cryptography working with finite fields.Every technique providing security but main focused is which provides the best results over the infinite fields without any dependencies. Elliptic Curve Cryptography is being used for Encryption and Decryption on networks but for finite fields. We have used the Elliptic Curve Cryptography concept working on finite field also. Elliptic Curve Cryptography saves memory but for finite fields. Here we are using Elliptic Curve Cryptography is the concept for Infinite fields but it is taking more memory. Encryption size of the data is dependent on the string size.

In future we will compare our algorithm with other different algorithms.

ACKNOWLEDGMENT

It is high privilege for me to express my deep sense of gratitude to Mr. Ashok K Chauhan who helped me by arranging the conferences and seminars which give me motivation.

V. REFERENCES

[1]Vivek Katiyar, Kamlesh Dutta, Syona Gupta, "A survey on Elliptic Curve Cryptography", IJCA Num-10 Article 8 in 2010.

[2]Schneider B. The secretary of security in IT Communications of the ACM, 47(10), 120-120. Retrieved August 2, 2008, from Academic Search Premier Database.

[3]Monika Sharma and P.C Agarwal . ECC Implementation for secured RFID communication, IJCSEE volume 2,Issue 1 (2014)

[4]Yalcin S, Radio Frequency Identification Security and Privacy Issues, Germany, p 3- 11,(2010)Springer.

[5]Tipton and M Krause , IT Security Management CRC Press, USA, 1064-1065, (2007).

About Authors:

1. Yogesh Anand Pursuing MCA from Amity University & done BCA from DAV Faridabad have knowledge about dot net technologies,oracle,database .

2. Assistant Professor (Grade II) & HVQ Coordinator at Amity University Noida and Research Scholar at Mewar University.

Qualification: (Pursuing PhD), MCA, MBA, Specialization: Wireless Security and Privacy, Software Engg., Operating System, Digital Electronics, Web designing.