A ROBUSTIC CRYPTOSYSTEM USING ASTROID CURVE OVER PRIME FIELD

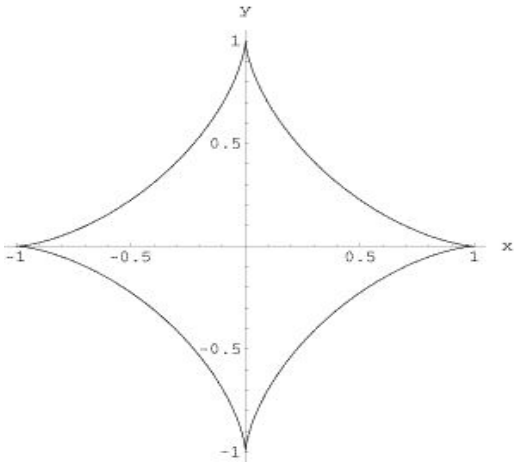
H.N.SHRUTHI, LINGARAJU.B.R, NEHA JAYAPRAKASH, VAIBHAVI.D.R, SMITHA SASI

***Abstract*— Public key cryptosystem or asymmetric cryptosystem has more security over the secret key cryptosystem or symmetric cryptosystem because this has a pair of keys which are mathematically related and are used at both sender and receiver end. In this paper we propose an efficient astroid curve over prime field. This public key cryptographic technique is used for secured data transmission and is highly reliable. This work includes encryption of the intelligent message at sender and the decryption of the unintelligent message at receiver end**

***Index Terms*— Sextic polynomial, Encryption, Decryption, Prime field, Public key, Private key, Cryptographic tool**

I. INTRODUCTION

In today's world secured data transmission remains challenging. The solution is to provide confidentiality of data during transmission through network security. Network security is the most important component in securing the information passed through the network computers. It includes both hardware and software functions The only one element which underlies all security mechanism in use is cryptographic techniques. Cryptographic techniques are crucial in establishing network security. Network security and cryptography is a mechanism to protect the network and to allow the secured data transmission over unreliable wireless networks. Network security involves authorization of access to the data in the network. Users are assigned an ID and password which gives them access to the data in the network. Cryptography is a study of secured data communication over the networks. Cryptographic algorithms can be segregated into symmetric key system and asymmetric key system. In symmetric key system common shared key is used for both encryption and decryption. A major drawback of this system is that both parties must exchange the key securely before initiation of data transmission. In public key system a pair of key is used which comprises of public key and private key where public key is used for encryption and private key is used for decryption. Public key is distributed and private key is never distributed. The major advantage of this system is improved security. In public key algorithms like RSA plain text is represented as integer number. In the proposed method plain text is represented as points of polynomial which reduces mathematical computations and complexity. So this paper proposes astroid curve over prime field cryptographic method.fig 1.shows astroid curve.



II. LITERATURE REVIEW

Rivest et al.[1]proposed a method to implement public key crypto system invented by Deffie Hellman where security lies message can be signed using privately held decryption key. This article motivated our paper since they not only presented public key cryptosystem but also digital signature. Prasant singh yadav et al[2] proposed how to implement the algorithm for security purposes and enhance the performance of this algorithm in the field of cryptosystem and network security.

This paper also proposes about the attacks against the algorithm. The main drawback of the RSA algorithm is the key size which could be overcome by the Elliptic Curve Cryptography.D.Sravana kumar et al[3] proposed a method for encryption of data using elliptic curve over finite field. This methods provides improved security at relatively low computational overhead. Each character is coded to a point on elliptic curve and each message point is encrypted as pair of points on elliptic curve. Asha rani misha et al[4] discuss about the different issues of wireless sensor network. Security is great challenge due to processing limitation of the sensor nodes and nature of wireless links. Security is implemented using software or hardware and is achieved using cryptographic methods and ECC is the best due to its key size. High security despite of smaller key which results in power efficient cryptosystem

Manuscript received May 17, 2015

H.N.SHRUTHI, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

LINGARAJU.B.R, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

NEHA JAYAPRAKASH, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

VAIBHAVI.D.R, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

SMITHA SASI, Associate Professor, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

III. PROPOSED WORK

Sextic polynomial is a polynomial of degree six and is also called as hexic polynomial. The general form of sextic equation is

$$y(x)=ax^6+bx^5+cx^4+dx^3+ex^2+fx+g.$$

where a is non zero and coefficients a,b,c,d,e,f,g may be integer or complex or real numbers.

Generate (x,y) points based on the equation and map characters on to the respective coordinate points.

ENCRYPTION

The sender starts the encryption with the plain text

Step 1:

Choose (pk1,pk2) as public key.

Step 2:

Choose (rk1,rk2) as reference key.

Step 3:

Corresponding coordinate points for the character in the plain text is chosen as (p1,p2)

Step 4:

Perform (p1,p2) /(pk1,pk2) mod (n^2-n+41) =(a,b) obtained by point division formula.

Where a=p1+n (pk1-p1) mod (n^2-n+41)

b=p2+n (pk2-p2) mod (n^2-n+41)

Step 5:

Perform (a,b) /(rk1,rk2) mod (n^2-n+41) = (c1,c2)

Where c1=a+n (rk1-a) mod (n2-n+41)

c2=b+n (rk2-b) mod (n2-n+41)

(c1,c2) is the encrypted data and is transmitted to the receiver end.

DECRYPTION

After receiving the encrypted data (c1,c2) the receiver starts performing decryption.

Step1:

Perform (c1,c2)(rk1,rk2) mod (n^2-n=41) =(a1,b1) obtained by point multiplication formula.

Where a1= (c1-nrk1)/(1-n)

b1=(c2-nrk2)/(1-n)

Step2:

Perform (a1,b1)/ (pr1,pr2) mod (n^2-n+41)= (p1,p2)

Where p1= a1+1/n(pr1-a1) mod (n^2-n+41)

P2=b1+1/n(pr2-b1) mod (n^2-n+41)

Relation between pk1 and pr1 is

Pr1=n [(b-n*pk1)/ (1-n) +b (1-n)/n] mod (n^2-n+41)

Relation between pk2 and pr2 is

Pr2=n [(a-n*pk2)/ (1-n) +a (1-n)/n] mod (n^2-n+41)

CONCLUSION

Astroid curve over prime field based cryptographic approach provides security and reduces computational complexity. This proposed algorithm is implemented using vb.net software tool. Encryption and decryption are done successfully and thus the results are verified . our proposed work can be used as cryptographic calculator which makes computations faster and is time efficient than the existing cryptographic methods such as RSA and ECC.

ACKNOWLEDGMENT

The successful completion of our project would remain incomplete without expressing our thankfulness to everyone who were a part of it. With a deep sense of deference, we acknowledge the help of our guide, Mrs.smitha sasi Asst. Prof., Dept. of TCE, DSCE, Bangalore, for her successful guidance, support, help and suggestions throughout. We would also like to extend our deep sense of gratitude to Dr A R Aswatha, Head of the Department of Telecommunication Engineering for his exemplary guidance, valuable suggestions, expert advice and encouragement. We take this opportunity in expressing our veneration to all those who directly or indirectly helped and encouraged us during the course of project.

REFERENCES

[1] R.Rivest, A.Shamir and L.Adleman "*A method for obtaining digital signatures and public key cryptosystems*", communication of the association for computing machinery , 1978, pp 120-126.

[2] Prasant Singh Yadav, Pankaj Sharma, Dr K. P Yadav, *" Implementation of rsa algorithm using elliptic curve algorithm for security and performance enhancement"* International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012

[3] D. Sravana Kumar, CH. Suneetha,A. ChandrasekhAR,"*encryption of data using elliptic curve over finite field"* International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[4] Asha Rani Mishra, Mahesh Singh, "*Elliptic Curve Cryptography for security in wireless sensor network"* International journal of engineering research and technology,vol.1-issue 3(may -2012).

[5] William Stallings, "*Cryptography and Network Security*",Principles and Practices, 3rd Edition, Prentice Hall 2003.

[6] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud "Performance evaluation of symmetric encryption algorithms" Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765

[7] Atul Kahate ―Cryptography and Network Security‖ 3rd edition.

[8] Asrjen K. Lenstra and Eric R. Verheul, "*Selecting Cryptographic key size*", Journal of Cryptology,2001, Volume-14, Number 4, pages 255-293.

[9] J. Edge, "*An introduction to elliptic curve cryptography"*, http://lwn.net/Articles/174127/, 2006.

[10] Alfred J. Menezes and Scott A. Vanstone, "*Elliptic Curve Cryptosystems and their implementations*", Journal of Cryptology, 1993, Volume-6, Number-4, pages 209-224.

[11] Vivek Kapoor, Vivek Sonny Abraham and Ramesh Singh, ―"*Elliptic Curve Cryptography*", ACM Ubiquity, vol. 0, Issue 20, May 20-26, 2008.

[12] Vishwa gupta, Gajendra Singh ,Ravindra Gupta,"*Advance cryptography algorithm for improving data security*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.