International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 5, May 2016

Survey Paper on: Elliptic Curve Cryptography

Tejaswini R M,
Assistant Professor,
GSSS Institute of Engineering & Technology for Women, Mysuru

Abstract: **Internet has become a main mode of communication in present era. The data used for communication is sensible and need to be protected from unauthorized users. Most of the devices used for communication are mobile/wireless devices that use ad-hoc or wireless network with low computational power, memory & limited bandwidth. Providing security to the data with lesser key size has become a challenging issue. Elliptic curve cryptography requires smaller key size and lesser computational power. This paper provides a brief introduction to elliptic curve cryptography and survey of various techniques used for encrypting the data using elliptic curve.**

I. INTRODUCTION

A specialized field in computer network involves securing a computer network. Cryptography is a science of providing security for information. Cryptography can be used to protect information and resources on both open & closed network. Cryptography originally aims at providing message secrecy through encryption. However, recently, the system is made capable to provide message integrity, authenticate the sender and prevent any repudiation. The objective of modern cryptosystems is not to provide perfect or risk-free security. Good cryptography-based security protects information until its value is significantly less than the cost of illicit attempts to obtain or tamper with the information.

Cryptography has three main objectives:

1. Confidentiality of the message: Only the authorized users must be able to decrypt the cipher.
2. Message Integrity: The receiver must be able to detect whether the message was altered during transmission.
3. Authentication of the sender: Receiver must be able to authenticate the sender of the message.

Basic Terms Used in Cryptography Encryption

A process of converting Plain Text into Cipher Text is called as **Encryption.** Cryptography uses the encryption technique to send the confidential information over an channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side. Encryption Algorithm is used to make content unreadable by all but the intended receivers.

Encrypt (plaintext,key) = ciphertext
Decrypt (ciphertext,key) = plaintext

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

II ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography is an approach to public key cryptography based on algebraic structure of elliptic curve. Elliptic Curve Cryptography uses smaller key compared to other cryptographic techniques.

III IMPLEMENTATION OF TEXT ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

In the classic method of elliptic curve cryptography the text is mapped on the elliptic curve for encryption. In this method the text is converted to the ASCII values, the ASCII values are paired up and a group is formed of the specific size. A single bit integer is assigned for each group and then the key is generated by taking the group id, private key of the sender, public key of the receiver. The cipher text is sent to the receiver. The receiver converts ASCII values to the required text, extract the plain text from the cipher text by applying the algorithm with the key generated.

As the mapping is done on the coordinates of the elliptic curve this method avoids sharing of a common lookup table between the sender and the receiver and saves

the bandwidth usage. This algorithm can work on any type of script. The algorithm generates different cipher text for same message so even if the attacker knows the encryption algorithm he will not be able to reveal the information because more than one plaintext cipher text pairs are formed with the secret key.

IV SECURED DATA TRANSMISSION USING ELLIPTIC CURVE CRYPTOGRAPHY

Cryptography techniques can be categorized into Symmetric, Asymmetric and key exchange. This scheme proposes a way to increase security consideration of the network using AODV (Adhoc-ondemand Distance Vector Routing) algorithm for transfer of data and to improve the efficiency of the AODV algorithms using elliptic curve cryptography.

AODV is a standard that controls how nodes decide which way to route the packets between computing devices in a mobile adhoc network. In adhoc network nodes do not know the network topology they have to discover it. The new node announces its presence and other nodes should listen for the announcement broadcast of its neighbours.

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad-hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

Ad hoc protocol can also be used as an improvised and often impromptu protocol established for a specific purpose. Table-driven (Pro-active) routing On Demand (Reactive) routing Hybrid (both pro-active and reactive) routing

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV is capable of both unicast and multicast routing.

V ELLIPTIC CURVE WITH MATRIX SCRAMBLING

In the world of communication network and gift era it is additional vital to secure line through that we will send and receive the info or we will communicate firmly over channel and keep information securely. Currently cryptography may be a methodology that protects information while we have a tendency to be transferring information from one network to another network. to stay safe information or avoid the disclosed data ancient and fashionable cryptography are used. There are some standard public-key secret writing algorithms that contain some advanced calculation, for instance ,RSA, ElGamal. Due to properties, options and characteristic of elliptic curve cryptography increased attention of the many skilled and scientists as a result of it have opened wealth potentialities in terms of security. Proposed a matrix scrambling algorithmic rule supported 2 way circular queues. Underneath this case, we have a tendency to introduce a new secret writing methodology on elliptic curve supported matrix Scrambling technique. This shows a new technique of encrypting information that permits smart diffusion and has a singular technique of decrypting it back to the plaintext and is straightforward to implement victimization matrix scrambling methodology that is predicated on random function and shifting. The selection of operation performed on rows or columns is predicated on Binary worth of prime no.

Encryption is done as follows the plaintext is remodeled on points of elliptic curve and therefore the corresponding code is organized into a circular queue system. Within the matrix M of n*m. The parameter p (Prime) represents the count of operations, say, the time of transformation we have a tendency to Created to matrix. The ECC methodology needs that we have a tendency to choose a random integer a, that has to be unbroken secret. Then base on the binary worth of prime circular shift is performed Let b=bit (rj), wherever j is bit position, the worth of b is considered and supported it circular left shift or circular right shift are performed on rows. Equally as rows, circular upward shift or circular downward shift are performed on columns.

Decryption process is done by reversing the Operations done in the encryption process. The cipher text is arranged into a matrix of n*m noted M.

VI CONCLUSION

This paper focuses mainly on the elliptic curve and the different application where the elliptic curve can be used for encryption and decryption. The advantages of encrypting the data by using elliptic curve are discussed.

REFERENCES

[1] J. J. Amador and R.W. Green, Symmetric-Key Block Cipher

[2] Image and Text Cryptography, International Journal of Imaging and Technology, Vol. 15, No. 3, pp. 178-188, 2005.

[3] Ting Liu, Member, IEEE, YangLiu, YashanMao, Yao Sun, XiaohongGuan, Fellow, IEEE, Weibo Gong, Fellow, IEEE, and Sheng Xiao "A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" IEEE Trans. Smart Grid vol. 5, no. 3, may 2014

[4] K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 643– 644, 2011

[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009

[6] L. Fengjun, L. Bo, and L. Peng, "Secure information aggregation for smart grids using homomorphic encryption," in Proc. 2010 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 327–332.

[7] R. Metke and R. L. Ekl, "Security technology for smart grid networks," IEEE Trans. Smart Grid, vol. 1, pp. 99–107, 2010

[8] W. Dapeng and Z. Chi, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 375–381, 2011

[9] H. Li, S. Gong, L. Lai, Z. Han, R. Q. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," IEEE Trans. Smart Grid, vol. 3, pp. 1540–1551, 2012.

[10] L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, pp. 1621–1631, 2012

[11] Y. Peizhong, A. Iwayemi, and Z. Chi, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," IEEE Trans. Smart Grid, vol. 2, pp. 110–120