International Journal of Computer Applications Technology and Research
Volume 5–Issue 10, 675-677, 2016, ISSN:-2319–8656

Literature Survey: Secure transmitting of data using RSA public key implemented with Vedic method

Mohit D. Singanjude
Dept. of Computer Engineering, MMCOE,
Savitribai Phule Pune University,Pune

Prof. R. Dalvi
Dept. of Computer Engineering, MMCOE,
Savitribai Phule Pune University,Pune

Abstract: In the military devices there is need to transmission of data security and fast. These proposed technique presents the secure, efficient and fast way to send images using Identity Based Cryptography and Visual Cryptography. In this application Identity Based Cryptography is used with Visual cryptography. In Identity based cryptography the RSA Cryptosystem is used to generate public and private key by using Ancient Indian Mathematics for fast mathematical calculation. RSA is the safest and standard algorithm. Vedic method is so efficient in multiplication terms of area, speed compered to its modern mathematics implementation. The regeneration of public/private key is adopted to make the system more secure from various attacks.

Keywords: MANET, RSA Cryptosystem, Vedic Mathematics, Modular Multiplication, Identity Based Cryptography, Visual Cryptography.

1 INTRODUCTION

Now a days data security is very important part of military devices. Also it needs to be work fast for sending and receiving secure data/images. In this paper we discuss the technique that secured, efficient and fast way to send images and data. Identity Based Cryptography and Visual Cryptography are used to encryption of data for secure transmission. This technique can be used in MANET specially for military surveillance. Visual Cryptographic technique, due to its simplicity and efficiency makes it the appropriate choice for sending and receiving images and finds use in transmitting encrypted images. In these techniques the private and public key pair is used to make system more secure. Identity based cryptographic technique represents a system having a solitary base station with numerous mobile nodes which is identical to that of Mobile Ad hoc Net-work (MANET). The steps of Identity based cryptography are adopted to set up the system and hence for encryption and decryption of data. The Indian Ancient Vedic mathematics is very popular for its tricky and fast performances to calculate the large prime numbers. Vedic mathematics has take less time compare to modern mathematics for calculation. In the RSA cryptography method has used by the modern mathematics to generate the public and private key. Here use Vedic mathematics techniques in RSA to generate the public and private key.

In this paper the technique of sending encrypted and decrypts data with efficient way. To improve the speed of RSA here uses the techniques of Ancient Vedic method for fast key generation.

2 MANET

Mobile Ad hoc Networks (MANETs) are multi hop wireless networks, in which nodes move and communicate with each other without any centralized control or base stations. Each node in MANETs acts as a source transmitting the data packets, as a destination receiving the packets transmitted by other source and also plays an additional role as a router, in routing the data packets which are destined to some other node. The applications of these networks are in battle field, disaster recovery and emergency rescue operations. In MANETs nodes are in mobile nature. Hence the topology of the network frequently changes. In recent years, it has received tremendous amount of attention from researchers, which led to the design and implementation of several routing protocols [2].

There are two variations of wireless mobile communications. The first one is known as infrastructure wireless networks, where the mobile node communicates with a base station that is located within its transmission range (one hop away from the base station). The second one is infrastructure less wireless network which is known as Mobile Ad hoc Networks (MANETs) [2].

Routing is defined as the process of finding path from a source to every destination in the network. There are three main requirements for designing ad hoc network routing protocols i.e. Low overhead, Adaptive and Resilience to loss. In case of low overhead, the routing protocol requires less number of control messages to transmit each data packet. Further the size of each control message is also very small. Hence it conserves bandwidth and battery. For adaptive, the routing protocol needs to be able to adapt to a highly dynamic environment in which topology and propagation conditions may vary significantly. For resilience to loss, the routing protocol needs to operate correctly and efficiently in the presence of packet loss. The packet loss in the ad hoc network environment is high, especially for multicast and broadcast packets.

3 VISUAL CRYPTOGRAPHY

Visual Cryptography was pioneered by Moni Naor and Adi Shamir in 1994. Encryption protected our data but key use for encryption it not be protected. Hence he introduce the concept of secrete share. They come up with a visual secret sharing scheme, where an image is divided or broken up into n shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can reveal no information about the original image [2]. Each share is printed on a separate transparency and decryption is performed by overlaying the shares when all n shares are overlaid, the original image gets appeared. Visual Cryptographic is one of the new techniques which provide information security and uses the simple algorithm unlike the complex one used in other traditional cryptography. This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex computation or algorithms.

Visual cryptography needs only the characteristics of human vision to decode the encoded images. It does not need any cryptographic knowledge or any kind of complex computation to decode the encoded image. Mainly this visual cryptography focuses on the security aspects to safeguard the secret image from two or more cover images so that any attacker cannot retrieve any data. Visual secret sharing schemes hide the secret image into several share images and distribute these share images to participants. With no computation, human beings are able to obtain the secret image by stacking the share images [5].

4 IDENTITY-BASED CRYPTOGRAPHY

In 1984, Shamir proposed a concept of identity-based cryptography. Here user use identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users certificates. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components. Before secure communications can take place, both sender and receiver must generate encryption and signature key pairs, submit certificate requests along with proof of identity to a Certificate Authority (CA), and receive CA-signed certificates, which they can then use to authenticate one another and exchange encrypted messages.

Here we discuss for the Identity based encryption and Identity based signature

A. Identity based signature

As mentioned earlier, in the IBE scheme, the sender can use the receiver’s identifier information which is represented by any string, such email address, IP addresses, social security number, a photo, a phone number, postal address etc., to encrypt a message. The receiver, having obtained a private key associated with his identity information from trusted third party called the Private Key Generator (PKG)”, can decrypt the cipher-text

B. Identity based signature.

As a mirror image of the above identity-based encryption, one can consider an identity-based the signature (IBS) scheme. In this scheme, the signer sender first obtains a signing (private) key associated with his identifier information from the PKG He then signs a message using the signing key. The verifier receiver now uses sender identifier information to verify receiver signature [6].

5 THE RSA ALGORITHM

The RSA algorithm was publicly described in 1977, the letters RSA are the initials of their surnames (RivestShamirAdleman). RSA is asymmetric key encryption technique and it is most versatile and widely used public key algorithm today RSA depends on the modular exponentiation of long integers. Regeneration of public/private keys of the complete system takes place ensuring more effective data security. Therefore, fast modular multiplication becomes the key to real-time encryption and decryption since a high throughput is needed in data communication [3]. The RSA is the most widely deployed public-key cryptosystem and is used for both encryption and digital signature. It is commonly used in securing ecommerce and e-mail, implementing virtual private networks and providing authenticity of electronic documents. It is implemented in most Web servers and browsers, and present in most commercially available security products. In fact, the ubiquity of RSA has placed it at the heart of modern information security. It would not be an overstatement to say that Internet security relies heavily on the security properties of the RSA cryptosystem [1].

The Sanskrit word ’Veda’ means ’knowledge’. The Vedas consist of a huge number of documents there are said to be thousands of such documents in India, many of which have not yet been translated, which are shown to be highly structured, both within themselves and in relation to each other. Vedic Mathematics is based on 16 sutras dealing with mathematics related to arithmetic, algebra, and geometry. Here mainly use Urdhva Tiryakbhyam method of Vedic multiplication it also called vertical and crosswise multiplication. Application of the Sutras improves the computational skills of the learners in a wide area of problems, ensuring both speed and accuracy, strictly based on rational and logical reasoning. Vedic methods are direct, and truly extraordinary in their efficiency and simplicity [3].

6 CONCLUSION

In this paper we describe the techniques for secure and fast transmission of data in MANET. Indian Ancient Vedic method is known for its performance. The Vedic method is very helpful to increases the speed of RSA to generate the public and private keys. The RSA is so secured as compare to other cryptography techniques. In the MANET there is need to refreshing key simultaneously so these methods will help to improve the performance of MANET.

7 ACKNOWLEDGMENTS

I am profoundly grateful to Prof. R. Dalvi, Computer Engineering Department for her expert guidance and continuous encouragement throughout to this research.

Also I must express my sincere heartfelt gratitude to all staff members of Computer Engineering Department and my family and friends who helped me directly or indirectly during this course of work.

8. REFERENCES

[1] Kumaravel, Ramalatha Marimuthu, VLSI Implementation of High Performance RSA Algorithm Using Vedic Mathematics, International Conference on Computational Intelligence and Multimedia Applications 2007.

[2] R. K. Sharma, Neeraj Kishore, Parijat Das, Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique, International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 3 Issue 2 February, 2014.

[3] Shahina M. Salim, Sonal A. Lakhotiya, Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013)Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] S. P. Pohokar, R. S. Sisal, K. M. Gaikwad, M. M. Patil, Rushikesh Borse, Design and Implementation of 16 x 16 Multiplier Using Vedic Mathematics, 2015 International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May 28-30, 2010

[5] Ms. Bhawna Shrivas, Prof. Shweta Yadav, A Survey on Visual Cryptography Techniques and their Applications, hawna Shrivasetal, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1076-1079

[6] Jaydipsinh B. Jadeja, HarikrishnaJethva, Bhadreshsinh G. Gohil Secure Transaction System Using ID Based Cryptography, Jaydipsinh B. Jadejaetal, International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 12, December

[7] G. Ganesh Kumar, V. Charishma Design of High Speed Vedic Multiplier using Vedic Mathematics Techniques, International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012.

[8] Sriraman, L. Dept. of Electron. Commun. Eng., Oxford Eng. Coll., Trichy, India; Kumar, K.S.; Prabakar, T.N.,Design and FPGA implementation of binary squarer using Vedic

[9] Jiawei Han, Micheline Kamber, Jian Pei, Data Mining : Concepts and Techniques : Concepts and Techniques (2nd Edition)