I.J. Information Engineering and Electronic Business, 2012, 2, 36-42
Published Online April 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2012.02.06

Secure Communication using Symmetric and Asymmetric Cryptographic Techniques

Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik , MV Ramana Murthy
Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia
Email: obarukab@kau.edu.sa, aikhan@kau.edu.sa, smsharief@hotmail.com, mv.rm50@gmail.com
And
Shahid Ali Khan
Department of Computer Science & Engg.
Waljat College of Applied Sciences, Oman
Email: shahid.ak1@gmail.com

***Abstract*—**Satellite based communication is a way to transmit digital information from one geographic location to another by utilizing satellites. Satellite as communication medium to transfer data vulnerable various types of information security threat, and require a novel methodology for safe and secure data transmission over satellite. In this paper a methodology is proposed to ensure safe and secured transferred of data or information for satellite based communication using symmetric and asymmetric Cryptographic techniques.

***Index Terms*—** Satellite based communication, Information security , Encryption, Cryptographic Algorithms

I. INTRODUCTION

Information security has it's own importance right from the early days of computing. As the technology is advancing, organizations also employing latest electronic equipments like satellite based communication, high end servers for information storage and data transmission. Most of the organizations preserve the data in electronic form. Satellite based communication is used for transmission of data over different geographical location, to ensure information security from different kind of threats an improved process is required.

Satellite based communication is a way to transmit digital information from one geographic location to another. Encryption process is helpful in ensuring certain security features like confidentiality, integrity, authentication and identification of data. For achieving the above mentioned features, combination of suitable cryptographic algorithms is essential.

To meet the present requirements, a methodology is proposed that comprises symmetric and asymmetric encryption techniques. The rest of the paper is organized as follows: sections II related work section III described briefly encryption and its present categories section IV About cryptographic algorithms and it's implementation to the present requirement and section 4.Described the proposed methodology.

II. Related Works

The author [1] developed a scheme Dual-RSA using Chinese Remainder Theorem (CRT) for its Decryption that improved roughly ¼ times faster performance of RSA in terms of computation cost and memory storage requirements [1].

The authors [2] give solution for security and privacy issues in Radio Frequency Identification Device (RFID) system using symmetric authentication. The main part of this work is a novel approach of an AES hardware implementation which encrypts a 128-bit block of data within 1000 clock cycles and has a power consumption below 9 A on a 0.35 m CMOS process [2].

The author [3] proposed scheme for privacy preserving RFID tags in which security and privacy of the user is secured in terms of time and space complexity with efficient communication cost involved in searching one tag among N tag. Support for mutual authentication between reader and tag with no information leakage [3].

Steganography make the presence of secret data appear invisible to eaves droppers such as key loggers or harmful tracking cookies where the users keystroke is monitored while entering password and personal information. The Steganography is used for secret data transmission. Steganography is derived from the Greek word steganos which means “covered” and graphia which means “writing”, therefore Steganography means “covered writing”. In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc. The steganography method provides embedded data in an imperceptible manner with high payload capacity. Encrypting data provides data confidentiality, authentication, and data integrity. [4]

Steganography is a powerful tool which increases security in data transferring and archiving. In the case of Steganography the confidential data is first encapsulated within another object which is called “cover object”, to form “stego object” and then this new object can be transmitted or saved. It causes the existence of the confidential data and even its transmission becomes secure and safe [5].

Signcryption proposed by Zheng [6] at Crypto'97 is a public key or asymmetric cryptographic method that provides simultaneously both message confidentiality and unforgeability at a lower computational and communication overhead than doing signature and public key encryption separately. Recent progress in the security analysis of signcryption indicates that the specific instantiations of signcryption demonstrated in [6] are indeed secure in a very strong sense. More specifically, it has been proven in [7][8] that these schemes are secure against adaptive chosen ciphertext attacks and existentially unforgeable against adaptive chosen message attacks, both in the random oracle model, relative to Gap Diffie-Hellman and Strong Discrete Logarithm problems respectively.

It should be emphasized that the signcryption schemes could be proven secure without any significant changes of the schemes. However to simplify analysis, [7][8] modified the original schemes slightly by introducing an extra one-way hashing into the signcryption and unsigncryption operations.

III. Modern Encryption and its Categories

Encryption means protecting data in such a way that while it transmitted, it should not be intercepted by anyone except the one who known how to transform it

back. Transmitting the data evolved data to travel across several un-trusted communication channels. It is a must to encrypt the data to be secure across all communication channels. There are three broad categories of encryption.

(a) Symmetric encryption

In this encryption technique as shown in figure 1 a single long random string of bytes is mathematically generated as a key to encrypt the information, this key is required by receiving party to retrieve the information, in other words both (sender and receiver) party must have this key to encrypt and decrypt the information, which some time not sufficient [9].

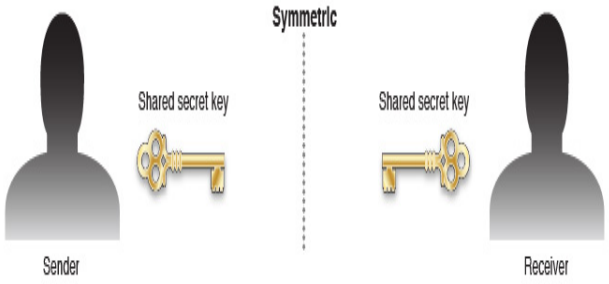

Figure 1: Symmetric encryption [9]

(b) A Symmetric Encryption

Asymmetric encryption also knows as public-key encryption is more complex and more secure, it uses private and public key concept to encrypt and decrypt information. Two related mathematically generated keys are used to transform information in encrypted form, one key is used to encrypt and the other key is used to decrypt and vice versa as shown in figure 2. Generally private key is used as secret key and public key is broadly available [9]. Suppose party 1 want to send encrypted information so they encrypt the information using their public key and public key is available to anyone who might want to send encrypted information. Public key can only encode data; it cannot decode it. Private Key stays safe with party 1. When the other party whom the message sent received the encrypted information, which is also known as ciphertext, decrypt it with their private key [10].

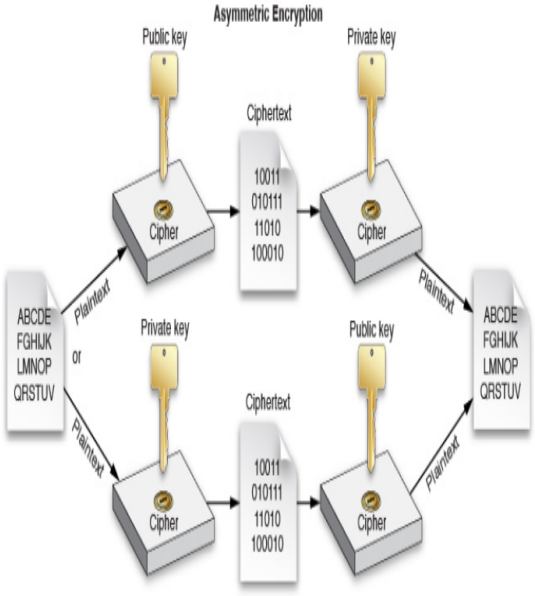

Figure 2: Asymmetric encryption [9]

(c) Steganography

Steganography is the technique of hiding confidential information within any media such as [picture, audio, video, text] etc, as show in figure 3. Steganography is mainly used for storing copyright information. The main purpose of steganography is to hide some secret information within a media in such a way that no one can recognize the presence of the hidden message in that media.

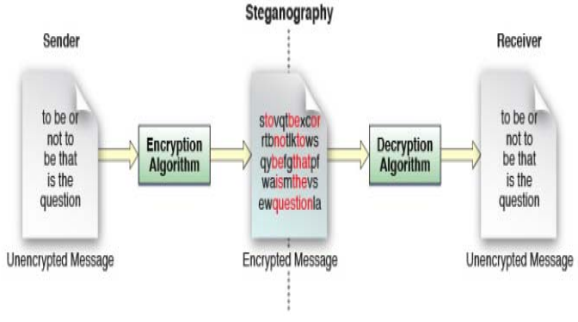

Figure 3: Steganography encryption [9]

IV. About Cryptographic Algorithms

Presently there are two types of cryptographic algorithms available for encryption/decryption process

[11]. In symmetric cryptographic systems a single key (a secret key) is shared for sender and recipient. Even these algorithms are more efficient (in terms of speed of encryption process), key management is difficult in real environment [12]. Further secured key distribution is one of the critical issues.

To overcome these problems, symmetric cryptographic algorithms are utilized [13]. These algorithms utilize a single key pair of public and private keys, which are related mathematically and a private key can't be derived from public key. Symmetric key algorithms are considered as quickest and most commonly used for encryption. Any information or a message, encrypted by a public key is decrypted only with the corresponding private key [14]. 3DES and AES symmetric encryption algorithms are the most widely used algorithms.

Asymmetric cryptographic algorithms depends on very large number based computation, encryption/decryption process is not as efficient as symmetric cryptographic algorithms and considered as slow algorithm. Following are the key properties of the proposed scheme.

(a) Confidentiality

Communication from one end to other should be secured against any kind of tapping in the network. To achieve confidentiality symmetric cryptographic algorithms is proposed, Symmetric cryptographic systems are popular for high speed encryption and low cipher expansion rate, comparing to asymmetric crypto systems. In this software package secured key transformation is achieved useing asymmetric cryptographic algorithm [16].

(b) Integrity

Tampering the information in the network is one of the critical threats. This problem can be identified, by utilization of message digest algorithm. Message digest algorithm is a one way hashing function gives a fixed size of hash value for variable length of messages. Comparison of hash values, both sides (sender and recipient) ensure information integrity.

(c) Authentication & Identification

Digital signature provides assurance for validity of origin of the information. This feature can be achieved by implementing asymmetric cryptographic algorithm with the combination of hashing algorithm [17].

V. PROPOSED SCHEME

In the proposed scheme, following algorithms are used for secured communication.

IDEA (International data encryption algorithm (utilizes 128 bits key)

RSA (1024 bit Asymmetric algorithm)

MD5 (Message Digest Algorithm gives 128 bits hash)

Following steps are used to achieve information confidentiality, authentication and integrity.

(a) Sender's side process

Sender generates a 128 bit hash value of a message, by using MD5. Hash value is encrypted with the sender's private key by using RSA. A digital signature is created and it is concatenated to the message (Mc).

Sender chooses a random 128 bit session key and encrypts the message with the session key by using IDEA. Session key is encrypted with the recipient's public key and the result is concatenated to Mc and this result is sent as a cipher text to the recipient.

(b) Recipient side process

Recipient decrypts part of the cipher message with his private key by using RSA, to obtain session key. Remaining part of the cipher message is decrypted with the session key by using IDEA, result has two parts, digital signature and message parts. Recipient generates hash value of the message by using MD5. Recipient decrypts the digital signature with sender's public key by using RSA. Further a hash value is generated from the result by using MD5. Recipient compares the two hashes values obtained from step 3 and step4. The following diagrams (Figure 4 and Figure 5) depict the way that a message is processed at sender and receiver's end.

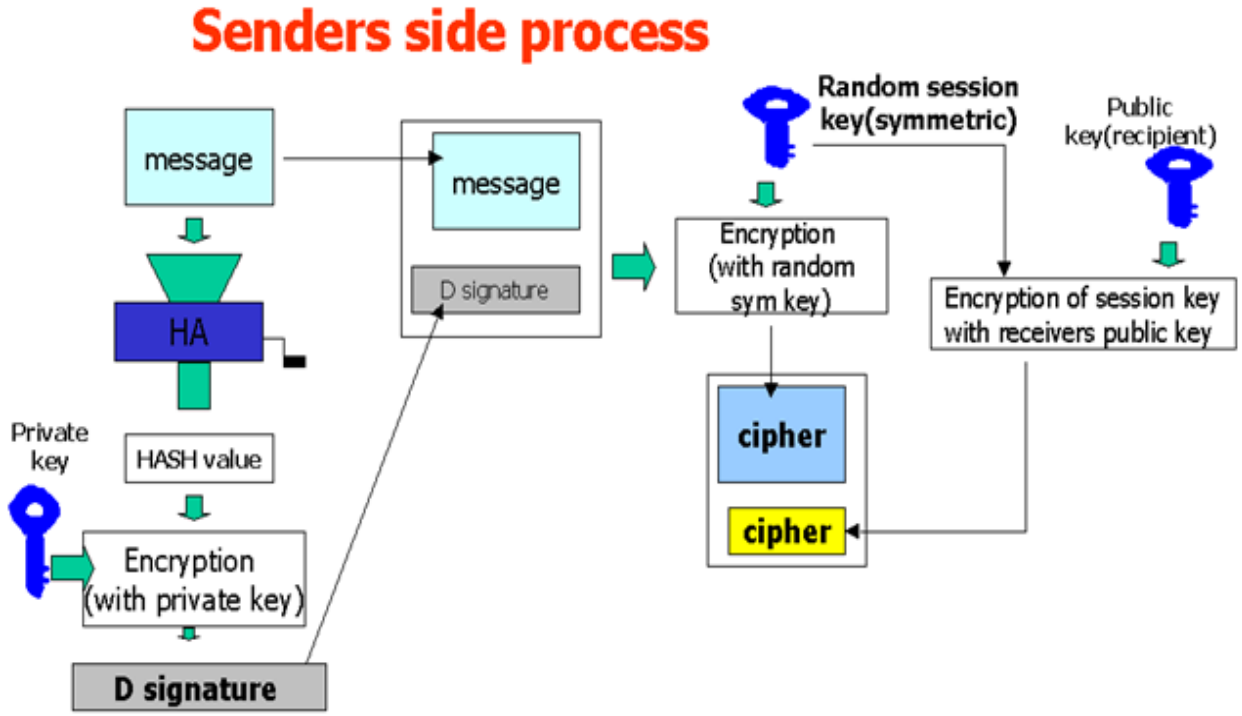

Figure 4: Sender side Process

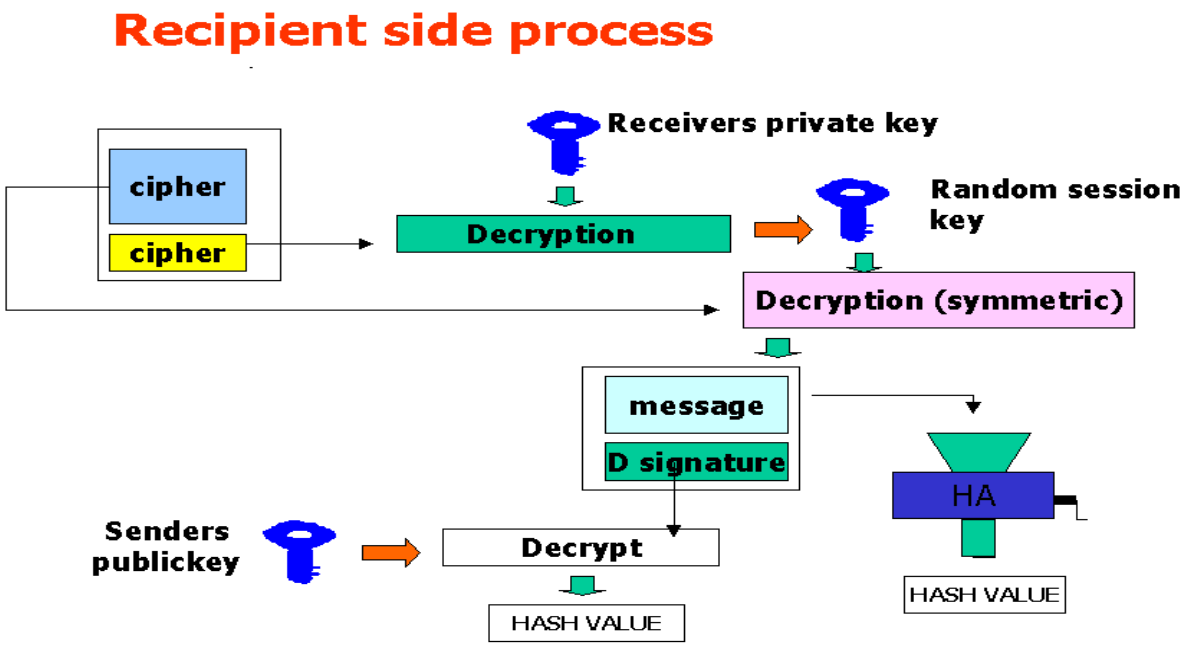

Figure 5: Recipient side process

VI. Conclusion

In this paper a cryptographic scheme that comprises symmetric and asymmetric algorithms is proposed for securing safe data transmission via satellite based communication channel. Java programming language is used to develop software based on this scheme. Results show that by utilizing strong cryptographic algorithms, this software ensures, information confidentiality, integrity and information authentication, which are the essential features for information security in a satellite based communication.

References

[1] s. Subasree and N. K. Sakthivel,, "Design of a new security protocol using hybrid cryptography algorithms", IJRRAS, vol. 2, 2010.

[2] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. Workshop on Cryptographic Hardware and Embedded Syst., M. Joye and J.-J. Quisquater, Eds. New York: Springer-Verlag, 2004, vol. 3156, Lecture Notes in Computer Science, pp. 357–370.

[3] Eun-Kyung Ryu, Tsuyoshi Takagi, "A hybrid approach for privacy-preserving RFID tags",Computer Standards & Interfaces, Elsevier, 31, pp. 812–815, 2010.

[4] H. S. Majunatha Reddy, & K B Raja, "HIGH CAPACITY AND SECURITY STEGANOGRAPHY USINGDISCRETE WAVELET TRANSFORM", International Journal of Computer Science and Security (IJCSS), Vol. 3: Issue (6) pp 462-472.

[5] Md. S. Khan, M V. V. Bhaskar, M V S. Nagaraju, "An Optimized Method for Concealing Data using Audio Steganography", International Journal of Computer Applications (0975 – 8887) Vol. 33– No.4, pp 25-30. 2011

[6] J. Baek, R. Steinfeld and Y. Zheng, "*Formal Proofs for the Security of Signcryption*", Proc. PKC , Vol. 2274 of LNCS, Springer- Verlag, pp 80-98, 2002.

[7] J. Baek, R. Steinfeld and Y. Zheng," *Formal Proofs for the Security of Signcryption*", a full version, submitted to Journal of Cryptology. A draft is available upon request to the authors.

[8] J. Baek and Y. Zheng, "Description of Provably Secure Signcryption Schemes", Retrieved on 21-03-2012 from http://www.signcryption.org/publications/pdffiles/yz-baek-sc-description-02.pdf, Aug 2002.

[9] Mac OS X Developer Library, "Security Overview", Retrieved on March 18th 2012 from, http://developer.apple.com/library/mac/#documentation/Security/Conceptual/Security_Overview/CryptographicServices/CryptographicServices.html

[10] A. Brandt and A. Krasne, "How It Works: Encryption hides your data from prying eyes. Learn how it works and what you need to use it", Retrieved on March 18th 2012 from, http://www.pcworld.com/article/15230/how_it_works_encryption.html

[11] Singh , S. Code "The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography", Doubleday, 1999

[12] Schneier B.,"Applied Cryptography", John Wiley New York

[13] Andrew s Tanebbaum, computer Networks, Third edition, Prentice-Hal inc, New Delhi, India 1999

[14] Stallings, W, "Cryptography and Network Security: Principles and practice", 2nd edition, prentice hall

[15] Diffe,W , Hellman, M , "New directions in cryptography", IEEE Trans, inform. Theory, 1996

[16] RL,Rivest et al , "A method for obtaining digital signatures and public-key crypto systems", 2000

[17] Rabin, M, "Probabilistic algorithms, In Algorithms and complexity", Academic Press, New York, 1986.

Authors Bibliography

Dr. Omar Mohammed Barukab is working as Assistant Professor, Department of Information Technology, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University. Dr. Omar got PhD degree in the year 1999 in Computer Engineering from College of Engineering, Florida Institute of Technology. His area of research interest is Information security.

Mr. Asif Irshad Khan received his Bachelor and Master degree in Computer Science from the Aligarh Muslim University (A.M.U), Aligarh, India in 1998 and 2001 respectively. He is presently working as a Lecturer Computer Science at the Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia. He has more than seven years experience of teaching as lecturer to graduate and undergraduate students in different universities and worked for four years in industry

before joining academia full time. He has published six research publications and his research interest includes Software Engineering, Component Based Software Engineering and Agent Based Software Engineering.

Mr. Mahaboob Sharief Shaik received his Bachelor and Master degree in Computer Science from the Osmania University, India. He is presently working as a Lecturer Computer Science at the Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia. He has more than ten years experience of teaching as lecturer to graduate and undergraduate students in different universities. His area of research interest is Database and Information security.

Prof. MV Ramana Murthy is working as a full professor in the Department of Computer Science, King Abdul Aziz University, Rabigh, KSA.

Mr. Shahid Ali Khan received his Bachelor and Master degree in Computer Science from the Aligarh Muslim University (A.M.U), Aligarh, India. He is presently working as a Senior Lecturer Department of Computer Science & Engg., Waljat College of Applied Sciences, Oman. He has more than twelve years experience of teaching as lecturer to graduate and undergraduate students in different universities. His area of research interest is Database and Information security.

