International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

Design of Hybrid Cryptography Algorithm for Secure Communication

Arpit Agrawal[1], Gunjan Patankar [2]

[1] *Lecturer, Computer Engineering, Institute of Engineering & Technology Devi Ahilya University Indore, Madhya Pradesh, India*

[2] *Student, Computer Engineering, Institute of Engineering & Technology Devi Ahilya University Indore, Madhya Pradesh,India*

Abstract - *Secure Communication in remote access is expected in server – client architecture and pear to pear devices. In-secure transmission may lead to leak sensitive credentials and information. Strong security policies are required to provide proper level of security policies to achieve confidentiality, authentication and integrity. To maintain confidentiality, Digital Envelope, which is the combination of the encrypted message and signature with the encrypted symmetric key, is also used. This research paper proposed a hybrid model to achieve confidentiality, authentication and integrity in same manner..*

Key Words: *Hybrid Secure Communication, Symmetric Key, Asymmetric Key*

1. INTRODUCTION

We ask that authors follow some simple guidelines. This document is a template. An electronic copy can be downloaded from the journal website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website

Cryptography is the ability to send information between participants in a way that prevents others from reading it. It plays a crucial role for data protection within applications of public networks. Several important desktop computing applications have emerged in recent years that use an Internet-scale decentralized architecture to simultaneously connect millions of users to share content, form social groups and communicate with their contacts. These applications are classified as peer-to-peer because of the elimination of servers to mediate between end systems on which the applications run, and their network behavior is described as An overlay network because the peer protocols form a virtualized network over the physical network.

The study of conventional system concludes that there is big scope of improvement in security policy of highly security expected applications.

To understand and develop a hybrid and secure security model work consider few security algorithms which are listed below;

Following algorithm will be used to develop hybrid security model.

1. Diffie-Hellman Key Exchange Algorithm
2. RSA algorithm for Confidentiality
3. Private Key Encryption for Authentication
4. SHA-1 for Integrity
5. RC5 to provide confidentiality over cipher text and message digest

2. RELATED WORK

Chauhan [1] present that hybrid cryptography is better approach to maintain confidentiality and privacy of information during communication. They also proposed a hybrid algorithm for strong encryption. They state that there are various algorithms are available for cryptography but all of them have certain drawbacks. Proposed algorithm is designed with combination of two symmetric algorithm techniques known as AES and DES. Proposed solution is implemented using 128 bit keys. Proposed solution is implemented using java technology. Here, they provide facility to select security algorithm as per requirement which may be AES, DES or hybrid algorithm. The complete work concludes that possibility of an algebraic attack on hybrid model is too poor and gives strong strength to encryption approach.

Shankar [2] address that RSA is one of the most common algorithm for encryption and decryption. Subsequently, Round-robin scheduling is one of the most common useful algorithms for task scheduling and processing. Authors proposed a technique to integrate RSAA algorithm with Round robin scheduling algorithm to extend level of

security. In this approach method uses RSA algorithm to generate cipher text based on priority. Receiver receive message and decrypt the message according to priority. Proposed method reduces probability of man-in-middle attack and timing attack.

Subasree[3] explore that computer network is an group of interconnected nodes. Various security threats attempt to compromise the network security and modify the content of packet. Confidentiality, authentication and integrity are the most crucial security principle used to maintain level of security. It requires the certain security algorithms to maintain security and maintain communication private. Proposed.

algorithm integrates Elliptic Curve Cryptography, Dual RSA algorithm and Message Digest MD5. This new security protocol has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

Tianfu [4] address that internet is one of the most unsafe communication medium due to huge connection and public network. Information protection is one the of essential requirement. At present various security algorithms are proposed to achieve security during communication. All of them have certain good point and certain bad point. To improve the strength of encryption algorithm they proposed a hybrid model. Proposed model is combination of AES and DES. Both algorithms are symmetric key technique and itself they are very much capable for encryption. Integration of AES and DES would give a strong level of security at encryption end. A significant improvement in results has been observed with proposed solution.

3. SECURITY ISSUES

Cryptography technique helps to achieve security during communication. The major problem with existing solution is they can't provide common security requirement into single solution. Confidentiality is required to provide privacy and isolation for information where authentication is used to verify proof of identity. In PKI encryption and decryption perform with different key where private key is non-sharable entity. As per the Asymmetric Key Cryptography if we encrypt the message with private key, anyone can decrypt the message by using its public key. Here, we can achieve authentication but cannot maintain the confidentiality. Furthermore, if wee encrypt the message by public key, only intended recipient can decrypt the message. It helps to maintain the confidentiality but cannot authorize sender. To overcome the above problem we use to perform public key encryption after private key. So, only intended receiver would be able to decrypt the message and also authentic the sender by decrypting the received cipher message with public key. Subsequently, there is a procedure to maintain authentication and confidentiality by implementation digital envelop for communication.

RSA governs the application of cryptography to data for digital envelopes and digital signatures. A digital envelope uses two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

Either of the following methods may be used to create a digital envelope:

Secret key encryption algorithms such as Rijndael or Twofish are used for message encryption. Furthermore, Public key encryption algorithm is known as RSA is used for secret key encryption with a receiver's public key.

A digital envelop may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data. An example of a digital envelope is Pretty Good Privacy

(PGP) - popular data cryptography software that also provides cryptographic privacy and data communication authentication. A digital envelope is also known as a digital wrapper. The complete study explore that, there is no procedure to maintain integrity of message. So, proposed algorithm will not only help to achieve confidentiality and authentication but integrity too.

4. PROPOSED SOLUTION

A method of encryption that combines two or more encryption schemes and includes a combination of symmetric and asymmetric encryption to take advantage of the strengths of each type of encryption is known as Hybrid Encryption.

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or

there may be a simple transformation to go between the two keys.

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

In cases where the same algorithm is used to encrypt and decrypt, such as in RSA, a message can be securely signed by a specific sender: if the sender encrypts the message using their private key, then the message can be decrypted only using that sender's public key, authenticating the sender.

The proposed solutions will not only give a way to establish secure communication but it will also help to improve level of encryption by reducing security overhead. System does not require any external system interface for development. Graphical user interface (GUI) will be used to interact with user. User will supply input through text box and file form from the user view and forward to show output at receiver end. A Bluetooth connection or wired network is required between sender and receiver computer for communication. Socket programming will be used to establish communication between sender and receiver.

5. HYBRID MODEL

There is no special memory requirement of proposed solution. A basic memory requirement of java application is recommended. Encryption and Decryption will be the leading operations of proposed solution. Subsequently, calculation of SHA-1[MAC] and SHA-1[MAC] verification process is also

important to establish strong integrity and authentication approach. A basic architecture of proposed system is shown in below Figure 5.1 Encryption & 5.2 Decryption.

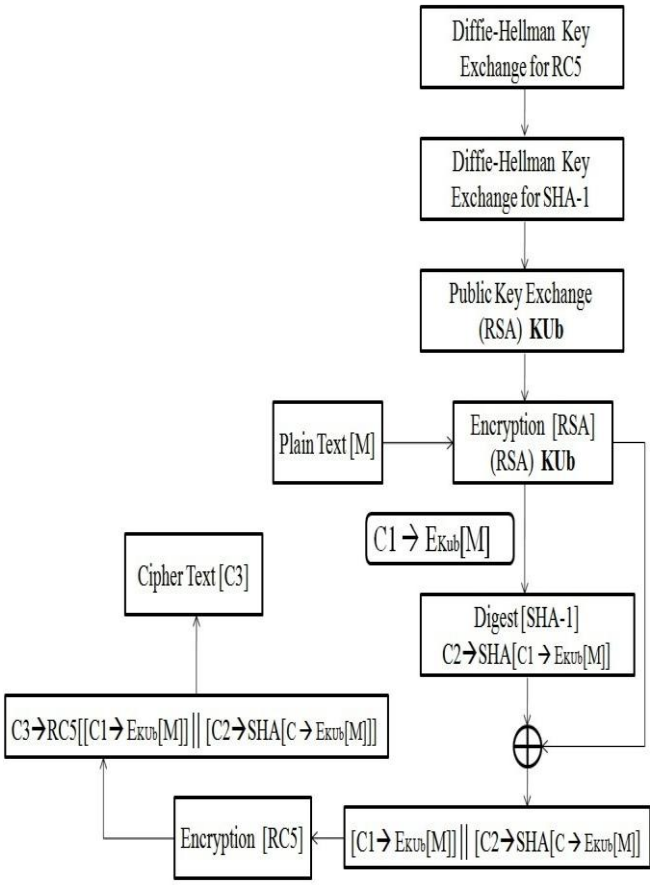

Figure 5.1 Proposed Encryption Algorithm's Architecture

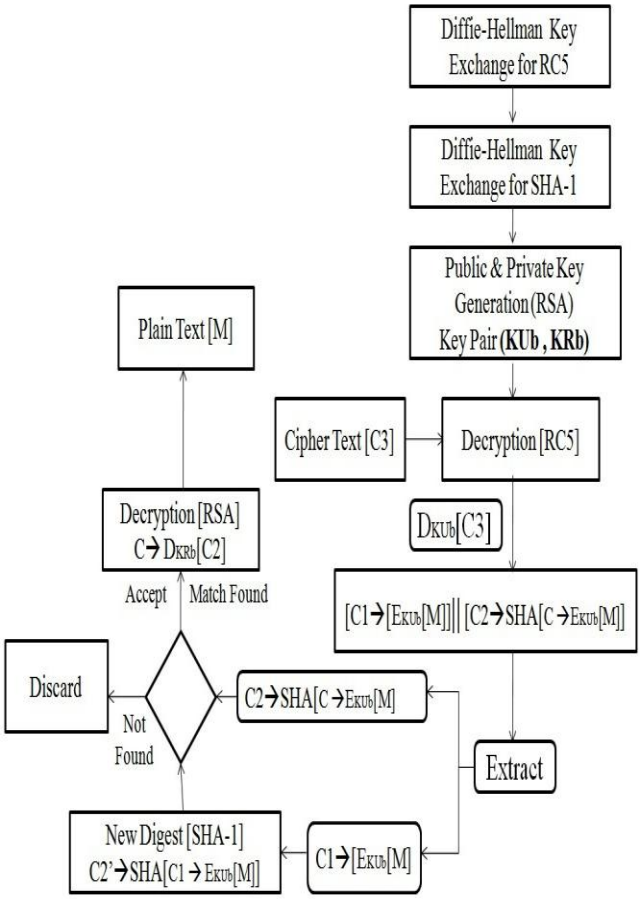

Figure 5.2 Proposed Decryption Algorithm's Architecture

This research work proposes an efficient technique to encrypt and decrypt plain text to keep information safe and secure from unwanted user interaction. It combines symmetric and asymmetric key cryptography algorithm to increase the strength of encryption process. Furthermore, encryption with private key in RSA will help to achieve authentication about sender. Subsequently, SHA-1 algorithm has been used to maintain integrity of content. Following security algorithms are used to achieve safe and secure communication.

6. CONCLUSION

The complete work concludes that proposed solution will give an alternative security model than SSL and digital envelop to maintain security in intranet. SSL require HTTPs protocol, where proposed solution does not require any kind of protocol

involvement in applications. Furthermore, the basic application of proposed solution is integration of security policy with local network based applications. It may helpful in such applications where privacy, authentication and integrity, all are primary demands.

7. REFERENCES

[1] Jigar Chauhan , Neekhil Dedhia, Bhagyashri Kulkarni , International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013. Enhancing Data Security by using Hybrid Cryptographic Algorithm.

[2] Meenakshi Shankar and Akshaya.P , International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014. Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts.

[3] S. Subasree and N. K. Sakthivel , IJRRAS 2 (2), February 2010. Design of A New Security Protocol Using Hybrid Cryptography Algorithms.

[4] Wang Tianfu, K. Ramesh Babu, International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283. Design of a Hybrid Cryptographic Algorithm.

[5] U.S. Department Of Commerce, National Institute Of Standards And Technology: Advance Encryption Standard (Aes).

[6] U.S. Department Of Commerce, William M. Daley, Secretary National Institute Of Standards And Technology, Raymond G. Kammer, Director: Data Encryption Standard (Des).