Policy for Secure Communication using Hybrid Encryption Algorithm

Amrita Jain
Department of Information Technology
IET DAVV, Indore

Vivek Kapoor
Department of Information Technology
IET DAVV, Indore

ABSTRACT

Secure communication in network environment is primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and e-commerce transactions, digital signatures using public key cryptography is extensively employed. 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 has proposed to develop a hybrid technique using Symmetric & Asymmetric key cryptography. It will also include Message authentication code to maintain integrity of message. Therefore, proposed model will not only help to maintain confidentiality and authentication of message and user but integrity of data too. Java technology has been proposed to validate the performance of proposed model in context of message length, key length, cipher text length and computational time for encryption and decryption.

Keywords

Hybrid Secure Communication, RSA, MAC, Symmetric Key.

1. INTRODUCTION

In the current era significant computing applications have emerged in recent years to simultaneously connect millions of users to share content, form social groups and communicate with their contacts. Network Environment is the key soul such applications. To maintain security in such applications, Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus basic purpose of this model is too developed within which security services and mechanisms can be viewed. The main purpose of this project is to provide an efficient way to user send or receive message over a secured channel. To maintain confidentiality and integrity of contents primary focus of proposed model.

This model integrate RSA algorithm along with Diffie Hellman Key Exchange Alg. There are various security algorithms are available but still they have scope of improvement. For Example RSA encryption can only provide confidentiality not integrity of content. Authentication can be achieved but on the cost of big key exchange overhead. The complete study concludes to develop a security mechanism consisting confidentiality, authentication and integrity on single platform

2. LITERATURE SURVEY

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.**

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

RSA derives its security from the difficulty of factoring large integers that are the product of two large numbers Multiplying these two numbers is easy, but determining the original prime numbers from the total -- factoring -- is considered infeasible due to the time it would take even using today's super computers.

The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, *p* and *q*, are generated using the Rabin-Miller primarily test algorithm. A modulus *n* is calculated by multiplying *p* and *q*. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length. The public key consists of the modulus *n*, and a public exponent, *e*, which is normally set at 65537, as it's a prime number that is not too large. The *e* figure doesn't have to be a secretly selected prime number as the public key is shared with everyone. The private key consists of the modulus *n* and the private exponent *d*, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of *n*. Considering arithmetic modulo n, let's say that e is an integer that is co prime to the totient φ(n) of n. Further, say that d is the multiplicative inverse of e modulo φ (n). These definitions of the various symbols are listed below for convenience:

n = a modulus for modular arithmetic

φ (n) = the totient of n

e = an integer that is relatively prime to φ(n)

[T his guarantees that e will possess a multiplicative inverse modulo φ(n)]

d = an integer that is the multiplicative inverse of e modulo φ(n)

The computational steps for key generation are

1. Generate two different primes' p and q

2. Calculate the modulus $n = p \times q$

3. Calculate the totient$\varphi(n) = (p - 1) \times (q - 1)$

4. Select for public exponent an integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$

5. Calculate for the private exponent a value for d such that

$$d = e-1 \bmod \varphi(n)$$

6. Public Key = [e, n]

7. Private Key = [d, n]

Furthermore, The Diffie–Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it available to Eve? At first glance it appears that Alice and Bob face an impossible task. It was a brilliant insight of Diffie and Hellman that the difficulty of the discrete logarithm problem for $F_* p$ provides a possible solution.

3. PROBLEM STATEMENT

The major problem with existing cryptographic scenario is, can't achieve authentication and confidentiality along with integrity in single step. 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.

A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.

A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.
Rivest, Shamir and Adleman (RSA) Public-Key Cryptography Standard (PKCS) #7 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, for message encryption.
- Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope 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

4. PROPOSED APPROACH

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. A block representation of proposed solution is shown in figure 1 and 2.

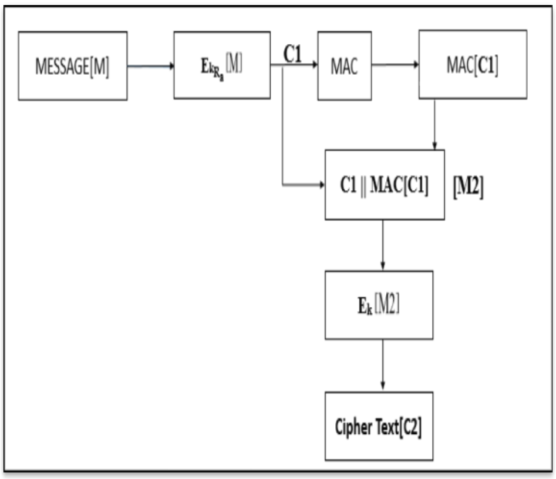

Figure 1: Encryption Process

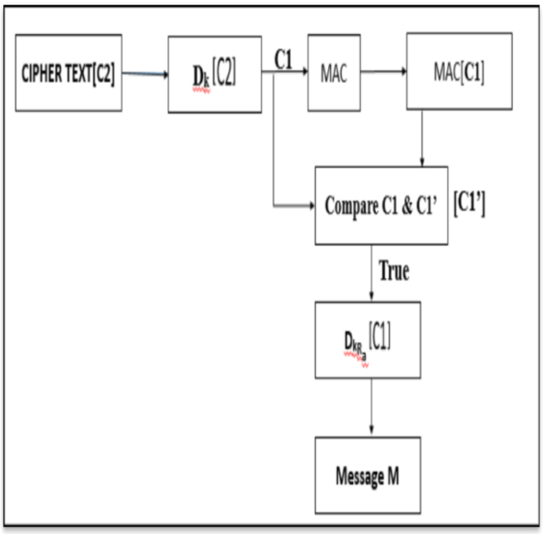

Figure 2: Decryption Process

5. EXPECTED OUTCOMES

The complete study explores the block representation of encryption and decryption process. Proposed work can be implement using java technology to estimate the performance of security mechanism

In order to develop proposed solution following assumptions will be consider for performance evaluation and secure message transmission

1. Maximum data block size for encryption = 128bit / 256bit / 512 bit
2. Maximum Key size for RSA = 128 bit
3. Maximum Key size for Diffie Hellman = 64bit
4. Maximum Key size for MAC = 36bit

It is observe that, variation in message size may be reason for variation in security overhead.

There is need to evaluate performance on multiple message sample on following parameters.

1. Encryption Time for RSA
2. Decryption Time for RSA
3. Encryption Time using Symmetric Key Algorithm
4. Decryption Time using Symmetric Key Algorithm
5. Total time consume in complete encryption and MAC padding
6. Total time consume in complete decryption with MAC verification
7. Total size increase of encrypted packet
8. Total size increase of decrypted

6. RESULT OBSERVATION

1. Encryption Process (Time Estimation)

Table 1: Time Consumption (Milliseconds)

Plain Text Size (KB)	RSA Encryption Time (ms)	SHA-1 Hash Generation Time (ms)	RC-4 Encryption Hash Value Time (ms)	RC-4 Encryption RSA-Data Time (ms)	Total Time For Encryption
10	73.761718	0.286494	0.245117	1.683222	75.7
18	67.319227	0.545779	0.230628	2.321977	70.3
32	68.785707	0.249948	0.067618	3.171437	72.07
65	71.278542	0.268059	0.09358	2.397445	73.7
126	70.095819	0.22278	0.059166	2.054522	72.25
250	75.447355	0.220968	0.057958	2.087123	77.68

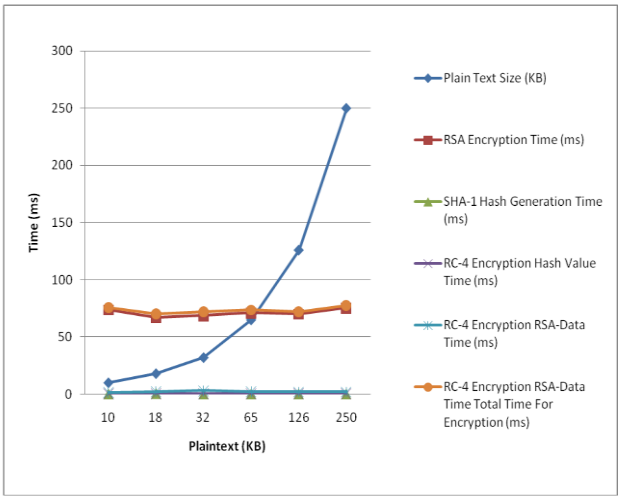

Figure 3: Encryption Time for various File size

2. Decryption Process (Time Estimation)

Table 2: Time Consumption (Milliseconds)

Plain Text Size (KB)	RSA Decryption Time (ms)	SHA-1 Hash Generation Time (ms)	RC-4 Decryption Hash Value Time (ms)	RC-4 Decryption RSA-Data Time (ms)	Total Time (ms)
10	0.374908	7.417703	276.10241	300.594908	584.489929
18	0.127111	14.299303	0.328533	311.975126	326.730073
32	1.257702	6.990553	2.456457	307.294363	317.999075
65	0.225448	6.941664	0.300038	292.19384	299.660

					99
126	0.112863	7.125486	0.285791	300.956686	308.480826
250	0.094146	7.329143	0.262883	304.591226	312.277398

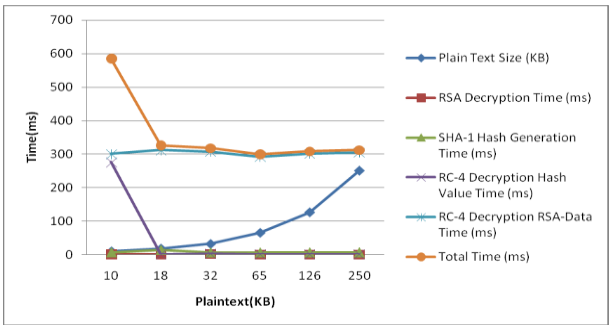

Figure 4: Decryption Time for various File size

3. Encryption (Message Estimation)

Table 3: Message Size Estimation (KB)

Plain Text Size KB	Encrypted Data Size KB
10	616
18	610
32	618
64	608
126	700
250	900

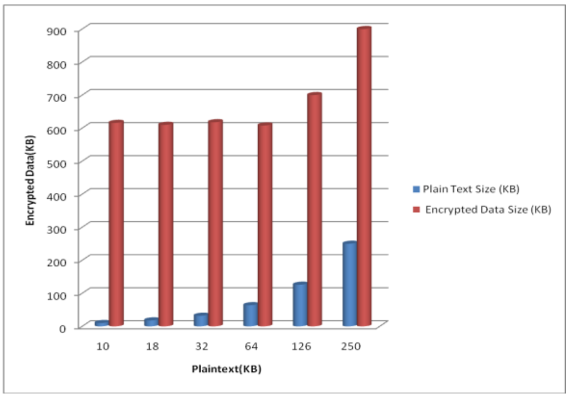

Figure 5: Various file size

7. CONCLUSION

The complete work concludes that, there is need to develop security mechanism to utilize confidentiality, authentication and integrity on single platform. This paper consist the study of security algorithms along with respective overhead. After investigating the problem it proposed a security model to improve security. Subsequently, future directions specify the implementation and evaluation strategy. This project is implemented in JAVA open source environment, which is cost effective and freely available for development. After implementation of the cryptographic technique the performance of the proposed technique is evaluated in different parameters. The obtained result demonstrates the integrity, authentication and confidentiality. Integrity means there is no manipulation in information. The sender send the data and this exact data is received by authorized receiver.

8. FUTURE WORK

In our future we will implement it for advance research like bulk amount of data would transmit easily including features like confidentiality, authenticity and integrity. More security would be produced using all these concepts. This is efficient and adoptable in terms of privacy, securely data access and memory consumption. Therefore the proposed architecture is extended with real world application like banking and financial transaction management. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smart phones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks In our future work we will implement it for move forward research such as image files, thumb impression, video files, verifying signatures etc.

9. REFERENCES

[1] Elichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval and Jacques Stern, *RSAOAEP is secure under the RSA assumption*, Journal of Cryptology, 2002

[2] Adrian Perrig, RobetSzewczyk, Victor Wen, David Culler and J.D. Tygar,*SPINS: Security protocols for sensor networks*, Mobile Computing and Networking, Rome, Italy, 2001

[3] Lai, Xuejia, and Massey, James L., A Proposal for a New Block Encryption Standard, Advances in Cryptology - EUROCRYPT ’90, Lecture Notes in Computer Science, Springer-Verlag, 1991:389-404.

[4] Menezes, A., van Oorschot, P., and Vanstone, S. 1996. Handbook of Applied Cryptography.

[5] CRC Press. This book may downloaded from http://www.cacr.math.uwaterloo.ca/hac/ Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, *New multipartyauthentication services and key agreement protocols*, IEEE Journal of Selected Areas in Communication, 18(4), 2000.

[6] Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang, *An efficient implementation of multi-prime RSA on DSP processor*, University of Texas, Texas, USA,2002.

[7] David Pointcheval and Jacques Stern, *Security proofs for signature schemes*, EUROCRYPT '96, Zaragoza, Spain, 1996.

[8] Bruce Scheneir, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.

[9] Adrian Perrig, RobetSzewczyk, Victor Wen, David Culler and J.D. Tygar,*SPINS: Security protocols for sensor networks*, Mobile Computing and Networking, Rome, Italy, 2001

[10] Lai, Xuejia, and Massey, James L., A Proposal for a New Block Encryption Standard, Advances in Cryptology - EUROCRYPT '90

[11] Lecture Notes in Computer Science, Springer-Verlag, 1991:389-404. Menezes, A., van Oorschot, P., and Vanstone, S. 1996. Handbook of Applied Cryptography.

[12] Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang, *An efficient implementation of multi-prime RSA on DSP processor*, University of Texas, Texas, USA,2002.

[13] David Pointcheval and Jacques Stern, *Security proofs for signature schemes*, EUROCRYPT '96, Zaragoza, Spain, 1996.

[14] AtulKahate,Cryptography and Network Security, Tata McGraw-Hill Publication Company Limited.

[15] Prasad S. Halgaonkar, Sukmal ,V.M. Wadhai," A review of Technology,Tags applications and security",2013.

[16] Tarek Salah Sobh and Mohammad IbrahiemAmer,"PGP Modificaion for securing Digital Envelope mail using COM+ and Web Services",2011.

[17] Brian LaMcchia, Kristin lauter, Anton Mityagin,"Strong security of Authentication key Exchange",2013.

[18] Ravi Kishore Kodali,NarasimhaSarma,"Low energy Digital Envelope Model for WSN's",2014.