IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 21-24
www.iosrjournals.org

Hybrid Cryptosystem Approach for secure communication

Ruchita Patil[a], Veena Kulkarni[b]
[a]*PG Student, Thakur College of Engineering and Technology,Mumbai-400 101,India*
[b]*Assistant Professor, Thakur College of Engineering and Technology,Mumbai-400 101,India*

Abstract: *Data security is of utmost importance in today's world. Especially when the data is travelling through an insecure communication network. Cryptography addresses the necessary elements for secure communication such as privacy, confidentiality, key exchange, authentication and non-repudiation. There are symmetric key encryption techniques which use only one key for both encryption and decryption of the data. . On the other hand, there are asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric. In this paper a hybrid asymmetric cryptosystem algorithm will be implemented which combine the methods RSA and El-gamal. The hybrid cryptosystem that improve the security and performance will be based on encryption time , decryption time and throughput.*

Keywords – *Encryption, Decryption, Hybrid cryptosystem*

I. Introduction

Data transfer is transferring information from a host to another host, or server. To have a secure data transfer, few methods can be applied, and one of them is encryption of data. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, and this method is called encryption. Cryptography is used to secure e-mail, messages, credit card info, and corporate data within the context of any application-to-application communication.

1.1 Symmetric Key Encryption

Encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

1.2 Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. The keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography[7].

ElGamal algorithm based on public key cryptosystem and elliptic curve cryptography encryption system is widely used in digital signatures aspects, which is used for not only data encryption but also digital signatures as well. Its safety depends on the calculation of the discrete logarithm finite field[6].

II. Related work

2.1 Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography

Priyanka Ora, Dr.P.R.Pal IEEE 2015. In this paper solution is provided to maintain data security and data integrity. This scheme contains a combination of RSA Partial homomorphic and MD5 hashing algorithm .In this solution data is encrypted by RSA Partial before uploading it on cloud server. After uploading its hash value is calculated by MD5 hashing scheme[1].

2.2 Security Enhancements of Networked Control Systems Using RSA Public-Key Cryptosystem

Takahiro Fujia, Kiminao kogiso,Kenji Sawada and Seiichi Shin IEEE 2015. In this study uses the homomorphism of the RSA cryptosystem to determine control signals directly from encrypted feedback signals and control parameters without performing any decryption processes[2].

2.3 Secure data sharing through Additive Similarity based El-Gamal like Encryption

M.D. Boomija, S.V. Kasmir Raja IEEE 2016. An efficiently implemented and secured data sharing by using the asymmetric key encryption algorithm called additive similarity based encryption with proxy re encryption method that prevents the outflow of illegal data. Homomorphism enables querying, retrieving and operating on encrypted information in the cloud and it allows data to be processed by third party without breaking the confidentiality[3].

III. Proposed System

Cryptosystem is used for secure communication for that two methods are their encryption and decryption. Cryptography which include various techniques in asymmetric key cryptography and symmetric key cryptography . In Symmetric Key Systems same keys are used where as in Asymmetric Key Systems various keys are used for encryption and decryption. Two process are there in cryptography which is encryption and decryption. For encryption plaintext covert into cipher text by level 1 using RSA algorithm and level 2 using Elgamal algorithm and final data will be store in database. Similarly decryption process covert cipher text into plain text level 1 using RSA algorithm and level 2 using el-gamal algorithm.

The hybrid encryption technique using a mixed encryption model based upon using the RSA and El-gamal algorithms. This paper is based on asymmetric cryptosystem and introduces an hybrid cryptosystem based on RSA algorithm and El-gamal algorithm. The RSA algorithm is based on Integer Factorization Problem (IFP). RSA uses three prime numbers to generate the public and the private keys. It enables faster encryption and decryption process and generates the public and the private key faster. The El-gamal cryptosystem is based on Discrete Logarithm Problem (DLP)[10]. To improve the strength of these algorithms, a combination of RSA and El-gamal is used. This will provide a higher level of security.

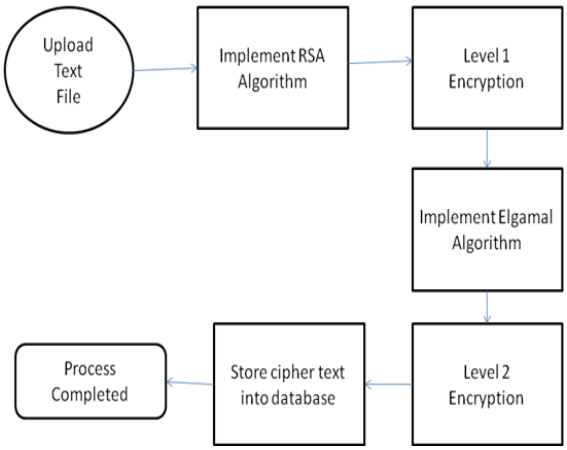

Fig 1. Block Diagram of Hybrid Cryptosystem for Encryption

Two process are there in cryptography which is encryption and decryption. For encryption plaintext covert into cipher text by level 1 using RSA algorithm and level 2 using Elgamal algorithm and final data will be store in database. Similarly decryption process covert cipher text into plain text level 1 using RSA algorithm and level 2 using elgamal algorithm.

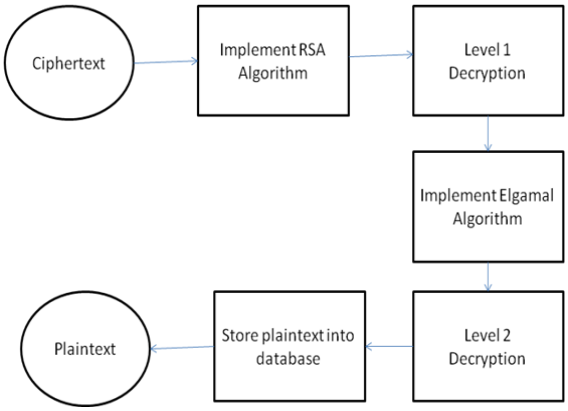

Fig 1. Block Diagram of Hybrid Cryptosystem for Decryption

IV. Methodology

Here is the using asymmetric encryption approach. Which have already know that asymmetric encryption approach has various techniques cryptography but here we are choosing RSA and El-gamal Algorithm. In the proposed technique we have a two keys between sender and receiver, which is known as public key and another is private key. Basically public and private key concept is the asymmetric key concepts where plain text is converting into encrypted text known as cipher text using public key where cipher text decrypted by private key into plain text.

There are three steps to perform algorithm Key Generation, Encryption and Decryption. Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted and decrypted. Encryption the process of converting information or data into a code, especially to prevent unauthorized access. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

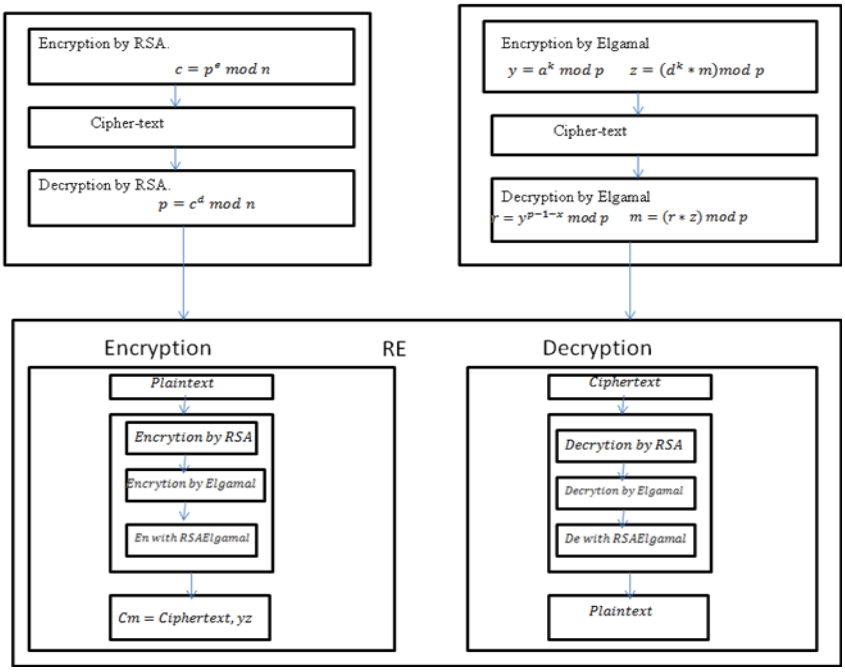

Fig 2. Flow chart of Hybrid System

V. Result and Discussion

The system will be implemented on the text data of various sizes. Compare the encryption and decryption time of each data using hybrid cryptosystem .

- Hybrid algorithm will included the improvement of the efficiency of computation.
- Comparison will be done with different configurations and different models.
- The performance evaluation to be done based on parameters: Throughput, Encryption and Decryption Time.

Message Size	RSA	El-Gamal
1KB	0.00326 sec	0.02697 sec
2KB	0.00346 sec	0.03959 sec
5KB	0.00829 sec	0.06758 sec
10KB	0.01669 sec	0.12194 sec
20KB	0.03186 sec	0.23498 sec
Average Time	0.01085 sec	0.06908 sec
Throughput(Mega Bytes/sec)	4.05069	0.63622

Table1. Expected Results

VI. Conclusion

In this paper, proposed new powerful algorithm for cryptography. The public and the private keys are generated using the RSA algorithm. These keys are then passed to the Elgamal algorithm. Security level is expected to be high as compared to the existing systems as a hybrid of RSA and El-gamal algorithm are used.

Acknowledgements

We take this opportunity to thank a number of individuals whose guidance and encouragement were of enormous help to us while preparing the paper. We thank our project guide as well also the Dean academics Dr. R.R.Sedamkar for their valuable advice and guidance in preparation of the paper.

References

[1] PRIYANKA ORA, DR.P.R.PAL "DATA SECURITY AND INTEGRITY IN CLOUD COMPUTING BASED ON RSA PARTIAL HOMOMORPHIC AND MD5 CRYPTOGRAPHY" IEEE 2015.

[2] Takahiro Fujia, Kiminao kogiso,Kenji Sawada and Seiichi Shin "Security Enhancements of Networked Control Systems Using RSA Public-Key Cryptosystem" IEEE 2015.

[3] M.D. Boomija, S.V. Kasmir Raja "Secure data sharing through Additive Similarity based ElGamal like Encryption" IEEE 2016.

[4] Liang Wang , Yonggui Zhang "ElGamal Algorithm for Encryption of Data Transmission" IEEE 2011.

[5] Ravi Shankar Dhakar, Prashant Sharma, Amit kumar Gupta "Modified RSA Encryption Algorithm (MREA)" IEEE 2012.

[6] Zengqiang Wu , Di Su and Gang Ding "ElGamal Algorithm for Encryption of Data Transmission", ICMC, IEEE 2014.

[7] Mitali, Kumar Vijay, Sharma Arvind, "A New Personal Information Protection Approach Based on RSA Cryptography", IJETTCS, Volume 3, Issue 4, July-August 2014, ISSN 2278-6856

[8] Saranya K, R Mohanapriya, J Udhayan, "A Review on Symmetric Key Encryption Techniques in Cryptography", Internation Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014.

[9] Gupta Vishwa, Singh Gajendra, Gupta Ravindra, "Advance cryptography algorithm to improve data security", IJARCSSE, Volume 2, Issue 1, January 20112 ISSN: 2277 128X.

[10] William Stallings, Cryptography and Network Security-Principles and Practice, Fifth Edition, Pearson publication, pp. 259-262.

[11] VikasAgarwal ,ShrutiAgarwal and Rajesh Deshmukh"Analysis and review of encryption and decryption for secure communication",IJSER, Volume 2,Issue 2,February 2014,ISSN:23473848.

[12] Mitali, Kumar Vijay, Sharma Arvind, "A Survey on Various Cryptography Techniques", IJETTCS, Volume 3, Issue 4, July-August 2014, ISSN 2278-6856