ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Study on Data Encryption Using AES and RSA

Farheen Sultana[1], Bikiran Choudhury[1], Shobha M.S [2],Dr.Jitendranath Mungara[3]

B.E Student., Department of ISE, New Horizon College of Engineering, Bengaluru, Karnataka, India[1]

Senior Assistant Professor, Department of ISE, New Horizon College of Engineering, Bengaluru, Karnataka, India [2]

HOD, Department of ISE, New Horizon College of Engineering, Bengaluru, Karnataka, India [3]

ABSTRACT: As technology advances there is an increase in the amount of data being transferred over the network. One of the principle challenge that is faced is security. Security is achieved by cryptography; cryptography is a study of mathematical techniques related to information security such as confidentiality, data integrity, entity authentication and data origin authentication. In this paper, a 256 bit AES symmetric block cipher is initially used to encrypt the message, the key obtained from the AES encryption is encrypted again using 1024 bit RSA algorithm. Similarly the decryption is done using RSA algorithm to obtain the key which is used to decrypt the message using AES algorithm.AES is a symmetric algorithm that uses only a private key and RSA is an asymmetric encryption system that works with two different keys: A public and a private key. Both work complementary to each other, which means, when a message is encrypted with one of them can only be decrypted by its counterpart. This combination of algorithms provides better security and efficiency.

KEYWORDS: AES, RSA, Security, Efficiency

I.INTRODUCTION

Cryptography is the science of keeping message secure. The method, in which we disguise a message in such a way that its contents are an encrypted message, which is cipher text. The process of conversion of cipher text to plain text is decryption.

Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: Public keys that may be disseminated widely paired with private keys which are known only to the owner. Symmetric cryptography is a cryptographic system that uses a single key to encrypt and decrypt .This project is a combination of both symmetric and asymmetric encryption techniques that provides a system that can overcome mutual drawbacks of both the techniques and enables a secure transaction of data that won't compromise on efficiency.

II. LITERATURE SURVEY

A.DES and AES Performance Evaluation

In cryptography, we encode data before sending it and decode it on receiving, for this purpose, we use many cryptographic algorithms. AES and DES are most commonly used Cryptographic algorithms .In this paper we discussed AES and DES and their comparison using MATLAB software .After applying AES and DES, we compare their result on the basis of avalanche effect, simulation time and memory required by AES and DES[1].

DES: Data Encryption Standard is a symmetric key algorithm. In DES , the key size is 56 bits. The 56-bit key is divided into eight 7-bit blocks and additional 8th odd parity bit is further added to every block. A DES key is actually 64 bits in length to avoid randomness; it is 56 bit for computation.

AES:The key size supported by AES is 128,192and 256 bits .AES takes 128 bits as minimum and maximum is taken 256 bits. Whereas DES key is small in size and its processor power has less technological advancement

Operations of AES are applied on the state during each round are:

- Sub byte

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

- Shift row
- Mix column
- Add round key

The comparison of Advanced Encryption Standard (AES) and Data Encryption Standard (DES)

Technique	Keeping key constant 1 bit variation	Keeping plain text constant 1 bit variation
AES	83	81
DES	43	41

In AES, the avalanche effect is more than in DES.

The comparison, on the basis of Memory usage for implementation and simulation time of AES and DES[5]

Techniques	Simulation time	Memory required for implementation
AES	0.32	43.3
DES	0.0304	10.2

Larger memory required for implementation in Advanced Encryption Standard (AES) as compare to Data Encryption Standard (DES) .It is also clear that simulation time in AES is more effective as compared to DES. In financial application encryption in done by DES but Memory usage is DES is more than in AES .Avalanche effective i.e. One bit variation is more in Advanced Encryption Standard (AES) as compare to Data Encryption Standard (DES). AES is mostly used in encryption of message in chat Channel and is also used in monumentry transaction.AES provides the improvement in security level in information world as compared DES.

.B. Data Encryption and Decryption Using RSA Algorithm in a Network Environment

Network Security is premised on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical[2][3]. This paper presents a design of data encryption and decryption in a network environment using RSA algorithm with a specific message block size. RSA is the most popular public key cryptography (PKC). It uses 2 key cryptosystem, a public key which is known by the sender and the receiver and a private key which is known only by the receiver, so that two parties can engage in a secure communication over a non secure communication channel without having to share key.

RSA encryption: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 primality 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*.

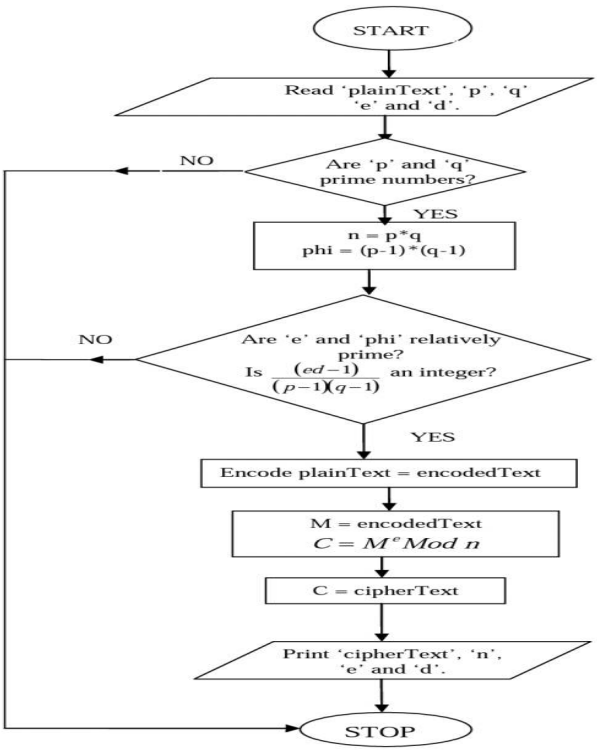
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

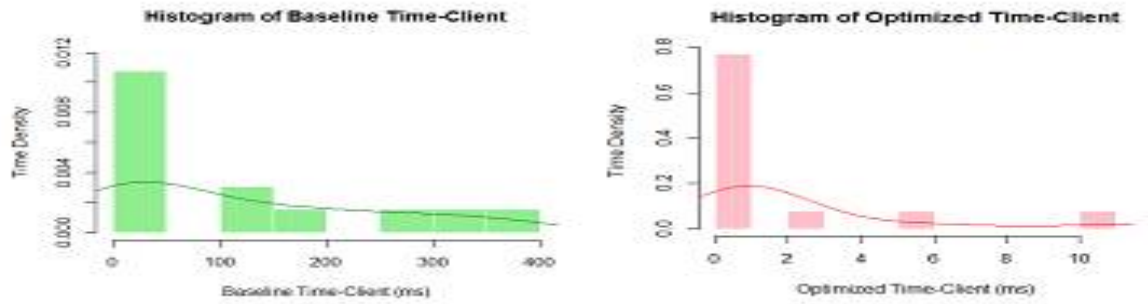


A flowchart illustrating the RSA decryption Algorithm

An eavesdropper that breaks into the message that is encrypted by RSA algorithm will return a decoded message that is a meaningless[4]. This ensures that data is secured against hackers within the network environment.

C . RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages

Asymmetric cryptographic algorithms are a robust technology used to reduce security threats in the transmission of messages on the network. The Major drawback is the mathematical solutions that require a greater amount of calculation leading to increased use of computational resources. This paper aims to optimize the RSA encryption algorithm and thus improve the security, integrity and availability of information.This is done by obtaining the RSA Value for each character of the message ,using a matrix the characters are mixed as an additional process for emcryption.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

In Base-line RSA model the key can be accessed by intruders whereas in optimized RSA model key is encrypted which makes it more secure upon evaluation of result optimized RSA model performs better than Baseline RSA model in terms of lowering time , memory , processor and network performance.

D. A Study of Encryption Algorithms AES, DES and RSA for Security

This paper by Dr. Prerna Mahajan & Abhishek Sachdeva (IITM India)is an effective comparison of the three important cryptography techniques using AES , DES and RSA comparing its performance based on simulation time for encryption and decryption and analysing the experimental result to realise effectiveness of each algorithm. encryption algorithms can be categorized into Symmetric (private) and Asymmetric (public) keys encryption.Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices . Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques due to computational processing power.

The four text files of different sizes are used to conduct four experiments, where a comparison of three algorithms AES, DES and RSA is performed with Encryption Time and Decryption Time as evaluation parameters .

S.NO	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9
2	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
3	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
4	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time and also that Decryption of AES algorithm is better than other algorithms. from the simulation result it is evaluated that AES algorithm is much better than DES and RSA algorithm .

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

In the table above a comparative study between AES, DES and RSA is presented in to eighteen factors.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

III.CONCLUSION

There is a need to secure sensitive and confidential data that is being transacted on day to day basis but the importance to security should not over shadow the efficiency and speed of the system , on reviewing the papers AES and RSA algorithms are found to be more efficient than other cryptographic techniques in terms of memory usage and simulation time. Hence the combination of AES and RSA becomes more reliable cryptosystem that enhances the speed and security .

REFERENCES

[1]International Conference on Computing, Communication and Automation (ICCCA2015) DES and AES Performance Evaluation Bawna Bhat School of Computer Science and Engineering Galgotias University

[2] Afolabi, A.O and E.R. Adagunodo, 2012. Implementation of an Improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.

[3] Gaurav, S., 2012. Secure file transmission scheme based On hybrid encryption technique. International Journal of management, IT and Engineering. Vol. 2, issue 1.

[4]Data Encryption and Decryption Using RSA Algorithm in a Network Environment ,Nentawe Y. Goshwe. Department of Electrical/Electronics Engineering ,University of Agriculture, Makurdi IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 .

[5] Akash Kumar Mandal1, Chandra Parakash2 "Performan ce Evaluation of Cryptographic Algorithms: DES and AES", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[6] Global Journal of Computer Science and Technology ,Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013, A Study of Encryption Algorithms AES, DES and RSA for Security By Dr. Prerna Mahajan & Abhishek Sachdeva IITM, India.

[7]JCNS International Journal of Computer Science and Network security,VOL.16 No.8,August 2016.RSA Encryption Algorithm Optimization to improve Performance and Security Level of Network Messages.Fausto Meneses,Walter Fuertes,Jose Sancho,Santigo Salvador,Daniela Flores,Hernan Aules,Fidel Castro.

[8]X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption",in 6th International Forum on Stratergic Technology(IFOST),2011

[9]G.singh and A.Supriya,"A Study of encryption algorithms(RSA,DES,3DES AND AES) for Information Security" in International Journal of Computer Applications 67(19),2013.

[10]Q.Liu, Y.Li,T.Li and L.Hao "The research of the batch RSA decryption performance" in journal of computational Information system 2011.

[11] Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard
Algorithm".International Journal of Engineering and AdvancedTechnology (IJEAT) ISSN: 2249 – 8958, Volume-2,Issue-5, June 2013.

[12] Chehal Ritika, Singh Kuldeep. "Efficiency andSecurity of Data with Symmetric Encryption Algorithms". International Journal of AdvancedResearch in Computer Science and Software
Engineering, ISSN: 2277 128X , Volume 2, Issue 8,August 2012,