ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Cryptographic Algorithms: Analysis and Performance Evaluation for AES, DES and RSA for Secure Two Party Communications

Mohammed Firdos Alam Sheikh

Research Scholar, Pacific Academy of Higher Education and Research University, Udaipur, India

ABSTRACT: In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system.. There is no single mechanism that will provide all the services specified. But we can identify a very important mechanism that supports all forms of information integrity is cryptographic technique. In this work we made to generate two algorithms which provide security to data transmitted. In this paper we implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption.

KEYWORDS: Encryption; DES; AES; RSA

I. INTRODUCTION

In this work both the algorithms are discussed in terms of computational security, computational complexity and computational overhead. Both the algorithms are studied for their strengths and limitations. A crypto analytical study of the algorithms with emphasis on probabilistic encryption is also considered in this study. The encryption algorithms are compared with standard algorithms like RC4 and DES. The algorithms are also discussed in terms of its applications and also about their advantages and limitations in network This study represents an exploration of advantages of encryption of data for security and confidentiality. The significance of encrypting data is of more relevance in light of the mushrooming applications and globalization of communication. Encryption of data is of particular significance or an imperative for applications like email, electronic transactions, digital cash, electronic voting and so on. The study traces the development of Encryption algorithms in terms of their diversity of applications that we feel in our daily lives. Some Encryption algorithms have been developed to make transmission and storage of data more secured and confidential[1]. The study discusses the distinguishing features of two encryption algorithms and their models in terms of their applications. . In this work an attempt has been made to generate two algorithms which provide security to data transmitted. The first algorithm considers a random matrix key which is multiplied with a ternary vector. A sign function is applied on the product to generate a sequence. This sequence is used to build three different encryption models [2]. Each model can be used for encryption of data. Two models like Model1 & Model2 are based on block cipher technique and Model3 is a stream cipher.

II. RELATED WORK

They can be categorizedinto Symmetric(private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys [1]. Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive. There are many examples of strong and weak keys of cryptography algorithms like DES, AES. DES uses one 64-bits key while AES uses various 128,192,256 bitskeys [2]. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

encryption and private key is used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user[2]. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [3]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [4].This study evaluates three different encryption algorithms namely; AES, DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document[5].

III. ENCRYPTION ALGORITHMS

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval [6].

IV. SYMMETRIC ENCRYPTION SCHEMES

Block ciphers take as input the key and a block, often the same size as the key. Further, the first block is often augmented by a block called the initialization vector, which can add some randomness to the encryption.

A. DES Algorithm

The most widely used encryption scheme is based on Data Encryption Standard (DES). There are two inputs to the encryption function, the plain text to be encrypted and the key. The plain text must be 64 bits in length and key is of 56 bits. First, the 64 bits of plain text passes through an initial permutation that rearranges the bits. This is fallowed by 16 rounds of same function, which involves permutation & substitution functions. After 16 rounds of operation, the pre output is swapped at 32 bits position which is passed through final permutation to get 64 bit cipher text. DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process [7].

DES algorithm consists of the following steps

ENCRYPTION

1) DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2) The plaintext block has to shift the bits around.
3) The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4) The plaintext and key will processed by following
   - The key is split into two 28 halves
   - Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   - The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
   - The rotated key halves from step 2 are used in next round.
   - The data block is split into two 32-bit halves.
   - One half is subject to an expansion permutation to increase its size to 48 bits.
   - Output of step 6 is exclusive-OR'ed with the 48- it compressed key from step 3.
   - Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   - Output of step 8 is subject to a P-box to permute the bits.
   - The output from the P-box is exclusive-OR'ed with other half of the data block. k.
   - The two data halves are swapped and become the next round's input.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

A. Advanced encryption standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure 1. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

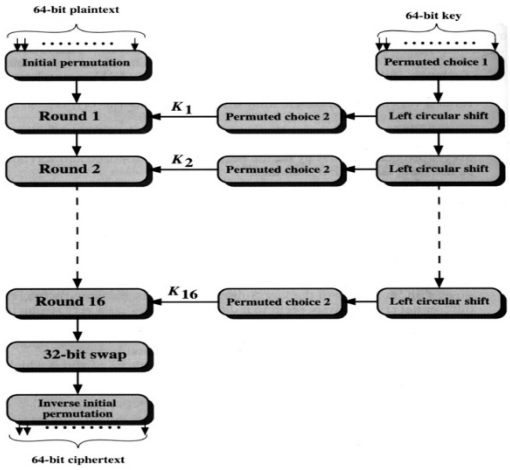

Fig. 1. DES algorithm

Algorithm Steps : These steps used to encrypt 128-bit block

1) The set of round keys from the cipher key.
2) Initialize state array and add the initial round key to the starting state array.
3) Perform round = 1 to 9 : Execute Usual Round.
4) Execute Final Round.
5) Corresponding cipher text chunk output of Final Round Step

C. Rivest-Shamir-Adleman (RSA)

RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA algorithm involves these steps:

1) Key Generation
2) Encryption
3) Decryption

Key Generation Steps:

- Generate a public/private key pair :
- Generate two large distinct primes p and q
- Compute $n = pq$ and $\varphi = (p - 1)(q - 1)$
- Select an e, $1 < e < \varphi$, relatively prime to φ.
- Compute the unique integer d, $1 < d < \varphi$ where $ed \equiv_{\varphi} 1$.
- Return public key (n, e) and private key d

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Encryption

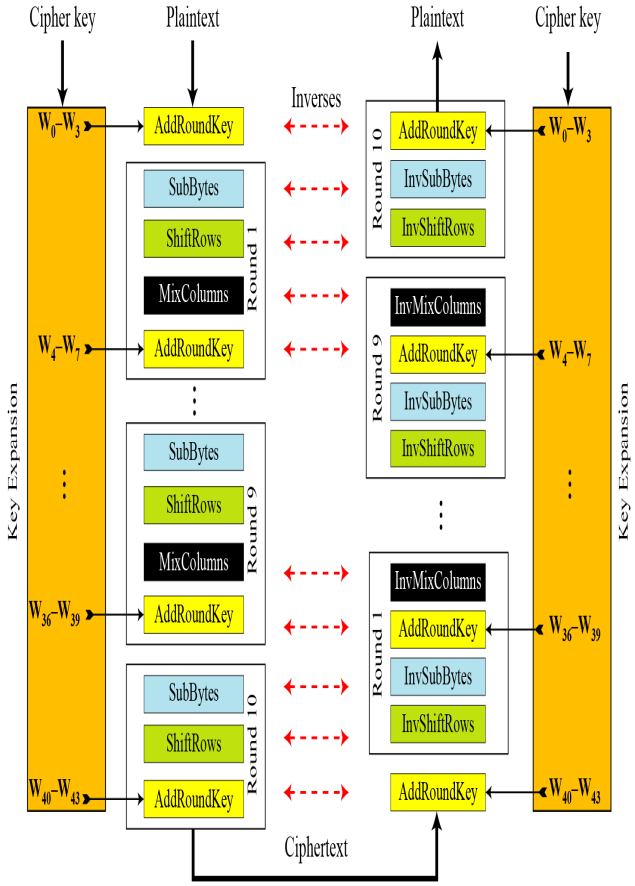

Fig. 2. AES algorithm

Encryption is the process of converting original plain text (data) into cipher text (data).
Encryption with key (n , e)

- Represent the message as an integer m € {0, . . . , n− 1}
- Compute c = me mod n

Decryption
Decryption is the process of converting the cipher text (data) to the original plain text(data). [10] Decryption with key d: compute m = cd mod n

V. RESULT

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.

- Evaluation ParametersPerformance of encryption algorithm is evaluated considering the following parameters.
  (i) Encryption Time
  (ii) Decryption Time

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

- The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text.

- Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time.
- Comparisons analyses of the results of the selected different encryption scheme are performed. [10]
- Experimental Results And Analysis
- Experimental result for Encryption algorithm AES, DES and RSA are shown in table-2, which shows the comparison of three algorithm AES, DES and RSA using same text file for four experiments.

By analyzing table-2, Time taken by RSA algorithm for both encryption and decryption process is much higher compare to the time taken by AES and DES algorithm.

Table I: Comparisons of DES, AES and RSA of Encryption and Decryption Time

S.NO	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	AES	210	1.8	1.5
	DES		2.1	1.32
	RSA		9.1	6.3
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

By analyzing Fig-4 , Fig-5 which shows time taken for encryption and decryption on various size of file by three algorithms. RSA algorithm takes much longer time compare to time taken by AES and DES algorithm. AES and DES algorithm show very minor difference in time taken for encryption and decryption process. The second algorithm considers not only key but alsoinitialization vector and time stamp to generate sub keys which are used for encryption process.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

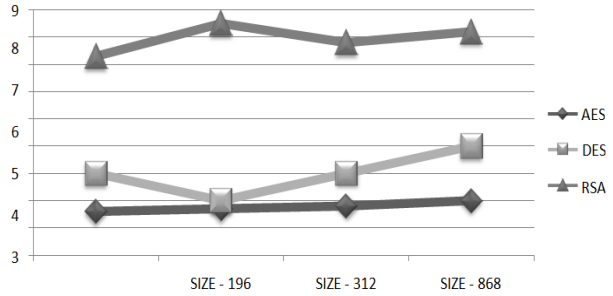

Fig. 3. Comparison of Encryption Time among AES, DES and RSA

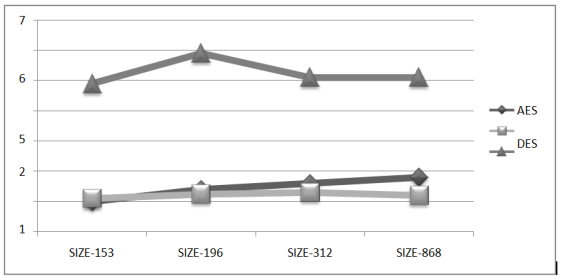

Fig. 4. Comparison of Decryption Time among AES, DES and RSA

VI. CONCLUSION

Our research work show the performance of existing encryption techniques like DES, AES and RSA algorithms.
Based on the experimental result and the text files used it was concluded that RSA consume longest encryption time and AES algorithm consumes least encryption time.We also observed that Decryption of AES algorithm is better than other algorithms.From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm Our future work will focus on compared and analysed existing cryptographic algorithm like AES, DES and RSA. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

ACKNOWLEDGMENT

This work was partially supported by Many people directly or indirectly. Prof. S.K. Sharma and Manish Kothari provided valuable feedback and suggestions that helped improve the paper.

REFERENCES

[1] Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu: A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007, pp73-81
[2] Lester S. Hill, Cryptography in an Algebraic Alphabet, The American MathematicalMonthly 36, June-July 1929, pp 306–312.
[3] Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct usingPalmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp 234-238, 2009
[4] Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic EncryptionScheme, On Line March 2007,
[5] C. Anley. Advanced SQL Injection In SQL Server Applications.White paper, Next Generation Security Software Ltd., 2002.
[6] D. Aucsmith. Creating and Maintaining Software that Resists Malicious Attack. http://www.gtisc.gatech.edu/bio aucsmith.html, September 2004. Distinguished Lecture Series.
[7] Blum L., Blum M , Shub M. : A simple unpredictable pseudo random number generator , SIAM J. compute , 1986, 15, (2), pp 364-383.
[8] Sage.math.Washington.edu/home/jetchev/Public.html/do cs/jetchev-talk.ppt-Broadcast encryption schemes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

[9] P. Finnigan. SQL Injection and Oracle - Parts 1 & 2. Technical Report, Security Focus, November 2002. http://securityfocus.com/infocus/1644
[10] Dr. Prerna Mahajan & Abhishek Sachdeva :A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013.
[11] R.S.Thore & D.B.Talange: Security of internet to pager E-mail messages (Internet forIndia-1997IEEE Hyderabad section) pp.89-94.
[12] R.H.Rahnan, N,Nowsheen: A New Symmetric Key Distribution Protocol UsingCentralized Approach, Asian Journal of Information Technology, 2007 6(8) pp 911-915.