Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

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

Abhishek Sachdeva[1]

[1] IITM

Received: 12 December 2012 Accepted: 2 January 2013 Published: 15 January 2013

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. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. 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. Experiments results are given to analyses the effectiveness of each algorithm.

Index terms— DES, RSA, AES, encryption, decryption, private key encryption, public key encryption, cryptography.

1 Introduction

any encryption algorithms are widely available and used in information security. They can be categorized into 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 bits keys [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 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].

2 Asymmetric encryption techniques are almost 1000

Authors ? ? : e-mail: aabhi616@yahoo.in 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].

3 II.

4 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]. a) Data Encryption Standard (DES) 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 i. 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 i. The key is split into two 28 halves ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round. iii. 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. iv. The rotated key halves from step 2 are used in next round. v. The data block is split into two 32-bit halves. vi. One half is subject to an expansion permutation to increase its size to 48 bits. vii. Output of step 6 is exclusive-OR'ed with the 48itcompressed key from step 3. viii. 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. ix. Output of step 8 is subject to a P-box to permute the bits. ii. Usual Round : Execute the following operations which are described above. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step. 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 i Key Generation Before the data is encrypted, Key generation should be done. [9] Steps: Generate a public/private key pair : 1. Generate two large distinct primes p and q 2. Compute n = pq and ? = (p ? 1)(q ? 1) 3. Select an e, 1 < e < ?, relatively prime to ?.

5 Comparision

In

6 Experimental Design

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.

7 Performance of encryption algorithm is evaluated considering the following parameters. A. Encryption Time B. Decryption Time

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. [11] V.

8 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 experiment. 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. algorithm. AES and DES algorithm show very minor difference in time taken for encryption and decryption process.

VI.

9 Conclusion

Encryption algorithm plays very important role in communication security. Our research work surveyed the performance of existing encryption techniques like AES, DES and RSA algorithms.

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.

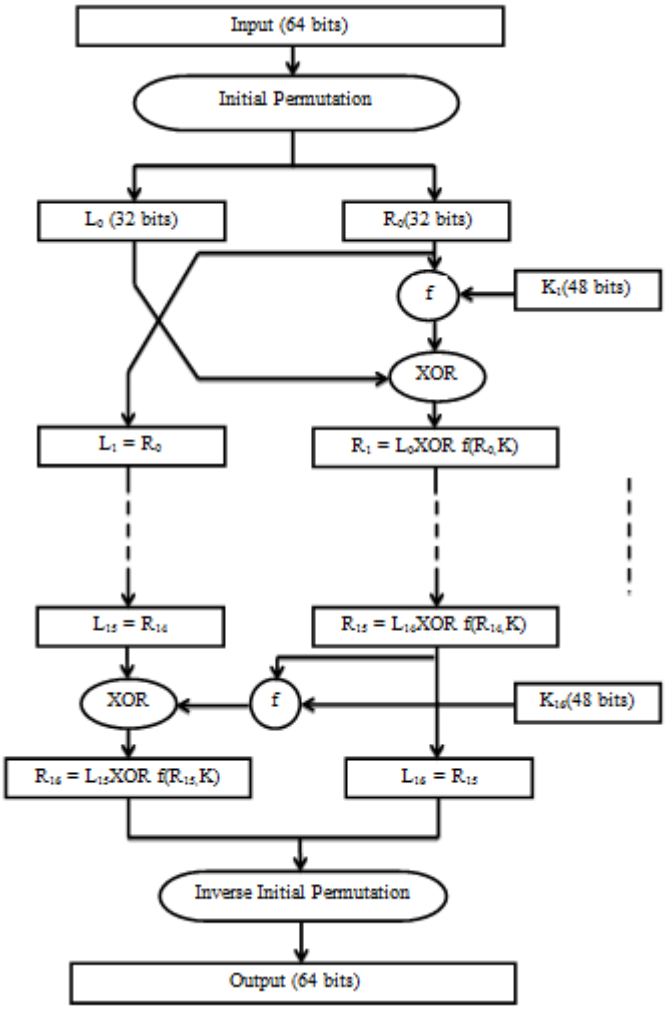
We also observed that Decryption of AES algorithm is better than other algorithms.

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.

1 

Figure 1: EFigure 1 :



2

Figure 2: Figure 2 :

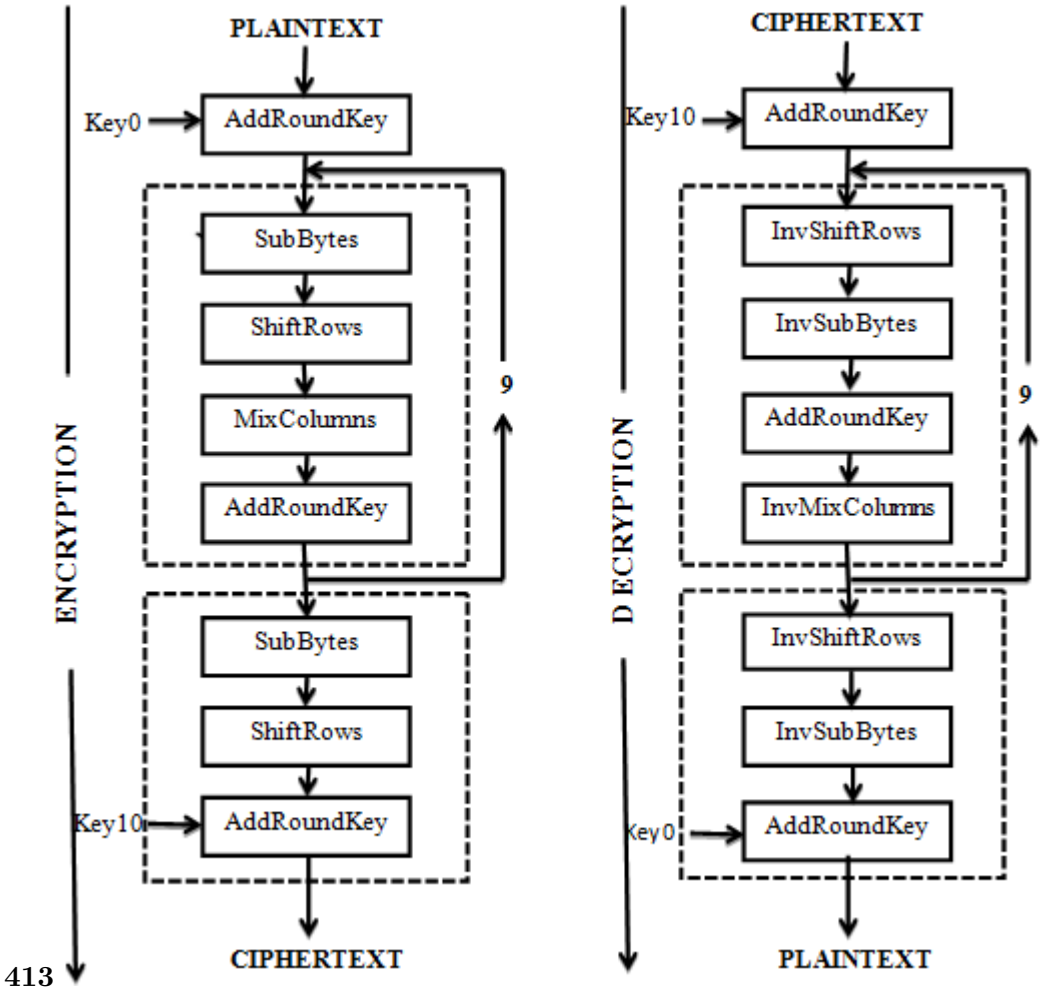


Figure 3: 4 .E 1 .Figure 3 :

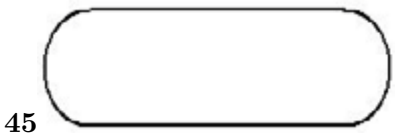


Figure 4: Figure 4 :Figure 5 :

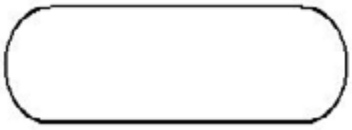


Figure 5:

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key , using K(round)

iii. Final Round: Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K(10)

iv. Encryption : Each round consists of the following four steps:

[Note: i Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits. ii Shift Rows : In the encryption, the transformation is called Shift Rows.iii]

Figure 6:

1

Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds, Stimulation Speed, Trojan Horse, Hardware & Software Implementation and Ciphering & Deciphering Algorithm.

Figure 7: Table 1 :

2

2 : 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	153	1.6 3.0	1 1.1
	DES		7.3	4.9
	RSA			

Figure 8: Table 2

[International Journal of Research in Computer and Communication technology (2012)] , *International Journal of Research in Computer and Communication technology* 2278- 5841. September 2012. 1 (4) p. 145. (IJRCCT)

[Prashanti and S Sandhya Rani (2013)] 'A Novel Approach for Data Encryption Standard Algorithm'. Deepthi G Prashanti , S & Sandhya Rani . *International Journal of Engineering and Advanced Technology (IJEAT)* 2249 -8958. June 2013. (2) p. 264.

[Idrizi et al. (2013)] 'Analyzing the speed of combined cryptographic algorithms with secret and public key'. Florim Idrizi , Dalipi , & Fisnik , Ejup Rustemi . ISSN: 2278-800X. *International Journal of Engineering Research and Development* 2278-067X. August 2013. 8 (2) p. 45.

[Padmapriya and Subhasri (2013)] 'Cloud Computing: Security Challenges & Encryption Practices'. Dr A Padmapriya , P Subhasri . *International Journal of Advanced Research in Computer Science and Software Engineering* 2277 128X. March 2013. 3 (3) p. 257.

[Ritika and Kuldeep (2012)] 'Efficiency and Security of Data with Symmetric Encryption Algorithms'. Chehal Ritika , Singh Kuldeep . *International Journal of Advanced Research in Computer Science and Software Engineering* 2277 128X. August 2012. 2 (8) p. 1.

[Sunitha and Prashanth (2013)] 'Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm'. K Sunitha , K S Prashanth . ISSN: 2278- 8727Volume 12. *IOSR Journal of Computer Engineering* 2278-0661. Jul. -Aug. 2013. (5) p. 64. IOSR-JCE

[Elminaam et al. (2010)] 'Evaluating The Performance of Symmetric Encryption Algorithms'. Diaa Elminaam , Abdual Salama Abd , Kader . *International Journal of Network Security* May 2010. 10 (3) p. 216. (Hatem Mohamed & Hadhoud, Mohiy Mohamed)

[Parsi and Sudha] Kalpana Parsi , Singaraju Sudha . *Data Security in Cloud Computing using RSA Algorithm*,

[Abdul et al.] *Performance Analysis of Symmetric Cryptography*, Abdul , D S Mina , H M Kader , M Hadhoud . p. 1.

[Debasis and Rajiv (2011)] 'Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm'. Das Debasis , Misra Rajiv . *International Journal of Network Security & Its Applications (IJNSA)* November 2011. 3 (6) p. 204.

[Hardjono ()] *Security In Wireless LANS And MANS*, Hardjono . 2005. Artech House Publishers.

[Narjeet and Gaurav] 'Security On Bccp Through Aes Encryption Technique'. Singh Narjeet , Raj Gaurav . *International Journal Of Engineering Science & Advanced Technology* (2) . (Issue-4, 813 -819. pp. 817.)