COMPARATIVE STUDY AND ANALYSIS OF VARIOUS CRYPTOGRAPHIC ALGORITHMS

[1]M. Harini, [2]K. Pushpa Gowri, [3]C. Pavithra, [4]M. Pradhiba Selvarani
[4]Assistant Professor,
[1,2,3,4]Department of Computer Science and Engineering
Kamaraj College of Engineering and Technology, Virudhunagar, India.
2131092@kamarajengg.edu.in

ABSTRACT

Data security is a major factor for every communication system. Communication becomes a necessary tool for any business, education, defence services etc. It is desired to communicate data with high security. At present, various cryptographic algorithms have been proposed and implemented. Those algorithms are broadly classified into symmetric and asymmetric algorithms based on the number of keys used. This paper, the comparison is made between algorithms such as RSA, AES, MD5 and the combination of AES-RSA-MD5 algorithms on the basis of execution time.

KEYWORDS - AES, RSA, MD5 and Execution time

I.INTRODUCTION

Cryptography is the study of techniques for secure communication. It is the way of protecting the information by encoding the data into an unreadable format. It is an efficient way of protecting sensitive information as it is stored or transmitted through a network communication path. It is used to achieve security services such as authentication, confidentiality and integrity [10]. Encryption is a technique that converts our data into a format called cipher text and decryption techniques are vice versa of it for promoting the data security. Different encryption techniques are used protect the secret data from an unauthorized use. Encryption techniques can be categorized into symmetric, asymmetric and hashing. Symmetric key cryptography is an algorithm that uses single key for both encryption [3] and decryption [5]. Asymmetric key cryptography uses one key to encrypt the message and another key to decrypt the same message [5]. It is also called as public key cryptosystem. Hashing functions are algorithms that use no key. They are called as one way encryption. On a given plain text a fixed length hash value is calculated because of this the plain text cannot be brought back.

II. BASIC TERMS USED IN CRYPTOGRAPHY

A. Plain text

In cryptography, plain text is a text which is in human readable form. It is a message that has to be sent to the receiver end from the sender end. It is also known as clear text. It is given as an input to the encryption algorithm for encryption process [11].

B. Cipher text

It is also known as encrypted text as it is a non-readable form of original text. It is a meaningless text that cannot be understood by human without decryption of cipher text. It is a result of an encryption technique. The plain text is converted into a cipher text before sending the original text [11].

C. Encryption

Encryption is a technique that allows the user to hide information from others. Encryption requires two basic things such as key and possible encryption algorithms [11]. It is used to send the confidential message to the user. It is a process in which the given original text is converted into a cipher text or unreadable form.

D. Decryption

Decryption is a reverse process of encryption. It is a process of converting a cipher text back into a plain text that the user can read [11]. It happens at the receiver end so that they can read the message that was send by the sender. It also needs a key and algorithm for decrypting the text.

E. Key

Key operates on the plain text and converts it into cipher text. The real strength of cryptography is in the key. It is used for both encryption and decryption process. Key could be a number, function or an algorithm. Key performs the transformation [11].

F. Cryptosystem

The system which is used to implement cryptography is known as cryptosystem.

III. ALGORITHMS USED

A. Advanced encryption standard (AES)

AES was developed in 1999. AES was announced by national institute of standards and technology (NIST). The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128,192 and 256 bits [1][9].The algorithm's overall structure is shown in Fig. 1.Unlike DES (the predecessor of AES), AES is a substitution-permutation network not a feistel network [8]. AES is relatively easy to implement and requires little memory. In AES, there are four transformations for one round.

1) Sub bytes: It adds confusion by processing each byte through an S-Box. An S-Box is a substitution table where one byte is substituted for another.

2) Shift rows: It provides simple permutation of data, where as other steps involve substitution. It performs a circular rotation on each row. When decrypting, it performs the circular shift in opposite direction for each row.

3) Mix columns: It is a substitution that makes use of each byte of a column. Each byte is mapped into new value that is a function of all four bytes in that column. The inverse used for decryption involves a different set of constants.

4) Add round key: It is a simple bitwise XOR of the current block with a portion of the expanded key. It is the only step which makes use of the key and obscure the result, hence must be used at start and end of each round.

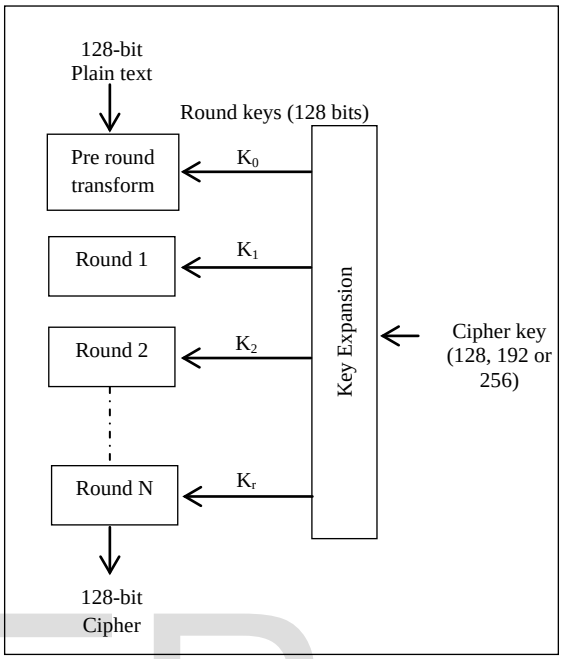

Fig. 1 AES Algorithm

B. RSA algorithm

It was first published by Rivest, Shamir and known to everyone. The encrypted message can only decrypted using the private key as shown in Fig. 3. In RSA each participant must generate the pair of keys, which requires finding primes Adlemen of MIT in 1978. It is an algorithm for public key cryptography [7]. It is suitable for both signing as well as encryption. It includes a public key and a private key. Here public key is used for encryption as shown in Fig. 2 and computing inverses. Both the prime generation and the derivation of a suitable pair of inverse exponents may involve trying a number of alternatives.

Steps in RSA algorithm

1) Generation of public and private key

Step1: Choose two prime numbers p and q.

Step2: Compute $n = pq$.

Step3: Compute $\varphi(p-1)(q-1)$.

Step4: Chose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ i.e., e and $\varphi(n)$ are co-primes.

Step 5: $d \equiv e^{-1} (\mathrm{mod}\ \varphi(n))$

2) Encryption

Plain text is converted into cipher text by the following formula [6]

$$Cipher = (Message)^e \ mod\ n$$

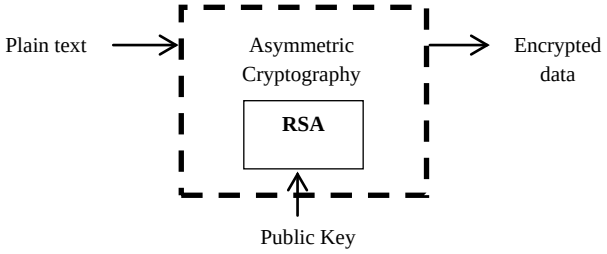

Fig. 2 RSA Encryption

3) Decryption

Cipher text is converted into original message by the following formula [6]

$$Message = (Cipher)^d \ mod\ n$$

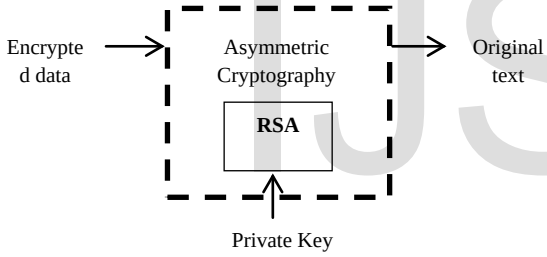

Fig. 3 RSA Decryption

C. MD5Algorithm

MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function. It is a hashing algorithm which is used to computer data finger print of a data block. MD5 converts a variable length message into a fixed-length of 128 bits. The input will be broken into 512 bit blocks. The message is padded so that its length is divisible by 512 [1]. MD5 is mainly used for data integrity to ensure that the original text is not being altered during transmission. It takes input message of arbitrary length and generates 128 bit long output hash MD5 hash algorithm consists of 5 steps as shown in Fig. 4.

Step 1: Append padding bits.
Step 2: Append length.
Step 3: Initialize MD buffer.
Step 4: Process message in 16-word Blocks.
Step 5: Output.

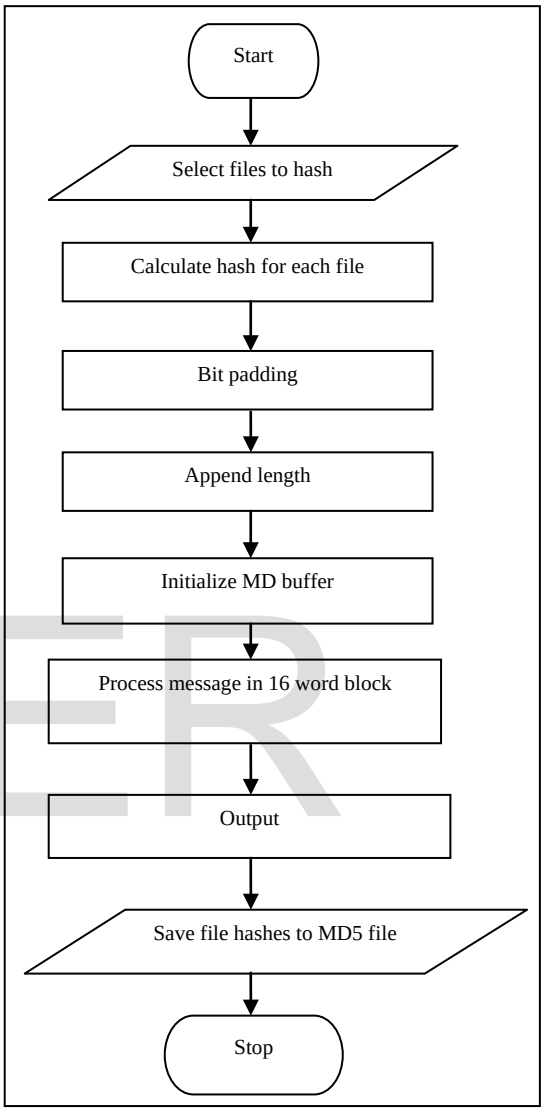

Fig. 4 Flowchart depicting the steps in MD5

IV. COMPARISON OF ALGORITHMS

In the table below (TABLE I) a comparative study between AES, RSA and MD5 is presented [2].

FACTORS	AES	RSA	MD5
Author	JoanDaemn, Incent Rijmen	Rivest, Shamir, Adlemen	Ronald Rivest
Year	1998	1977	1992
Structure	Substitution Permutation	Public Key Algorithm	Merkle Damgard
Rounds	10, 12, 14	1	4
Key length	128, 192, 256	Greater than 1024 bits	512
Block Size	128	128	512
Level of Security	Strongly ciphered	High security	Moderately secure
Execution speed	Faster	Slower	Moderate
Vulnerabilities	Brute Force (Not yet proved)	Oracle attack	Collision, Preimage vulnerability
Encryption/ Decryption speed	Faster	Low	Faster
Algorithm	Symmetric	Asymmetric	Hashing

TABLE I. Comparison of Algorithms

V. EXPERIMENTAL RESULTS

AES, RSA and MD5 have been implemented in java and the following results were obtained.

A. Implementation of AES

Fig.5 shows the input given to the AES algorithm.

Fig. 5 Input for AES algorithm

The encryption and decryption of the AES algorithm was shown in Fig. 6 and Fig. 7.

Fig. 6 AES encryption

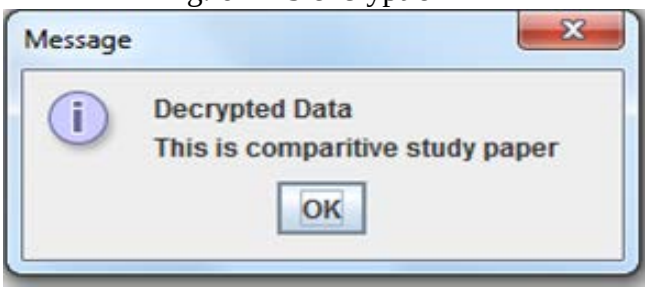

Fig. 7 AES decryption

The Fig. 8 shows an execution time of the AES algorithm.

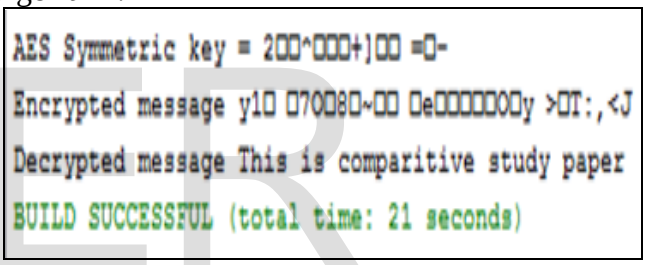

Fig. 8 Execution time for AES

B. Implementation of RSA

In Fig. 9, The input was given to the RSA algorithm. The given input was converted into bytes and then encryption and decryption processes were performed.

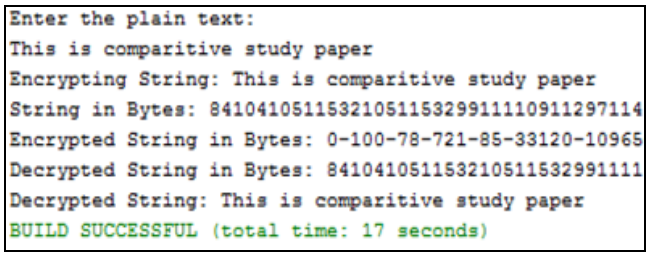

Fig. 9 RSA Implementation

D. Implementation of MD5

Fig. 10 shows the hash code generation of the MD5 algorithm for the given input.

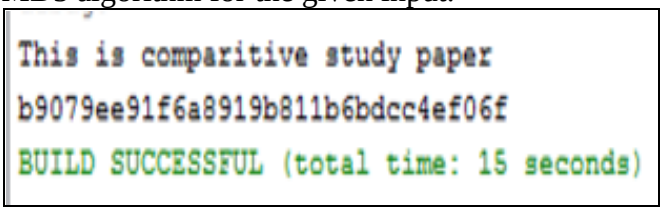

Fig. 10 MD5 Implementation

D. Comparison of Algorithms using Execution Time

In TABLE II, the execution time of three algorithms (AES, RSA, MD5) was compared.

TABLE II. COMPARISON OF EXECUTION TIME OF THE ALGORITHMS

ALGORITHMS	EXECUTION TIME (in seconds)
AES	21
RSA	17
MD5	15

VI. CONCLUSION

Cryptography algorithm is a science in secret code. Rapidly rising cybercrime and the growing prospect of internet being used as a medium for attacks create a major challenge for network security. This paper presents a comparative study of different cryptographic algorithms AES, RSA and MD5.Each algorithm has been compared based on execution time (refer TABLE II) of these algorithms. From the result the symmetric encryption algorithm AES are most secured and efficient. RSA is secured and can be used in many applications because of its good speed. MD5 provide assurance abut integrity of transferred file.

VII. REFERENCES

[1] Kirtiraj Bhatele, Amit Sinhal, and Mayank Pathak, "**A Performance-Centric Comparative Study of Hybrid Security Protocol Architectures**", Proceedings of All India Seminar on Biomedical Engineering 2012, Page No. 231 - 238.

[2] Dr. Prerna Mahajan, and 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.

[3] VekariyaMeghna, "**Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms",** International Journal of Computer Engineering and Science, August - 2014.

[4] C.Radha, P.Sakthi Priyanka, Dr.S.Prabha, "**Enhanced Hybrid Cryptography Technique to Secure the Network**", International Journal of Emerging Technology in Computer Science & Electronics, Volume 19, Issue 2, January 2016.

[5] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, **"Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features**", International Journal of Network Security & Its Applications, Vol.6, No.4, July 2014.

[6] Ritin Behl, Garima Sehgal, Mridula Kumar, Pushkar Gupta, "**Experimental comparison between Hybrid RSA-AES and RSA Algorithms in IP Security",** International Journal of Modern Trends in Engineering and Research , Volume 02, Issue 06, June – 2015.

[7] Prashant Kumar Arya et al, Dr Mahendra Singh Aswal, Dr Vinod Kumar, "**Comparative Study of Asymmetric Key Cryptographic Algorithms",** International Journal of Computer Science &

Communication Networks, Vol 5(1), June 2014.

[8] Shraddha Soni, Himani Agrawal, Dr. Monisha Sharma, **"Analysis and Comparison between AES and DES Cryptographic Algorithm**", International Journal of Engineering and Innovative Technology, Volume 2, Issue 6, December 2012.

[9] Roshni Padate, Aamna Patel, "**Encryption and Decryption of Text using AES algorithm**" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 5, May 2014.

[10] Ankita Verma, Paramita Guha, Sunita Mishra**, "Comparative Study of Different**

[11] **Cryptographic Algorithms",** International Journal of Emerging Trends & Technology in Computer Science, Volume 5, Issue 2, March - April 2016.

[12] Priti Bali, "**Comparative Study of Private and Public Key Cryptography Algorithms**", International Journal of Research in Engineering and Technology, Volume: 03 Issue: 09, Sep-2014.

[13] Mr. Mahavir Jain, Mr. Arpit Agrawal, "**Implementation of Hybrid Cryptography Algorithm**", International Journal of Core Engineering & Management, Volume 1, Issue 3, June 2014.