Cryptography: Avalanche effect of AES and RSA

Rohit Verma*, Aman Kumar Sharma**

* Department of Computer Science, Himachal Pradesh University, India

*verma.rohit218@gmail.com, **sharmaas1@gmail.com

DOI: 10.29322/IJSRP.10.04.2020.p10013
http://dx.doi.org/10.29322/IJSRP.10.04.2020.p10013

Abstract- Security is a major concern in the field of computer science. With the advancement in technology security of data from theft has become a major obstacle. It is necessary to encrypt data before sending it through the internet. Cryptography plays an important role. Through cryptography, one can easily convert his/her data in a human unreadable form and send it over the internet. In this paper two most widely used cryptography algorithms AES and RSA have been analyzed. Simulation is performed using CrypTool. This simulation is performed on two different types of data. These algorithms are analyzed based on the avalanche effect due to change in a single character of plain text and memory required by these algorithms in the secondary storage device.
Index Terms- AES, asymmetric key, avalanche effect, cryptography, RSA.

I. INTRODUCTION

Nowadays transmission of plain data (readable data) over the internet is not considered safe because of various intruders, that try to steal our precious information. This precious information could be like e-banking passwords, confidential emails, or some social media private conversations. So, to make our data secure some safety mechanisms are used. One of those safety mechanisms is cryptography. Cryptography plays a vital role in the security of information [1]. Cryptography is a Greek word which means "study of hidden secrets" [2] [3]. In cryptography plain text message gets converted in some human unreadable form or ciphertext; termed as encryption and at the receiver side, that ciphertext or encoded text gets decoded into plain text which is in human-readable form; termed as decryption. So, from this, it is stated that decryption is the reverse process of encryption. The system which performs both encryption and decryption is called cryptosystem. Figure 1 shows how encryption and decryption were done.

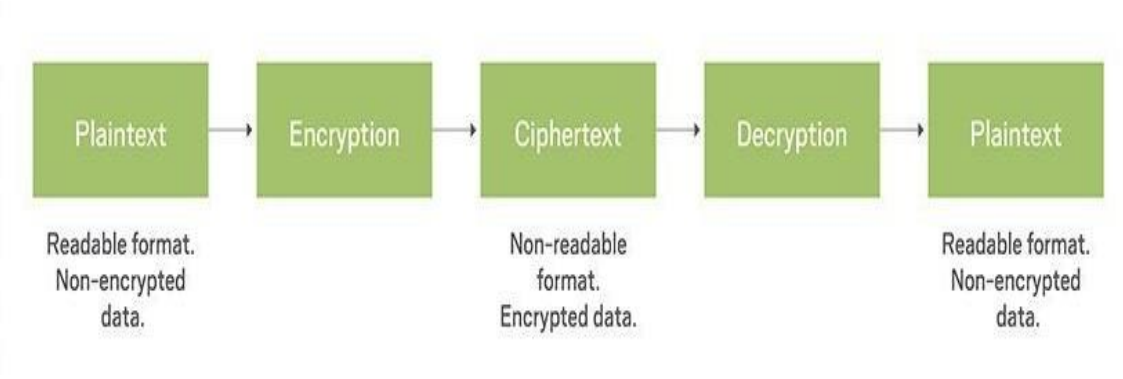

Figure 1: Cryptography [1]

The main aim of cryptography is to provide integrity, authentication, confidentiality, authorization, and availability [4] [5].

1. Integrity: When data is exchanged between two parties, the receiver has to ensure that data sent by the intended sender and not been altered by any other unintended person in between transmission. Cryptography secures the data from passive as well as from active attacks.
2. Authentication: when the receiver is not sure who sends the data. Authentication can be achieved either by using username or password, digital signatures or by using secret-key algorithms.
3. Confidentiality: Protecting the data from the disclosure from unintended persons. Other than legitimate users no other can read the data transmitted.
4. Authorization: setting the privileges or access levels to different users on different resources so that each user should get as much access as they need.

5. Availability: the ability of the user to access any resource or any information when needed. When any system gets attacked by the intruder the services of users should not affect. So, cryptography ensures that the user continues to get services even in case of an attack.

In cryptography avalanche effect [1] defines a specific property of encryption algorithm. Avalanche effect is one of the most essential property of any cryptography algorithm. It means that a minor change in plain text or even a bit of plain text gets changed then it should result in a significant change in the plain text or multiple bits of ciphertext should change.
A good cryptography algorithm should always satisfy the following equation:

$$Avalanche > 50\% \text{ [2]}$$

This ensures that the attacker should not easily predict the ciphertext from plain text or vice versa. The cryptography algorithm that does not satisfy the Avalanche effect equation and easily breached by the cryptanalyst.

A. Terms used

Plain Text: The unique message that Alice/sender wants to send to bob/receiver is called plain text. This message is in readable form, anyone can read this message.

Cipher Text: The encoded or encrypted message is called ciphertext. This message cannot be understood by anyone except the sender (who is sending the message) or by the receiver (to whom the data is sent).

Algorithm or cipher: It is a well-defined mathematical function that is used to encrypt or decrypt data.

Key: String of bits that are used by the cryptographic algorithm to convert plain text message into ciphertext [6].

Avalanche effect: if a single bit of ciphertext gets altered then it should alteration multiple bits of a plain text message or vice versa.

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Based on keys used for the encryption and decryption cryptography algorithms are categorized into two types:

1. Symmetric key cryptography
2. Asymmetric key cryptography (public-key cryptography)

A. Symmetric key cryptography (secret key cryptography)

It is also recognized as Private Key Cryptography or secret key cryptography**.** The symmetric key algorithm is divided into two types based on the type of data they use for encryption and decryption processes. In figure 2 categories of symmetric algorithms are shown.

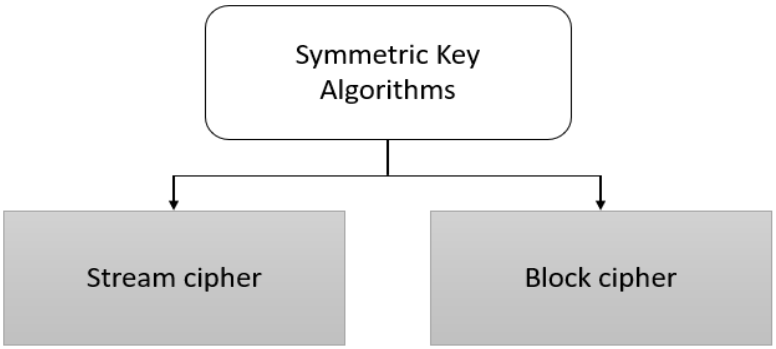

Figure 2: Types of symmetric algorithms

The input of block cipher is a block of plain text and it generates a block of ciphertext, generally of the same size [7]. The size of the block depends upon the scheme the user is using. The choice of block size does not affect the strength of the encryption algorithm. The strength of cipher depends upon the key used in the encryption process. In-stream cipher one bit at a time gets converted into ciphertext. In the symmetric algorithm, the only key is used for encryption and decryption process, which is shared among the sender and receiver during the transmission of data. This key should be kept secret because a single key is responsible for encryption and decryption of data.

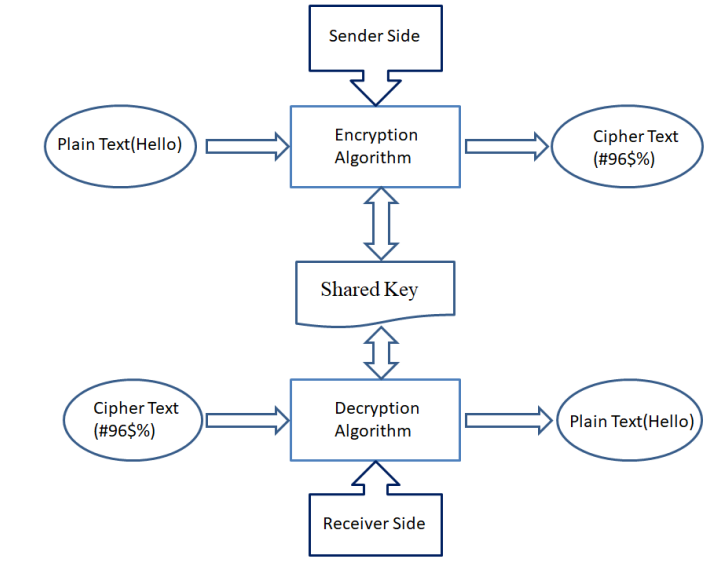

Figure 3: Symmetric key cryptography

Figure 3 shows the encryption and decryption process of symmetric key algorithms.

B. Asymmetric Key Cryptography (secret key cryptography)

In these algorithms, two different keys are used. One key i.e. public key is used for encryption of data and the second key i.e. the private key is used for decryption of data. Data get encrypted with the public key of the receiver which is declared publically and decrypted by the private key of the receiver which is kept secret by the receiver. No key other than the receiver's private key can decrypt data not even key used for encryption can able to decrypt that data [8].

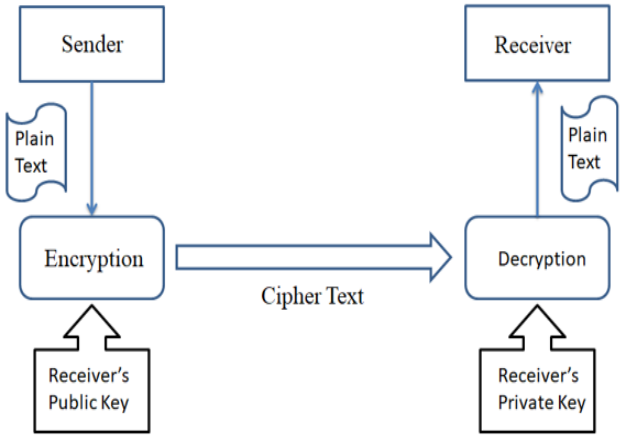

Figure 4: Asymmetric key cryptography

Encryption and decryption process of asymmetric key algorithms are shown in figure 4.

III. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES is one of the most popular cryptography algorithms that is used in modern applications. Another name given to AES is Rijndael. Rijndael was proposed by Joan Daemen and Vincent Rijmen. The name Rijndael was a combination of their surnames (Rijmen and Daemen) [9]. It is used in many protocols such as Secure Sockets Layer (SSL)/Transport Layer Security. Rijndael operates on a mathematical concept known as the Galois field theory [10]. The plain text block size varies from 128 bits to 256 bits [11]. Table 1 shows the key size, plain text block, and several rounds.

Table 1: Round Length

Key Size	Block Size	Number of Rounds
128	128	10
192	128	12
256	128	14

Number of rounds in AES is variable and depends on the length of the key [12] [13]

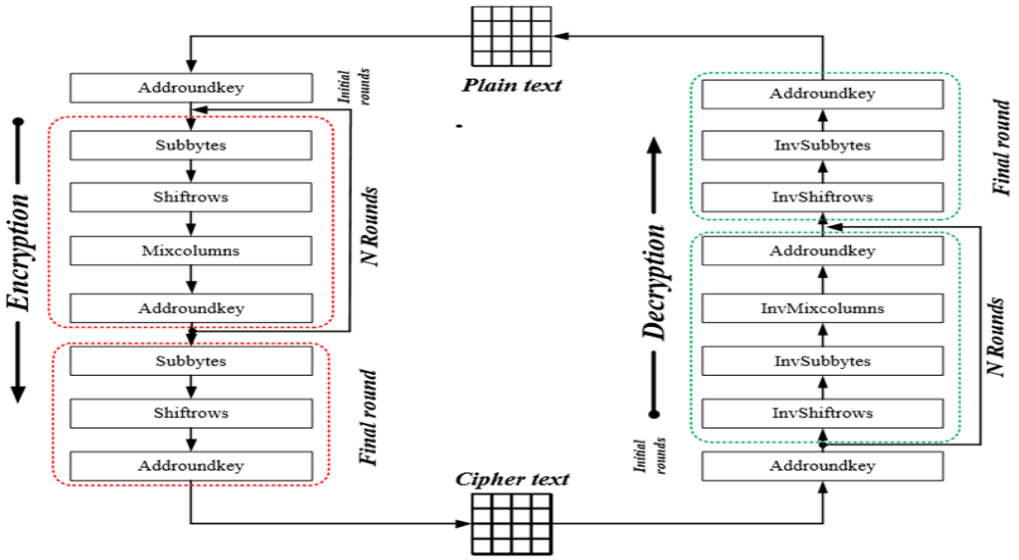

Figure 5: Advanced Encryption Standard [14]

Each round uses a different 128-bit round key, which is calculated from the original AES key.

IV. RSA ALGORITHM

RSA algorithm is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman [15]. It was developed in 1978. It is based on a mathematical fact that it is easy to find and multiply two large prime numbers but factoring them is a difficult task [16]. The private and public key used for encryption and decryption is based on this fact.

Algorithm:

1. Elect two big prime numbers P and Q.
2. Compute N by multiplying P and Q
   $N = P * Q$
3. Choose the public key E such that it is not a factor of
   (P-1) and (Q-1)
4. Choose the private key D such that it satisfies the following condition
   $(D*E) \bmod (P-1) * (Q-1) = 1$
5. For encryption, calculate cipher text (CT) from plain text (PT)
   $CT = PT^E \bmod N$
6. Send ciphertext (CT) to receiver
7. For decryption calculate plain text (PT) from ciphertext (CT)
   $PT = CT^D \bmod N$

V. PREVIOUS WORK DONE

The study presented by Mandal et al. [17], use two most common algorithms i.e. data encryption standard (DES) and Advanced Encryption Standard (AES) and they are implemented using MATLAB and compared on the basis of avalanche effect occurred due to variation of one bit in the key by keeping plain text constant. They concluded that the avalanche effect of AES is high as compared to DES.
Similarly, Bhat et al. [18], compared DES and AES based on avalanche effect and encryption time in MATLAB and they concluded that AES has a high avalanche effect and DES requires more encryption and decryption time as compare to AES.

VI. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

For the experiment, CrypTool is used as a simulator. The computer used in the simulation was Intel® Core (TM) i7-7700 HQ CPU @ 2.80 GHz with 8 GB of RAM and 1TB HDD. The performance of these algorithms are evaluated on the basis of parameters such as avalanche effect and storage memory required by the algorithms to store ciphertext.
This experiment is performed on two different data:

1) **Data 1:** Contains alphabetical character (cryptography = cryptogrephy).
2) **Data 2:** Contains alphanumeric character (data4 = deta2).

Table 2: Algorithm Setting

Algorithm	Key in Bits	Block Size (Bits)
AES	256	128
RSA	512	64

Table 2 shows the algorithm setting for both types of data.

VII. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental Results of RSA and AES are shown in Table 3.

Table 3: Avalanche effect of algorithms

	Avalanche (AES)	Avalanche (RSA)
Data1	47%	51%
Data2	53%	56%

Table 3 displays the avalanche effect of cryptography algorithms. The results show that AES has a low avalanche effect therefor anyone can easily find out the plain text from the ciphertext. Whereas RSA has a high avalanche effect which makes RSA more secure.

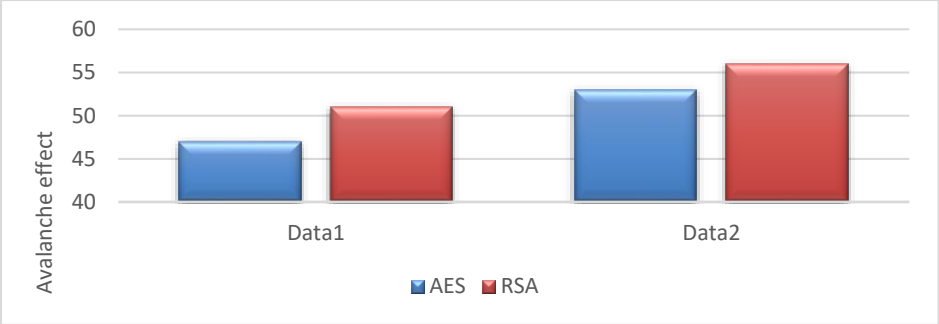

Figure 6: Avalanche effect of algorithms

Figure 6 is a graphical representation of the avalanche effect. For analysis single character of plain text data is changed. The comparison shows that AES has significantly below average avalanche effect for data1. So, AES is not suitable for the encryption of a single character type of data. Whereas RSA performs well in both the cases hence making it suitable for the encryption and decryption process.

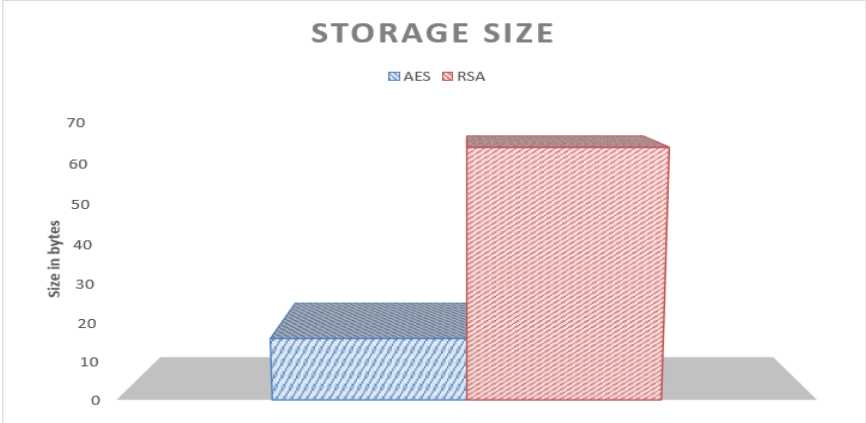

Figure 7: Storage size of algorithms

Figure 7 shows that in terms of storage space needed RSA performs poorly as RSA needs more storage space as compared to the AES algorithm. RSA needs four times more storage space as compared to the AES algorithm. If someone has storage as a constraint then AES can be used as a prime cryptography algorithm.

VIII. CONCLUSION AND FUTURE WORK

In the security of data, cryptography plays an important role. This work presents the comparative study of cryptographic algorithms i.e. RSA and AES on the basis of avalanche effect and storage space these algorithms needed. An experimental result shows that RSA has a high avalanche effect as equating to AES which makes it difficult to break. Plain text encrypted with the RSA has more security other than plain text encrypted with AES. In terms of memory required, AES needs less storage memory. So, from a security point of view, RSA is an ideal algorithm for encryption. In the future, these algorithms can be implemented on different simulators. New performance matric can be formed which can give more ideas about these algorithms and their effect on the data.

REFERENCES

[1] A. Kumar and N. Tiwari, "Effective Implementation and Avalanche Effect of AES", *International Journal of Security, Privacy and Trust Management*, Vol. 1, No. ¾, pp. 31-34, 2012.

[2] Md. A. Hossain, Md. B. Hossain, S. Md. Imtiaz and Md. S. Uddin," Performance Analysis of Different Algorithms," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, No. 3, pp. 659-665, 2016.

[3] T. Limbong and P. D. P. Silitonga, "Testing the Classic Cipher Cryptography using of MATLAB", *International Journal of Engineering Research and Technology*, Vol. 6, No. 2, pp. 175-178, 2017.

[4] A. Khate, "Cryptography and Network Security," 2nd ed., in *Tata McGraw Hill Education Private Limited, New Delhi*, pp. 7-10, 2003.

[5] R. Sinha, H. K. Srivastva and S. Gupta," Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", *International Journal of Scientific & Engineering Research*, Vol. 4, No. 5, pp. 720-725, May 2013.

[6] A. A. Hasib and A. A. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," in *Third 2008 International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 505-510.

[7] P. C. Mandal, "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 9, pp. 196-201, 2012.

[8] Md. I. Alam and M. R. Khan," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, No. 10, pp. 713-720, 2013.

[9] J. Daemon and V. Rijmen, "AES Proposal: Rijndael", 1999.

[10] V. K. Singh and M. Dutta, "ANALYSING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK," *International Journal of Advanced Studies in Computer Science and Engineering*, Vol. 3, No. 4, pp. 1-9, 2014.

[11] D. Selent, "Advanced Encryption Standard," *Rivier Academy Journal*, Vol. 6, No. 2, 2010.

[12] G. Kaur and M. Mahajan, "Analyzing Data Security Algorithms in Cloud Computing Using Cryptographic Algorithms," *International Journal of Engineering Research and Applications*, Vol. 3, No. 4, pp. 782-788, Sept-Oct 2013.

[13] R. Kaur and S. Kinger, "Analysis of security Algorithms in Cloud Computing," *International Journal of Application or Innovation in Engineering & Management*, Vol. 3, No. 3, pp. 171-176, March 2014.

[14] X. Zhang and K. K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm," *IEEE Circuits and Systems Magazine*, Vol. 2, No. 4, pp. 24 – 46, 2002.

[15] P. Rogaway, M. Bellare and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption," *ACM Transactions on Information and System Security*, Vol. 6, No. 3, pp. 365-403, August 2003.

[16] S. Nagpal, "Quantum Cryptography Integrated Effective Communication Approach for WPAN," *International Journal of Enhanced Research in Management & Computer Applications*, Vol. 5, No. 9, pp. 1-5, Sept 2016.

[17] A. K. Mandal, C. Parakash and A. Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", in *IEEE Students Conference on Electrical, Electronics and Computer Science*, 2012.

[18] B. Bhat, A. W. Ali and A. Gupta, "DES and AES Performance Evaluation", in *International Conference on Computing, Communication and Automation*, 2015, pp. 887-890.

WEB REFERENCES

[1] M. Rouse, Cryptography, Sept. 2018, Accessed on 02/03/2020 at 11:10 PM. [Online]. Available: https://searchsecurity.techtarget.com/definition/cryptography

[2] Accessed on 03/03/2020 at 12:13 AM. [Online]. Available: https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/