# Cryptography: A Comparative Analysis of AES and RSA Algorithms

**Rohit Verma**
*Department of Computer Science, Himachal Pradesh University, Shimla, India*

**Aman Kumar Sharma**
*Department of Computer Science, Himachal Pradesh University, Shimla, India*

## ABSTRACT

Security of digital data is the main concern in today's era. Especially when someone is transmitting data over the internet there is always a risk of data misuse. It is possibility that when two parties are communicating over the internet someone is reading their messages or when transmitting confidential information like (E-Banking passwords) someone got that and misuses that. So, there is always a need for security of data. This can be achieved by Cryptography. Cryptography algorithms are of two types: symmetric key cryptography and asymmetric key cryptography. This paper discusses the most famous symmetric key cryptography algorithm AES and asymmetric key cryptography algorithm RSA. These two algorithms are compared, and this comparison is performed on three different machines and two identical machines but differs in CPU usage and Memory usage and these algorithms are operated on three different types of data. Then these algorithms will be analyzed based on encryption and decryption time and factors that affect the encryption and decryption of algorithms.

**Keywords:** AES, Cryptography, Encryption, Performance Analysis, RSA, Symmetric.

## 1. INTRODUCTION

The vital necessity of security is the protection of the computer system and digital information from unauthorized users or intruders. By mean of security, one can hide his/her data from irrelevant users and malicious attackers [1]. Basic principles of security are [2] [3] [4] [5]:

- Authentication
- Authorization
- Integrity
- Confidentiality

Fig. 1 shows relation between various security principles.
One of the most common and popular computer-based security mechanism is cryptography. Cryptography is a Greek word which is a combination of two words kryptós which means "hidden or secret" and graphein which means "to write or study" [18]. So, cryptography can be called as "the study of hidden secrets".

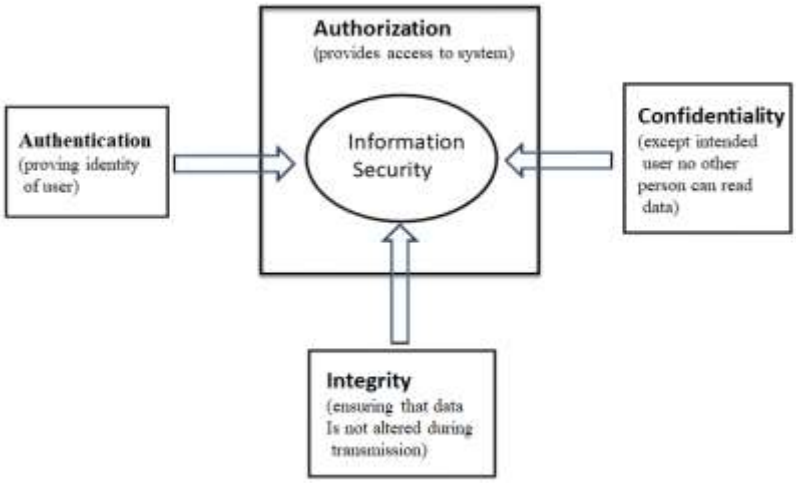


**Figure 1: Principles of security**

One of the most common and popular computer-based security mechanism is cryptography. Cryptography is a Greek word which is a combination of two words kryptós which means "hidden or secret" and graphein which means "to write or study" [18]. So, cryptography can be defined as "the study of hidden secrets". One technique to implement cryptography is "Encryption". Encryption is the process of converting plain text message into some encoded message or cipher text which is in unreadable forms. This unreadable form of message is totally different from the original plain text message. For encryption, an algorithm and key is needed. Key is a string of bits that are used by the cryptographic algorithm to convert plain text message into cipher text [1]. Key is a core part of the encryption process. Security of data depends upon the length of the key. If a weak key is used for encryption then it becomes very easy for intruder or attacker to decrypt data and read it. Decryption is the reverse process of encryption. Decryption is the process of converting encrypted/encoded/cipher text into plain text or in human-readable form. For decryption, an algorithm is needed which is usually the same for both encryption and decryption and key which can differ. Figure 2 represents how encryption and decryption are done.

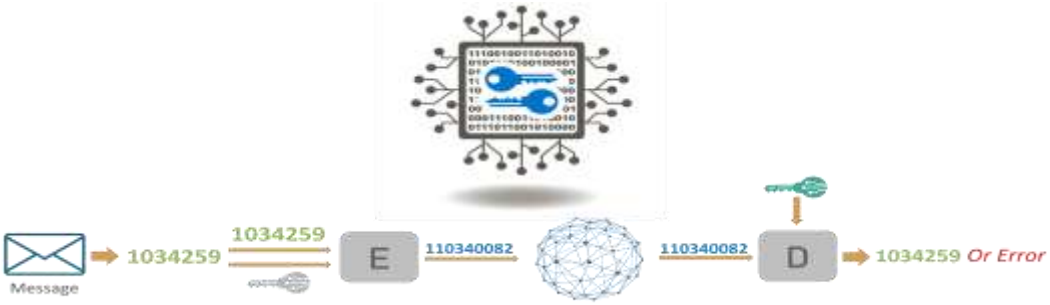


**Figure 2: Encryption and Decryption [2]**

## 1.1 Basic terms used in cryptography

**Plain Text:** The original 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 cipher text. 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.

**Encryption Time:** Time taken to convert plain text into cipher text.

**Decryption Time:** Time taken to convert cipher text into plain text.

## 2. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms have advanced over time along with the evolution of computer systems and data.
There are two categories of cryptographic algorithms that are listed below:

- Symmetric key cryptography (Secret Key)
- Asymmetric key cryptography (Public Key)

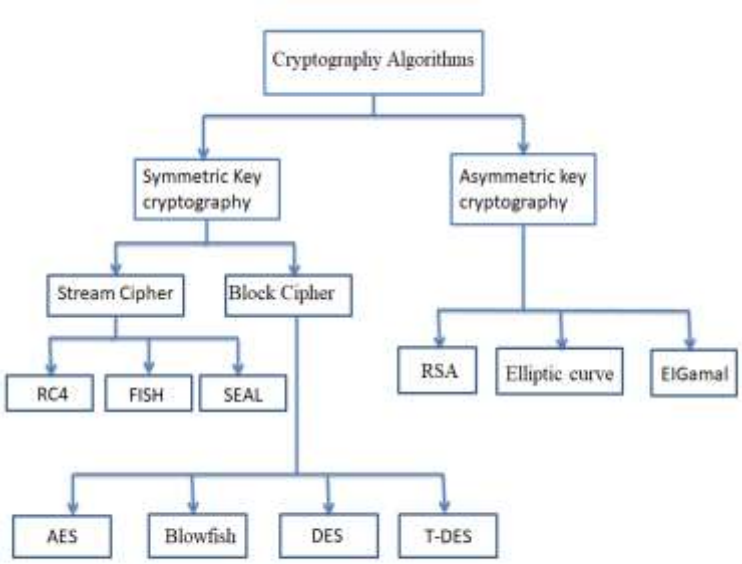


**Figure 3:** Types of cryptography algorithms

These two categories of algorithm are further divider into sub categories as shown in Fig. 3.

### 2.1 Symmetric Key Cryptography

It is also called as Secret Key Cryptography/Private Key Cryptography. In these types of algorithms single key or shared key is used for encryption and decryption process which is shared among both parties during the transmission. This key should be kept secret because if anyone gets access to the key he/she can easily decrypt the data and read or alter it. Before the transmission of data both the parties i.e. sender and receiver must agree upon the key. There are different mechanisms that are used for a key generation like Diffie-Hellman Key Exchange/Agreement algorithm [1] [6] which are based on some mathematical principles. Some of the symmetric algorithms are AES, DES, T-DES, Blowfish, etc. Fig. 4 shows the encryption and decryption process of symmetric algorithms.

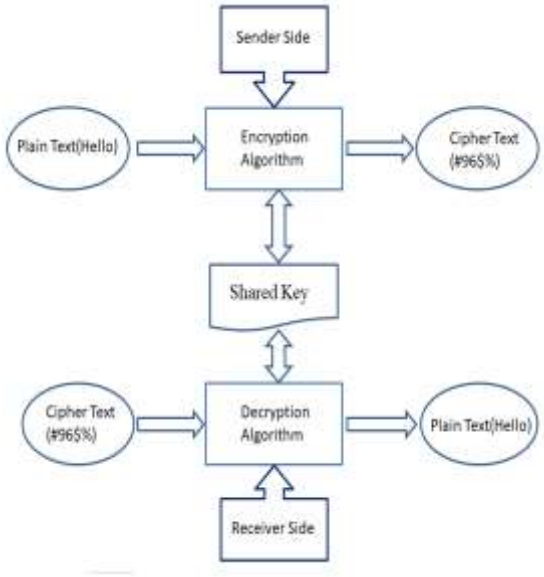


**Figure 4**: **Encryption and Decryption**

## 2.2 Asymmetric Key Cryptography

Another name of asymmetric key cryptography is Public Key Cryptography. In these algorithms, two different keys are used to form a key pair. One key (known as a private key) [20] is used for decryption of data and another key (known as public key) id used for encryption of data. A public key is announced publically or shared with everyone. No key other than receiver's private key can decrypt data not even key used to encryption can able to decrypt that data. Fig. 5 shows the encoding and decoding process of asymmetric algorithms.

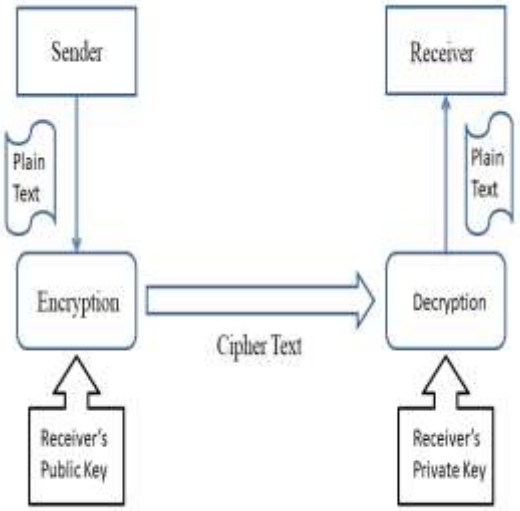


**Figure 5: Encoding and decoding of asymmetric algorithms.**

## 3. RSA ALGORITHM

RSA is the most general and broadly used public key encryption algorithm [7] [8]. RSA algorithm is named after its three inventors Ron Rivest, Adi Shamir, and Leonard Adleman [19] [21]. It is

developed back in 1978. RSA is based on a mathematical fact that it is easy to find and multiply two large prime numbers but to factor their product is an extremely difficult task. The private and public key used in RSA for encryption and decryption is based on large prime numbers. Security provided by RSA algorithm depends upon the length of prime numbers; large prime numbers provide more security whereas small prime numbers provide less security. However, RSA has many faults in its design [9].

**Algorithm:**

1. Elect two large prime numbers P and Q.

2. Compute N by multiplying P and Q

$$P * Q = N$$

3. Select the public key E (Encryption Key) such that it is not a factor of

$$(P-1) \text{ and } (Q-1)$$

4. Select the private key D (Decryption Key) 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)

$$PT^E \bmod N = CT$$

6. Send cipher text (CT) to receiver

7. For decryption calculate plain text (PT) from cipher text (CT)

$$CT^D \bmod N = PT$$

## 4. AES ALGORITHM

Full form of AES is Advanced Encryption Standard. It is also called as Rijndael. It was invented by Joan Daemon and Vincent Rijmen. AES was developed to overcome the weaknesses of DES algorithm. In AES algorithm, the plaintext block size varies from 128 to 256 bits. One of the three keys for encryption and decryption purpose can be used i.e. 128 bit, 192 bit, 256 bit. It uses 10, 12, 14 rounds which depend on the type of key used for example if 128-bit key is used then 10 round encryption and decryption process is used. Similarly, for 192-bit key 12 round encryption and decryption is used and for 256-bit key 14 rounds is used. Encryption process starts from "Add round key stage". In each round 4 transformation processes takes place.

- **Substitute byte transformation or sub-bytes:** AES uses 128-bits block of data. In sub-bytes transformation, every bit of data gets transformed by other data using 8-bit substitution box or also called as Rijndael s-box.

- **Shift Row transformation:** The bytes of data in three rows are shifted in a left cycle way. In second row one-byte circular left shift is done and in third and fourth row two and three bytes left shift is done.
- **Mix Column transformation:** In this stage multiplication of every column is done with a stable matrix.
- **Add round key transformation:** In this stage, XOR operation is performed among 128-bits of the current state and 128-bits round key.

## 5. PREVIOUS WORK DONE

Several works have been done in past years to find which algorithm is efficient and good for encoding and decoding. The paper offered by **Nadeem et al.** [10], the popular and widely used secret key algorithms (DES, AES, T-DES, Blowfish) were compared, their implementation was done in Java platform (JDK 1.4). These algorithms were implemented using uniform programming language i.e. Java and tested on two different machines and then compared on the basis of encryption time for varying size of data.

The study presented by **Penchalaiah et al. [11],** they analyze the structure and design of DES (Data Encryption Standard) and AES (Rijndael Cipher). The main reason to carry out this study is to find out the similarities and dissimilarities of DES and AES.

**Settia** [5] did cryptanalysis on various secret key algorithms like IDEA, DES, RC2, RC4, AES, and TDES. The cryptographic simulator CrypTool was used to analyze the possible attacks on these algorithms. It was observed that these algorithms can be broken by Brute force attack. If a large key was used, then CPU time can drastically increase and 2128 key range can be considered secure for the current era.

**Seth et al.** [12] relate three most popular algorithms RSA, DES, AES. They conclude that DES requires least encryption time as compared to other two and AES requires least memory. Whereas RSA requires longest encryption time and consumes most memory.

**Thakur et al**. [13] relate three encryption algorithms (DES, AES, and Blowfish) and results shows that Blowfish is the perfect algorithm in terms of performance.

Another study performed by **Marwah et al.** [14], they compare three algorithms namely RSA, DES, TDES. The results show that TDES is the optimal algorithm in terms of security. DES required less memory as compared to TDES and RSA.

In the work presented by **Mandal et al.** [15], they compared symmetric key algorithms based on performance and then propose a new algorithm. Throughput of their proposed algorithm is high and power consumption is less.

**Apoorva et al.** [16] analyzed that Blowfish is the ideal algorithm for encryption and decryption and it requires less energy.

Another study that was carried out by **Abood et al.** [17], they have done a comparison of asymmetric and symmetric algorithms and conclude that symmetric key algorithms can encrypt and decrypt data more rapidly than asymmetric algorithms.

## 6. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

For the experiment, in this experiment CrypTool is used as a simulator. It contains inbuilt tools for analysis and provides visual results. On five machines experiment has performed. Among these five machines, three have different configurations and two machines have the same configurations but CPU utilization and Memory consumption of these machines are different. Configurations of machines used are given below:

- **System 1:** Intel® Atom (TM) CPU N2600 @ 1.60 GHz
- **System 2:** Intel® Core (TM) i5-8500 CPU @ 3.00 GHz
- **System 3:** Intel® Core (TM) i7-7700 HQ CPU @ 2.80 GHz
- **System 4:** Intel® Core (TM) i7-4790 CPU @ 3.60 GHz (CPU utilization = 2% and memory utilization = 64%)
- **System 5:** Intel® Core (TM) i5-8500 CPU @ 3.00 GHz (CPU utilization = 14% and memory utilization = 51%)

This experiment is performed on three different data. Table 1 shows the description of data used.

**Table 1: Type of Data Used**

| | **Size** | **No. of Records** | **No. of Images** | **No. of Tables** | **No. of Gif** |
|---|---|---|---|---|---|
| **Data 1** | 90 Kb | 13161 | - | - | - |
| **Data 2** | 291 Kb | 1081 | 14 | 5 | - |
| **Data 3** | 5750 Kb | 1081 | 14 | 5 | 5 |

Both the algorithms are evaluated according to their Encryption and Decryption time, and how they perform on different environments at different data.

**Table 2: Algorithm Setting**

| **Algorithm** | **Data 1 (Key in Bits)** | **Data 2 (Key in Bits)** | **Data 3 (Key in Bits)** | **Block Size (Bits)** |
|---|---|---|---|---|
| AES | 256 | 256 | 256 | 128 |
| RSA | 512 | 512 | 512 | 64 |

Table 2 shows the algorithm setting used in experiment.

## 7. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental Results for RSA and AES are shown in Table 3 and Table 4.

**Table 3**: Encryption time of AES

| **Hardware System** | **Dataset 1** | **Dataset 2** | **Dataset 3** |
|---|---|---|---|
| **System 1** | 56 | 490 | 858 |
| **System 2** | 24 | 92 | 632 |
| **System 3** | 25 | 81 | 513 |
| **System 4** | 20 | 71 | 502 |
| **System 5** | 20 | 73 | 503 |

Table 3 displays the encryption time of AES algorithm in milliseconds working on dissimilar hardware environment where different type of data used.

Similarly, Table 4 displays the encryption time of RSA algorithm in milliseconds working on dissimilar hardware environment where different type of data used.

**Table 4: Encryption time using RSA algorithm (in milliseconds)**

| Hardware System | Dataset 1 | Dataset 2 | Dataset 3 |
|---|---|---|---|
| **System 1** | 188 | 672 | 10109 |
| **System 2** | 30 | 96 | 1593 |
| **System 3** | 28 | 85 | 1397 |
| **System 4** | 24 | 80 | 1286 |
| **System 5** | 24 | 82 | 1314 |

From Table 3 and Table 4, it is concluded that AES needs less encryption time as compare to RSA algorithm. These algorithms run differently on different hardware environments.

**Table 5: Decryption time of AES (in milliseconds)**

| Hardware System | Dataset 1 | Dataset 2 | Dataset 3 |
|---|---|---|---|
| System 1 | 59 | 499 | 863 |
| System 2 | 31 | 96 | 640 |
| System 3 | 32 | 89 | 517 |
| System 4 | 24 | 76 | 509 |
| System 5 | 25 | 78 | 511 |

Table 6 displays the decryption time of AES algorithm in milliseconds working on dissimilar hardware environment where different type of data used.

**Table 6:** Decryption time of RSA (in milliseconds)

| Hardware System | Dataset 1 | Dataset 2 | Dataset 3 |
|---|---|---|---|
| System 1 | 2436 | 8000 | 129723 |
| System 2 | 424 | 1393 | 22680 |
| System 3 | 387 | 1182 | 19370 |
| System 4 | 349 | 1134 | 18411 |
| System 5 | 351 | 1135 | 18501 |

Table 6 displays the decryption time of RSA algorithm in milliseconds working on dissimilar hardware environment where different type of data used.

From Table 5 and Table 6, it is concluded that the decryption time of RSA algorithm is approximate twice the amount of time it takes for encryption this is because for encryption and decryption RSA uses modular exponentiation whereas AES uses small and fixed exponents.

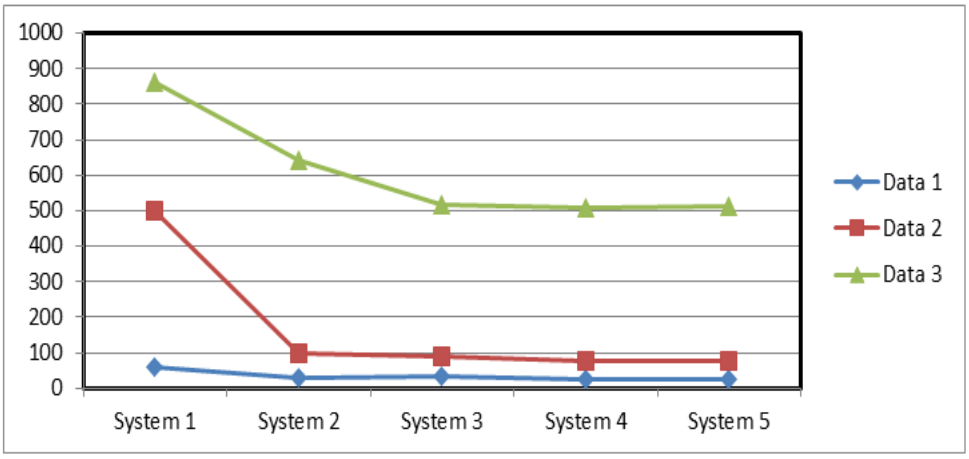


**Figure 6: Encryption using AES algorithm**

Figure 6 and figure 7 shows the time needed for encryption and decryption (in milliseconds) for various data using AES algorithm. From these figures it is concluded that System 1 has poor performance in terms of encryption and decryption time and System 4 performs better for every data.

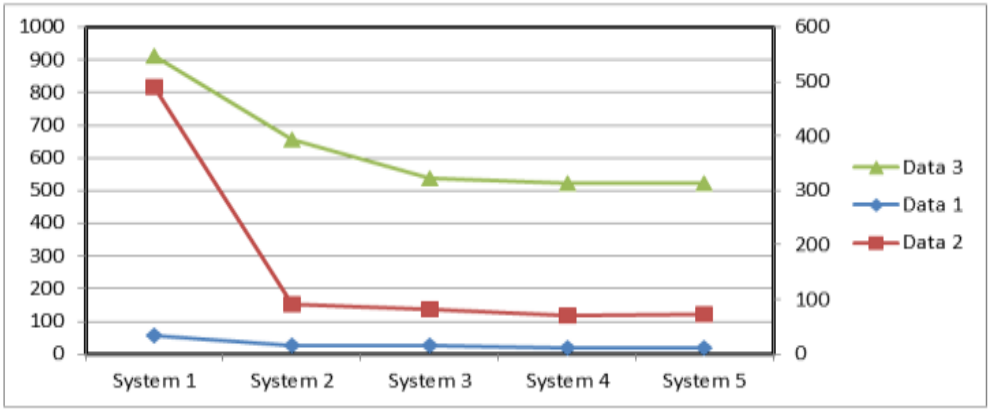


**Figure 7: Decryption using AES algorithm**

Hence, the encryption and decryption rate depends upon the type of data used and type of system on which encryption and decryption is performing. CPU usage and memory usage also perform a huge role in encryption and decryption of data.

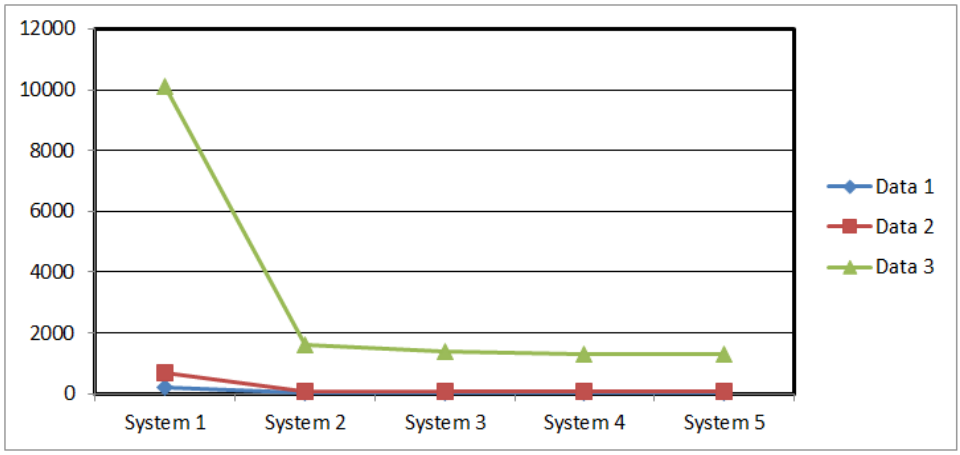


**Figure 8: Encryption using RSA algorithm**

Figure 8 shows the time need for encrypting different type of data using AES algorithm by different machines. Here, System 1 required large amount of time and time required by other Systems are nearly same.

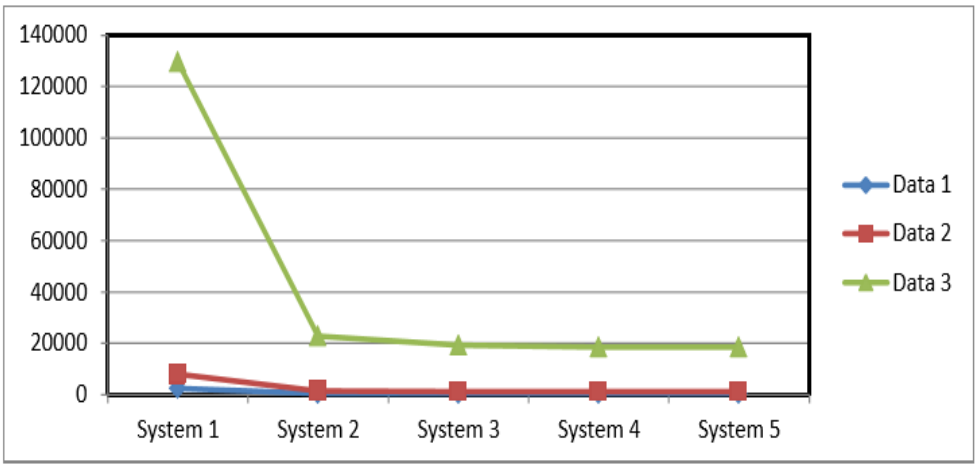


**Figure 9: Decryption using RSA algorithm**

Figure 9 shows decryption time (in milliseconds) needed to decrypt data using RSA algorithm. System 1 has poor performance and other Systems shows nearly same performance.

## 8. Conclusions and future work

Cryptographic algorithms play very important role in securing our digital data when one is communicating over internet. Our research work presents the comparative study of most popular and widely used cryptographic algorithms i.e. RSA and AES. An experimental result shows that encoding and decoding of AES is faster than RSA algorithm, but it fails to provide that much security, but RSA cryptosystem can be broken by numerous attacks. For encryption and decryption of large and complex data RSA takes huge amount of time but provides great security. From the analytical results, it is clear that AES is superior to RSA algorithm. System 1 has poor performance in terms of encryption and decryption time and System 4 performs better for every data.

Encryption and decryption time depend upon following parameters: -

- Type of data

- Type of system
- CPU Utilization

In future these algorithms can be compared based on some different performance factors and can be implemented at different simulators. New Hybrid algorithm can be developed using the features of AES and RSA algorithm.

## REFERENCES

[1] 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.

[2] R. Helton and J. Helton, "Mastering Java Security: Cryptography, Algorithm and Architecture", in *Wiley Publishing Inc*., USA, 2002, pp. 6-9.

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

[4] 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.

[5] N. Settia, "Cryptanalysis of Modern Cryptographic Algorithms," *International Journal of Computer Science and Technology*, Vol. 1, No. 2, pp.166-169, Dec 2010.

[6] R.L. Rivest, A. Shamir and L. Adleman," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, No. 2, pp.120-126, Feb 1978.

[7] S. Pavithra and E. Ramadevi, "Study and Performance Analysis of Cryptography Algorithms," *International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 1, No. 5, pp.82-86, July 2012.

[8] X. Zhou and X. Tang," Research and Implementation of RSA Algorithm for Encryption and Decryption," in *6th International Forum on Strategic Technology*, pp. 1118-1121, 2011.

[9] S. O. AL. F. M. Koko and A. B. A. N. Mustafa, " Comparison of various Encryption Algorithms and Techniques for improving Secured data communication," *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 17, No. 1, pp. 62-69, 2015.

[10] A. Nadeem and M. Y. Javed, "A Performance Comparison of Data Encryption Algorithms," in International Conference on Information and Communication Technologies, 2005, pp. 8489.

[11] N..Penchalaiah and R.Seshadri," Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", *International Journal on Computer Science and Engineering*, Vol. 02, No. 05, 1641-1645, 2010.

[12] S. M. Seth and R. Mishra,"Comparative Analysis Of Encryption Algorithms For Data Communication," *International journal of Computer Science and technology*, Vol. 2, No. 2, pp. 292-294, 2012.

[13] J. Thakur and N. Kumar," DES, AES, Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," *International Journal of Emerging Technology and Advanced Engineering*, Vol. 1, No. 2, pp. 6-12, 2011.

[14] M. Marwaha, R. K. Bedi, A. Singh and T. Singh,"Comparative analysis of Cryptographic algorithms," *International Journal of Digital Technology and Economy*, Vol. 1, No. 2, pp. 127-134, Sept 2013.

[15] B. K.Mandal, D. Bhattacharyya and S. K. Bandyopadhyay," Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm," in *International Conference on Communication Systems and Network Technologies*, pp. 453-461, 2013.

[16] Apoorva and Y. Kumar," Comparative Study of Different Symmetric Key Cryptography Algorithms," *International Journal of Application or Innovation in Engineering and Management*, Vol. 2, No. 7, pp. 204-206, 2013.

[17] O. G. Abood and S. K. Guirguis,"A Survey on Cryptography Algorithms," *International Journal of Scientific and Research Publications*, Vol. 8, No. 7, pp. 495-516, 2018.

[18] 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.

[19] D. Pugila, H. Chitrala, S. Lunawat and P. M. D. R. Vincent," An Efficient Encryption Algorithm Based on Public Key Cryptography," *International Journal of Engineering and Technology*, Vol. 5, No. 3, pp.3064-3067, 2013.

[20] 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.

[21] A. Ganpati and N. Tyagi,"A Survey of Different Public-Key Cryptosystems," *International Journal Of Computer Science Trends and Technology*, Vol. 3, No. 6, pp. 66-70, 2015.

**WEB REFERENCES**

[1] techopedia. Cryptographic Key [Online]. Available: https://www.techopedia.com/definition/24749/cryptographic-key
Accessed on 20/09/2019 at 12:08 am

[2] dureka. What is Cryptography? – An Introduction to Cryptographic Algorithms [Online]. Available:edureka.co/blog/what-is-cryptography
Accessed on 20/09/2019 at 12:15 am