International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3680

E-ISSN : 2454-6135

Volume.7, Issue 1
January -2021

Improved key of RSA Algorithm Generated from The image based on SHA256 Algorithm

Rasha Thamer Shawe

Assistant Teacher

Department of Computer Science

Collage of Education, Mustansiriyah University

Baghdad- Iraq

ABSTRACT

At the present time, information security has become very necessary and is considered a very difficult problem in the event that it is exposed by the attackers and becomes easy and available to them. Therefore, data protection and non-disclosure to unauthorized persons are required to do so. The solution is to encrypt it and there are a large number of encryption algorithms in use. In this paper, both the RSA generic encryption algorithm and the hash algorithm known as SHA256 were used, in which the RSA algorithm was improved by generating the algorithm keys from an image generated with the SHA256 hashing algorithm. Where two keys are formed, one of which is public for encryption and is available and the other is a private key that is not disclosed only to the person who has access to the message, and effective encryption of the data was produced in addition to the retrieval of the original text. The proposed method has been programmed in VisualBaic.Net 2012 language.

Key Words: *RSA, SHA256, Cryptography, Decryption, Encryption.*

1. INTRODUCTION

Due to the rapid growth in Internet technology and the transfer of large data via the Internet, therefore the role of data security necessitated a difficult problem and there is an urgent need to protect data and transfer it safely via the internet. Encryption, a word that means "secret writing" and is of Greek origin. Where the message that has not been subject to any encryption algorithms is known as the plain text, while the encryption algorithms are run on it by the encrypted text. When the message is received from the other party, it is necessary to decrypt it and return it to the plain text [1]. The coding and decoding work is shown in Figure 1 [2]. Figure 1: illustrates the sending of an encrypted message by the sender that encrypted the secret key and then sends it to the recipient, then the receiver decrypts the message based on the secret key. Encryption is characterized by providing a number of security objectives to ensure the privacy of data and not change the data, etc. Due to the great security advantages of encryption, it is widely used today [3].

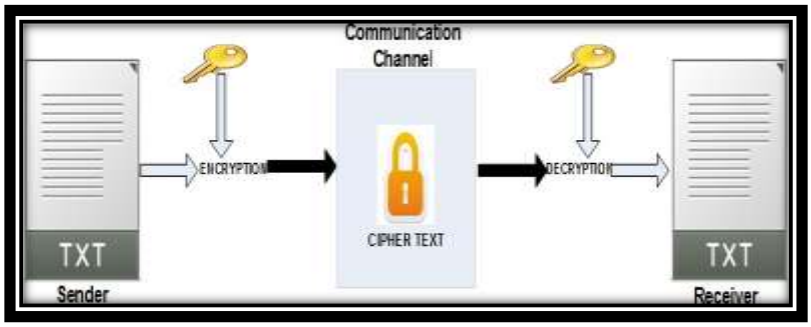

Figure .1: Encryption and decryption work[3].

Licensed Under Creative Commons Attribution CC BY

2. CLASSIFICATION OF CRYPTOGRAPHY

The encryption algorithms are classified into two broad categories: public key encryption and private key encryption as well as hash algorithms [1].

A. Private Key Cryptography

The private algorithm is also called shared key cryptography. This type of encryption has the advantage of using the same key in both the encryption and decryption process during data transfer [4]. There are multiple types of proprietary algorithms such as Advanced Encryption Standard (AES), Blowfish, Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES) [5].

b. Public Key Cryptography

This type of encryption uses two keys, one of which is used for encryption, which is a "public key" and the other is used for decryption, which is a "private key" [4]. There are several types of general algorithms, other than Rivest Shamir Adlemen (RSA), ECC, Digital Signature Algorithm (DSA), etc [5].

c. Hash Function

This part represents an important role in encryption, as its function is to hash the cipher in the sense of a mathematical function where it creates fixed-size data. There are several algorithms that have relied on this type of them (MD and SHA). This type of encryption is useful in security issues that require security applications, for example digital signatures, authentication, message integrity, etc [6].

3. OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS:

In this part we will describe the algorithms that were used in carrying out this research, namely RSA and SHA256.

A. RSA Cryptography

In 1977, Ron Revist, Adi Shamir and Leonard Adelman presented a cryptographic method that relied on public encryption, as they created two keys, one of them public and the other private, called RSA. This algorithm was based on a mathematical problem called analysis of large integers [7].

This technique uses two exponents (e is used for encryption and d is used for decryption) are the public and private keys [8]

- **Key generation by RSA**

Generating the keys in the RSA algorithm is a time consuming process in addition to being complex and can be calculated by specifying two large prime numbers to calculate the total parameter where the two numbers p and p2 are represented, and the overall parameter is as follows Φ (n) = (p-1) * (q -1) 3. Provided that the general exponent is an integer e with 1 <e.[8].

B. Secure Hash Algorithm (SHA256):

The SHA-256 algorithm is one of the hash algorithms where the output is one-way, where a text is generated as a fingerprint and as a fixed value whose text cannot be retrieved and works as follows [9]:

1- The message, M, is lined by appending bit “1” at the end of the message, followed by k zero

Bits, so its length is identical to 448mod512.

2- The liner message is parsed into N 512 bits’ message blocks, M (1), M (2), ..., M (N), by appending a 64-bit block.

3- The initial hash value, H (0) = IV, consisting of eight 32-bit words, has been set in hexadecimal form.

4- SHA-256 uses a 32-bit sixty-four-word message table. The words for the message table are W0, W1,.. W63.

DOI : 10.31695/IJERAT.2021.3680

4. FRAMEWORK FOR THE PROPOSED METHOD:

In this part, the method of work followed is explained. In this framework, where the key is generated from numeric values generated from an image using the SHA256 hash algorithm, then encrypts the message using the RSA algorithm, and then returns the original text by decoding as shown in the work diagram in Figure 2.

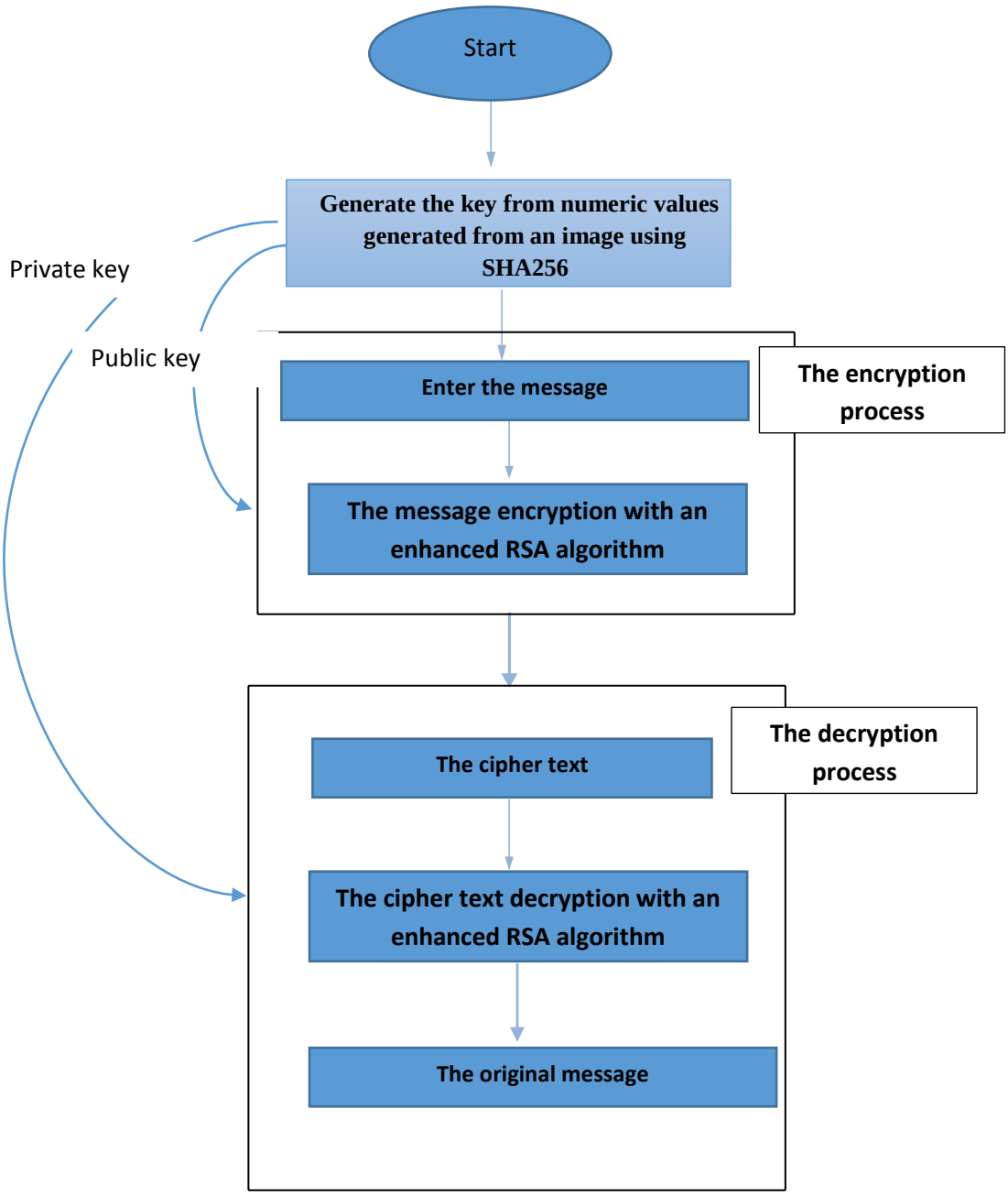

Figure 2. Framework for the proposed method

DOI : 10.31695/IJERAT.2021.3680

5. METHODOLOGY THE PROPOSED METHOD AND ITS IMPLEMENTATION

The proposed system consists of three phases, which are the key generation phase, the encryption process phase, and the decryption process phase. In this paper, we used a new generation method for RSA algorithm from numerical values generated from an image using the SHA256 hash algorithm. Better encryption for RSA is included, as the time that the algorithm takes in the computation of generating it is reduced, and keys generated from numerical values of the SHA256 image are used. The proposed method was efficient in its work and took less time in the encoding and decoding process.

The three phases, according to the proposed method in the research, will be explained as in figure. 6, figure 7 and figure. 8, which represent the key generation phase, the coding phase and the decoding phase successively according to the framework shown in figure.2.

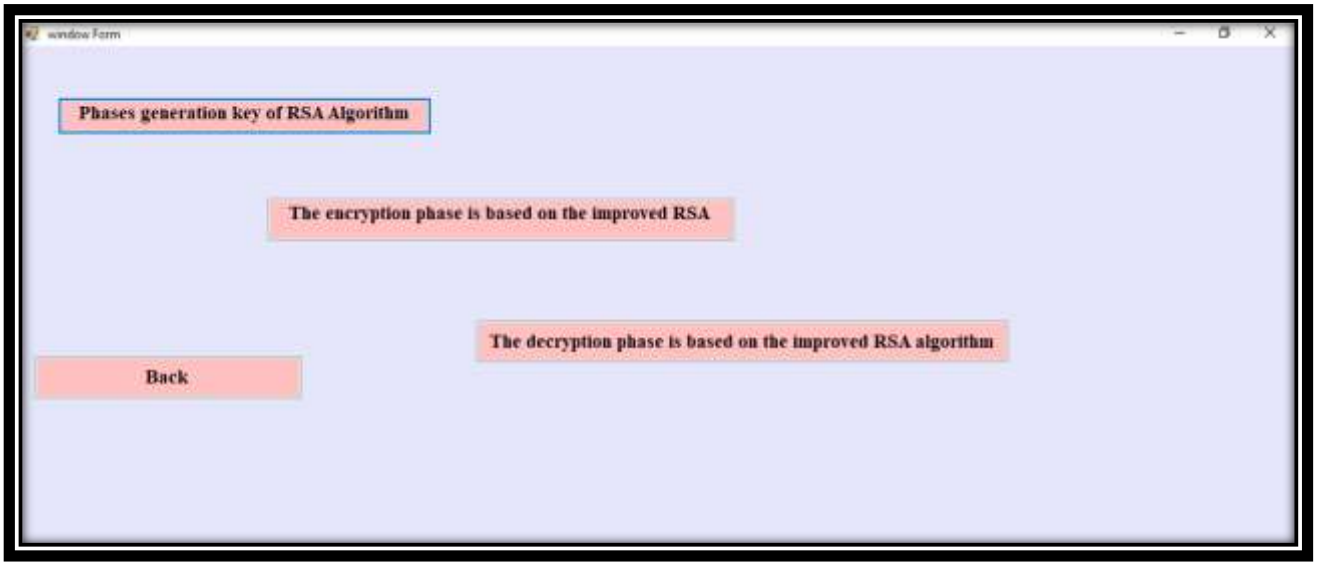

Figure 3. Window form for the proposed method.

➢ The key generation phase

In the key generation stage, an image is loaded and then double-pressed on the SHA256 algorithm. The result is a numeric value representing the key for the RSA algorithm, where it is divided into two parts, one of which is general for encryption and the other is special for decryption, as shown in Figure 4

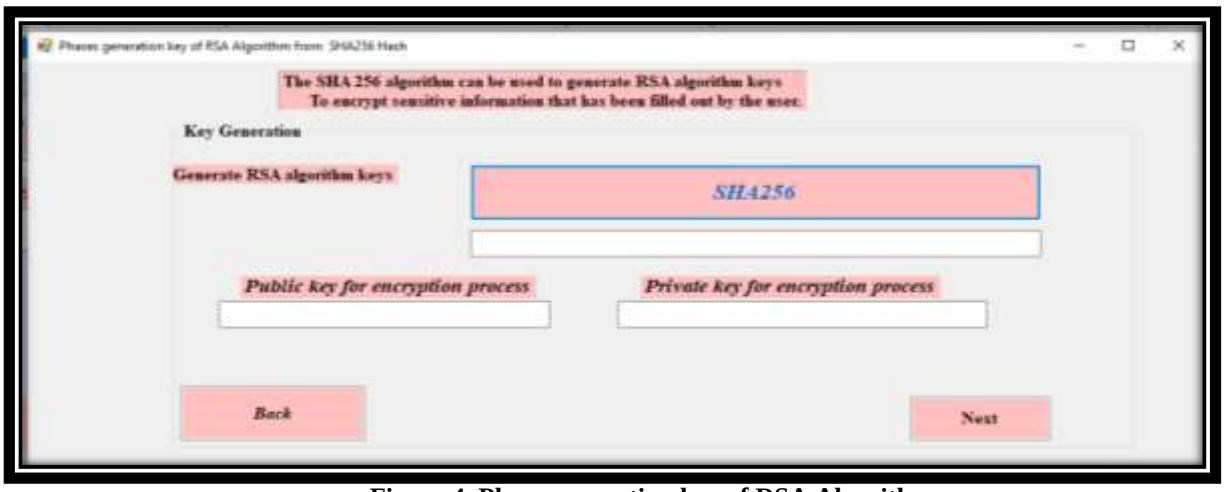

Figure 4. Phase generation key of RSA Algorithm.

DOI : 10.31695/IJERAT.2021.3680

Figure 5. upload of image to generation key of RSA Algorithm.

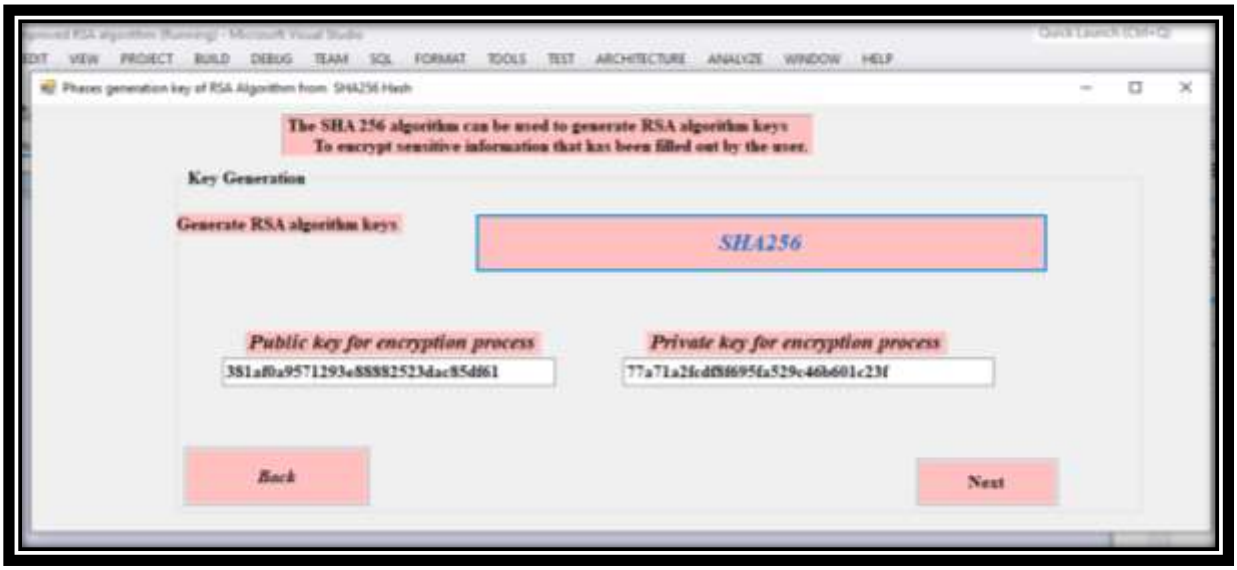

Figure 6. key generated from image using SHA256 Algorithm.

- **The Encryption Stage**:

The message is encrypted using the enhanced RSA algorithm depending on the public key that is generated from numerical values of an image depending on the SHA256 algorithm. The resulting message is encrypted as shown in Figure 7.

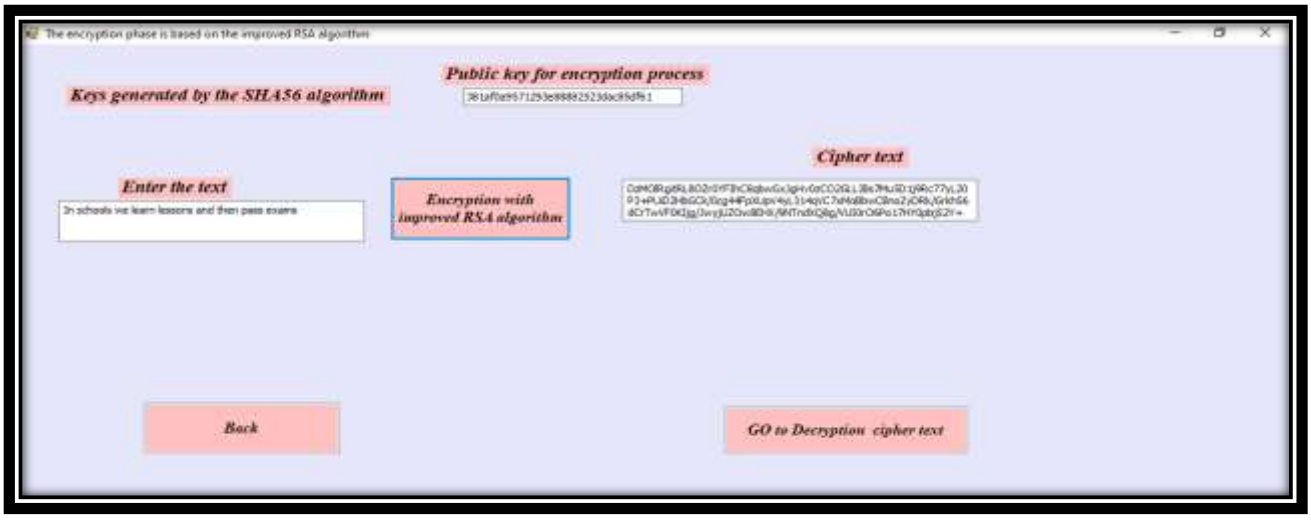

Figure 7. The Encryption phase using Improved of RAS Algorithm.

DOI : 10.31695/IJERAT.2021.3680

➢ The decryption stage:

Here, in this stage, the original text is retrieved using the improved RSA algorithm, depending on the private key that is generated from the numerical values of an image based on the SHA256 algorithm. The result is the original message as shown in Figure 8.

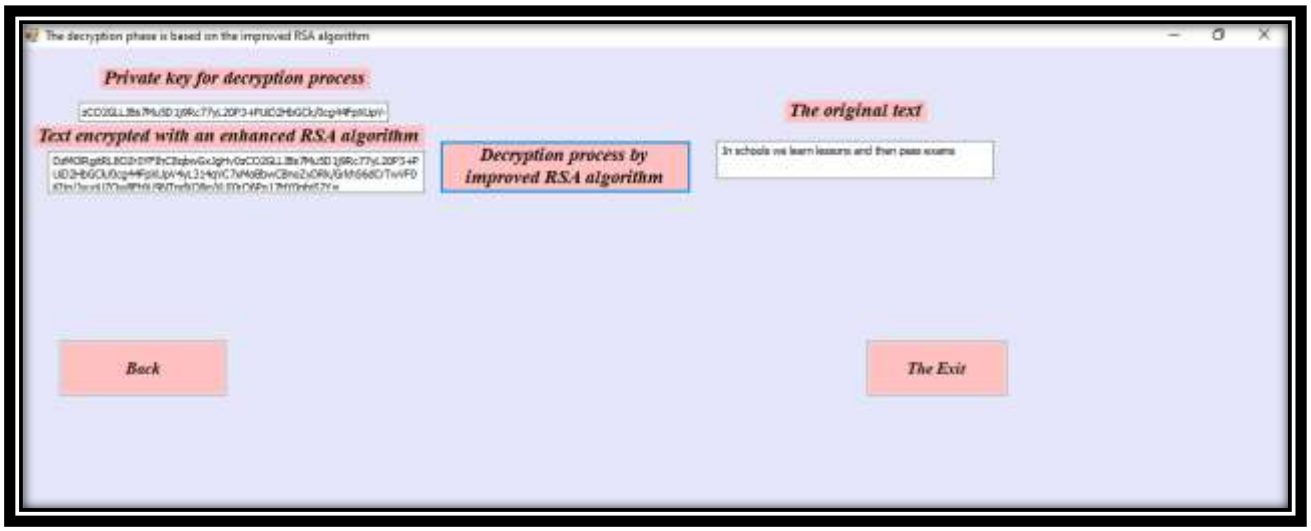

Figure 8. The Decryption phase using Improved of RAS Algorithm.

6. CONCLUSION

In this paper, the combination of the asymmetric encryption algorithm and the hash algorithm give strength in terms of system construction, as a hybrid system with hash function is proposed, which is a combination of RSA and SHA256. The process of generating RSA algorithm keys from the hash algorithm and from the origin of the image is difficult to predict by the attacker, and it gives strength to the proposed system in addition to fast execution as the key generation time was reduced and the encryption process was reduced for the message and returned without implementation restrictions. In the future, we will deal with several algorithms, whether public or private encryption, and use other methods of improving it, whether it is in the key generation stage or otherwise and the data used in the coding in this work, focus on text only. In the future, different types of data can be embedded, including image, video, or audio.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (www.uomusiriyah.edu.iq), Baghdad-Iraq for its support in the present work.

REFERENCES

[1] N. Bisht and S. Singh, “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms”, Int. J. Innovative Res. Sci. Eng. Technol., Vol. 4, no. 3, pp.1028-1031, Mar. 2015.

[2] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, “Cryptography: A Comparative Analysis for Modern Techniques”, Int. J. Adv. Comput. Sci. Appl., Vol. 8, no. 6, pp.442-448, 2017.

[3] P. Verma, J. Shekhar, Preety, and A. Asthana, “A Survey for Performance Analysis Various Cryptography Techniques Digital Contents”, Int. J. Comput. Sci. Mobile Comput., Vol.4, no.1, pp. 522-531, Jan. 2015.

[4] Verma, P. Guha, and S. Mishra, “Comparative Study of Different Cryptographic Algorithms”, Int. J. Emerg. Trends Technol. Comput. Sci., Vol. 5, no. 2, pp. 58-63, Mar-Apr 2016.

[5] K. Uma, G. Karthik, and R. V. Prasath, “A comparative analysis of Symmetric and Asymmetric key cryptography”, J. Chem. Pharm. Sci., Vol. 10, no. 1, pp.324-326, Jan-Mar 2017.

[6] E. Swathi, G. Vivek, and G. S. Rani, “Role of Hash Function in Cryptography”, in National Conference on Computer Security, Image Processing, Graphics, Mobility and Analytics, India, 2016, pp.10-13.

DOI : 10.31695/IJERAT.2021.3680

[7] K. Keerthi and B. Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption", in International Conference on Circuits Power and Computing Technologies, India, 2017.

[8] A Shankar and G Ayappan, " Medical Image Authentication Using RSA Algorithm with SVD Techniques", International Journal of Trend in Research and Development, Volume 4(6), ISSN: 2394-9333 www.ijtrd.com, IJTRD | Nov-Dec 2017 Available Online@www.ijtrd.com

[9] R. Roshdy1 , M. Fouad2 , M. Aboul-Dahab 3, "DESIGN AND IMPLEMENTATION A NEW SECURITY HASH ALGORITHM BASED ON MD5 AND SHA-256", International Journal of Engineering Sciences & Emerging Technologies, August 2013. ISSN: 2231 – 6604 Volume 6, Issue 1, pp: 29-36 .

DOI : 10.31695/IJERAT.2021.3680