I.J. Information Technology and Computer Science, **2022, 2, 45-53**
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2022.02.04

Implementation of Improved Cryptography Algorithm

Rohit Verma
Department of Computer Science, Himachal Pradesh University, Shimla, India
E-mail: verma.rohit218@gmail.com

Jyoti Dhiman
University Institute of Technology, Himachal Pradesh University, Shimla, India
E-mail: dhimanjyoti831@gmail.com

Received: 01 October 2021; Accepted: 23 December 2021; Published: 08 April 2022

Abstract: A network is an interconnected group of independent computing devices which uses a different set of protocols to communicate with each other independently and meaningfully. This communication should be carried out securely. Due to different attacks, this security sometimes gets compromised. So, to communicate securely different cryptography algorithms are used i.e., symmetric and asymmetric algorithms. Cryptography helps to achieve authentication, confidentiality, integrity, non-repudiation, and availability of data. Nowadays many algorithms provide security to data but these algorithms have various security flaws. To improve the strength of these algorithms, a new security protocol is designed using features of symmetric key and asymmetric key algorithms. The security principles can be achieved by AES and RSA algorithms. The main purpose of designing this algorithm is to provide better security to data in transit against passive as well as from active attacks. The new proposed hybrid algorithm is implemented in MATLAB R2019a. This algorithm will be analysed and compared on three parameters like avalanche effect, performance, and security against attacks. The proposed model will contribute towards improving the excellence of educators and academics, as well as increase competitiveness of educational programmes on cybersecurity among similar institutions in the EU countries.

Index Terms: AES, asymmetric algorithm, avalanche effect, cryptography, MATLAB, RSA, symmetric algorithm.

1. Introduction

Nowadays computers and other electronic devices have become the need of humans, for every work they depend upon technology. So, with the increasing need for electronic devices, there is a need to secure digital data that is transmitted by electronic devices over the internet or in the personal network. Computer security protects the information that is stored in systems. That’s why computer security is often called as information security [1]. One of the most common computer-based security mechanisms is cryptography. In earlier days cryptography was achieved through manual techniques. The most famous human-based cryptography algorithm was Caesar Cipher. Cryptography is “the art of writing or solving codes” [2]. One method to achieve cryptography is by encryption and decryption.

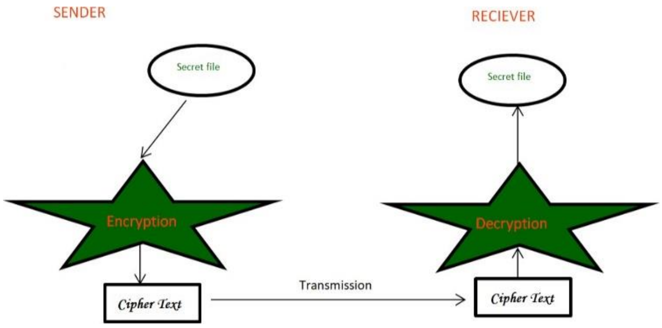


Fig.1. Simplified Model cryptography [1]

Fig 1 is the simplified model of cryptography and shows how encryption and decryption are done. Sender uses the encryption algorithm to encrypt the data. Encryption is the process of changing plain text or human- readable message into some secret codes that are unreadable to humans which are termed as ciphertext then, this ciphertext is sent over transmission medium and at the receiver, side reverse process of encryption is performed called decryption and converts cipher text into plain text [22].

The following five goals are used in cryptography [3,6,21]:

- *Authentication:* The receiver is not sure who sends the data. Authentication can be achieved by using a username or password etc.
- *Confidentiality:* it can be defined that the message cannot be known to unintended parties other than the authorized parties.
- *Integrity:* refers to making sure that the data does not modify over its entire life cycle.
- *Non-Repudiation:* refers to the ability to make sure that a person or a party connected with communication cannot deny the authenticity of their signature over sending of a message.
- *Availability:* refers that computer resources are available to authorized parties when needed.

The basic need for cryptography is given below:

- to communicate and share information
- to communicate separately

These needs gave rise to the art of coding the messages so that only the intended person can read a message.

The main objective of this study is to develop a better hybrid algorithm by combining the features of symmetric and asymmetric algorithms and to validate the proposed hybrid algorithm with the existing algorithms. Tt was observed that the most used algorithm in symmetric algorithms is AES. And is the most popular in asymmetric cryptography is RSA. There are many parameters where improvement is needed. These parameters are execution time, avalanche effect and algorithm are how secure from any attack. It is already known that among existing algorithms no algorithm is ideal for data encryption as no algorithm performs better in all these parameters. The secure algorithm is not that fast and which is fast is not comparatively secure. Key length is an important issue in designing any algorithm because the larger key will cause slow execution and poor performance of the algorithm similarly smaller key can result in poor security. The performance of the AES algorithm is very good but in terms of security its avalanche effect is very low and the performance of the RSA algorithm is very poor but its avalanche effect is quite high as compare to AES. Where these algorithms provide security against active attacks but fail to provide security against passive attacks.

The new proposed cryptography algorithm is a block cipher that operates on a block of data of equal length and then encrypts each block using a Key. This algorithm is containing features (like speed and security) of both AES as well as RSA algorithm and it also has some extra security features which make it more secure from all types of attacks.

The purpose of the model is to build the necessary competence in cybersecurity by promoting and disseminating the European expertise and good practice in cybersecurity to the business sector, legal regulatory bodies, and government institutions of Ukraine, as well as to the scientific and educational institutions. This model can be adoptedby other countries and institutes that suffer from the lack of cybersecurity expertise.

2. Types of Attacks

There are various types of security attacks [4,5] that can be faced by an individual or an organization. These attacks are:

1. Passive Attacks
2. Active Attacks

Fig 2 shows the different types of attacks and their functionalities.

1. *Passive Attacks:* - Attacks in which attacker involves in analyzing or monitoring of data. In other words, the main aim of the attacker is to obtain the information that is in transit. These types of attacks are hard to detect because no modification on data is performed by the attacker.
2. *Active Attacks:* - Unlike passive attacks, active attacks are based on a modification of the original message or creation of a false message. These types of attacks are easy to detect but very difficult to prevent. These attacks can be in the form of interruption, modification, and fabrication.

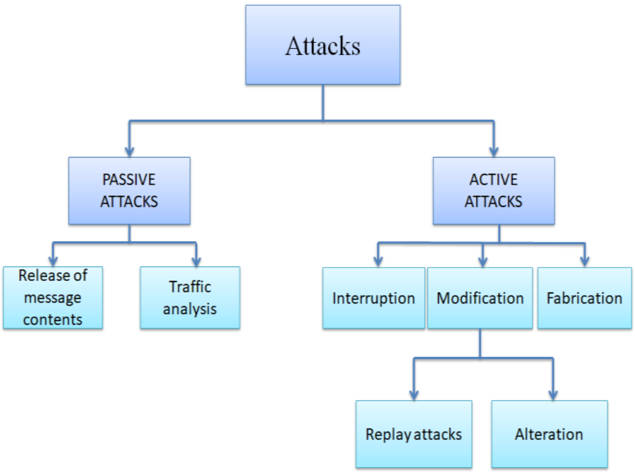


Fig.2. Types of attacks

3. Existing Algorithms

The cryptography algorithm is divided into two categories: First, algorithms use the same key called as the secret key for both encryption and decryption, known as symmetric key algorithms [7,8] and second, algorithms use two different keys one is used for encryption and other is used for decryption, known as an asymmetric key algorithm [9].

Many algorithms lie in these categories but in this study, only two algorithms are considered relevant. Those algorithms are Advanced Encryption Standard (AES) and RSA.

3.1. Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher algorithm that was developed in 1998 by Joan Daemen and Vincent Rijmen [10]. Fifteen symmetric key algorithms were submitted to the National Institute of Standards and Technology (NIST) for preliminary analysis and out of which only five were selected and AES is one of them. AES has become a universal standard of encryption and used in various applications.

AES uses a 128-bit block of plain text data and after encryption, these 128 bits of plain text data get converted into 128 bits of ciphertext. AES algorithm was based on 128-bit block and 128, 192, 256 bits of keys [11,23]. It is also used in TCP/IP protocols such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) [2]. AES uses the basic technique of substitution and transposition (i.e., permutation) [12] but the number of rounds depends upon the key length.

Table 1 shows the key size, plain text block and the number of rounds.

The entire document should be Times New Roman at 10 points in size. Other font type and size may be used if needed for special purposes. Recommended font type and sizes are shown in Table 1.

Table 1. Round Length

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

Steps involved in AES [4]

1. Repeat the steps (a, b, c) one-time initialization process:

   a. Expand the 16-byte key to get the actual Key block.
   b. Prepare one-time initialization of the 16-byte plain text block.
   c. XOR the state with the key block.

2. For each round, repeat steps a, b, c:

   a. Apply S-box to each plain text bytes.
   b. Rotate row k of plain text by k bytes.

c. Perform a mix column operation.
d. XOR the state with a key block.

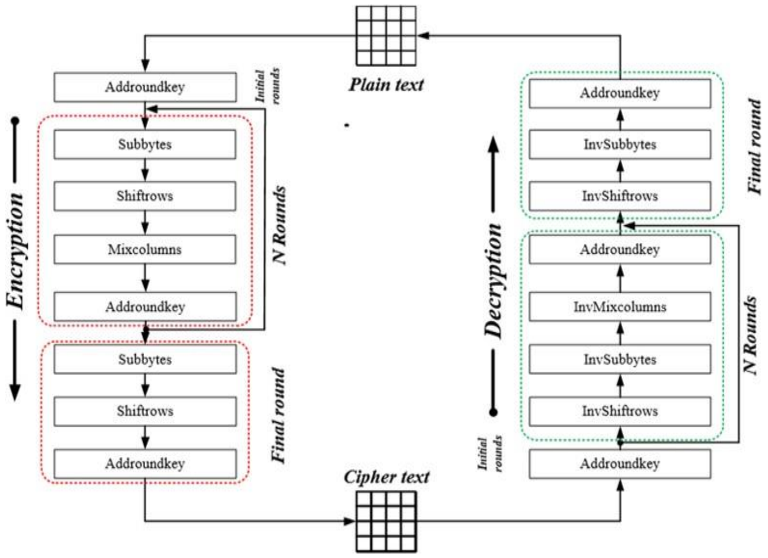


Fig.3. Advanced Encryption Standard [13]

Fig 3 shows the encryption and decryption of the AES algorithm

3.2. *RSA Algorithm*

RSA is an asymmetric key algorithm named after its three inventors- Ron Rivest, Adi Shamir, Leonard Adleman [14,15] in 1978. It is based on a mathematical fact that it is easy to find and multiply two large prime numbers but to factor, their product is a really difficult task [13]. Both keys are functions of a pair of large prime numbers. Conversion of plaintext from the public key and the ciphertext is considered equivalent to factoring the product of the two primes. RSA involves the following three steps [16]:

1) Key Generation*:* Encryption and decryption keys are generated.
2) Encryption: the public key of receiver data gets converted into human unreadable form i.e., into ciphertext.
3) Decryption: with receiver’s private key ciphertext gets converted into human-readable form i.e., into plain text.

4. Problem Specification

There are many parameters where improvement is needed. These parameters are execution time, avalanche effect and algorithm are how secure from any attack. It is already known that among existing algorithms no algorithm is ideal for data encryption as no algorithm performs better in all these parameters. The algorithm that is secure is not that fast and which is fast is not comparatively secure. Key length is an important issue in designing any algorithm because the larger key will cause slow execution and poor performance of the algorithm similarly smaller key can result in poor security. The performance of the AES algorithm is very good but in terms of security its avalanche effect is very low and the performance of the RSA algorithm is very poor but its avalanche effect is quite high as compare to AES. Where these algorithms provide security against active attacks but fail to provide security against passive attacks.

5. Problem Statement and Methodology Used

Zorain et al. [19] offers the implementation restrictions of existing algorithms such as DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6 of symmetric and RSA of asymmetric techniques. It had been also analyzed parameters like key exchange, flexibility and security issues of the algorithms which governs the efficiency of the cryptosystem. The results shows that yet asymmetric algorithms are superior in security, they take more time for processing and requires more memory. Asymmetric algorithms like RSA are used only for the key exchange.

Settia [20] had ardent her study to the security and attack parts of cryptographic techniques and discussed the leading issues of security and various attacks.

To meet the objective, descriptive, analytical, fundamental, and simulation approaches have been used. The research method used a theoretical approach for study and selection of tools for the objective which includes literature survey, articles, books, research paper, and content hosted on websites, thesis, conference proceedings, publications, journals, reports.

6. Proposed Algorithm

This new proposed cryptography algorithm is a block cipher that operates on a block of data of equal length and then encrypts each block using a Key. This algorithm is containing features (like speed and security) of both AES as well as RSA algorithm and it also has some extra security features which make it more secure from all types of attacks. This algorithm uses a symmetric key as well as an asymmetric key for encryption and decryption of data. The key length used in the proposed algorithm is 512 bits and block size is of 128 bits with 10 rounds of encryption. The plain text in the proposed algorithm goes into two different encryption and decryption process hence it is more secure than existing algorithms.

The proposed algorithm was implemented in MATLAB R2019a. Some of the main MATLAB functions that are used in implementation are [17,18]:

1. function plaintext = aes_decryption(OriginalMessage,round_keys)
2. function cipher_text = aes_encryption(plaintext,round_keys)
3. function Ciphertext = Encrypt (Modulus, PublicExponent, cipher_text)
4. function Message = Decrypt (Modulus, PrivateExponent, Ciphertext)
5. function [PublicExponent, PrivateExponent, Modulus] = GenerateKey

6.1. Implementation Details

Fig 4 describes all important aspects of implementation details. The algorithmic model shows how the implementation of algorithm works.

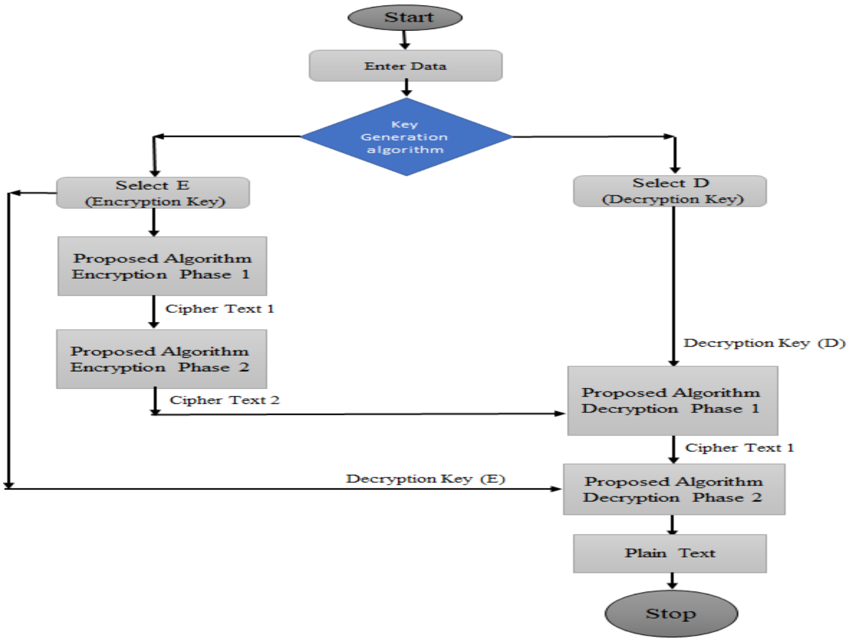

Start
Enter Data
Key Generation algorithm
Select E (Encryption Key)
Select D (Decryption Key)
Proposed Algorithm Encryption Phase 1
Cipher Text 1
Proposed Algorithm Encryption Phase 2
Cipher Text 2
Decryption Key (D)
Proposed Algorithm Decryption Phase 1
Cipher Text 1
Decryption Key (E)
Proposed Algorithm Decryption Phase 2
Plain Text
Stop

Fig.4. Algorithmic Model

Both encryption and decryption processes will run concurrently. But first, the encryption phase will complete, followed by the phase decryption because at one time data will either go through the encryption process or decryption process. In this algorithm first step is to enter plain text. This plain text is of the user’s choice. Then the user selects the public key for encryption as well as a private key that will be used for decryption. For user help, one key generation algorithm was there which will select the keys automatically of user choice.

Then the plain text will go through the dual process of encryption in which one encryption key got selected by the algorithm itself. After the encryption process ends the data goes through the decryption phase where one decryption key will be selected by the algorithm.

There because of these dual key features and because of dual encryption security of this algorithm is maximum.

7. Experimental Methodology and Environment

The experiment was implemented in MATLAB R2019a. The system used in this experiment was Intel® Core (TM) i7-7700 HQ CPU @ 2.80 GHz with 8 GB of RAM and 1TB HDD. The proposed algorithm was evaluated based on three parameters; avalanche effect, security against all types of attacks and performance.

This experiment is performed in two different data:

1) Data 1: Contains alphabetical character (ABCDEFGHIJKLMNOP).
2) Data 2: Contains alphanumeric character (0123456789ABCDEF).

Table 2. Algorithm Setting

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

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

8. Experimental Results and Analysis

The plain text is given as an input to encryption algorithms, and their output is an encrypted message or ciphertext. Then, this ciphertext was inputted to the decryption algorithm to get the decrypted message.

8.1. Avalanche effect

if a single bit of ciphertext gets altered then it should result in the alteration of multiple bits of a plain text message or vice versa. A good cryptography algorithm should always have an avalanche greater than 50% [3].

Table 3. Avalanche effect

Algorithms	Avalanche effect (Data 1)	Avalanche effect (Data 2)
AES	48%	53%
RSA	81%	91%
Proposed Algorithm	90%	95%

Table 3 shows the avalanche effect of cryptographic algorithms. Simulation was performed on Data 1 and Data 2. First data 1 was run on all three algorithms and then data 2 was run on 3 algorithms and their result is given in the table 3. From this table, it is clear that AES has a poor avalanche effect hence it is not that much secure against attacks. On the other hand, RSA is considered a secure algorithm but it also repeats some of the bits. But the proposed algorithm has an avalanche effect of 95% because every time the same data gets encrypted it generates different ciphertexts.

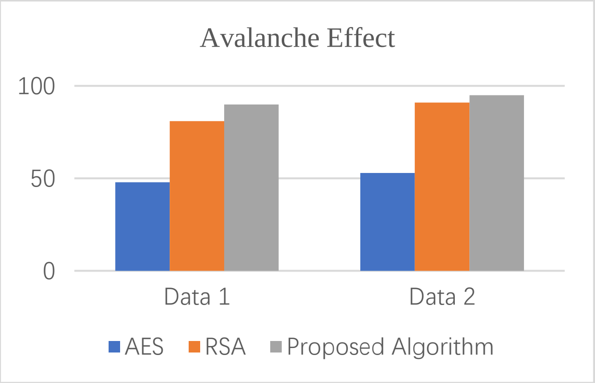


Fig.5. Avalanche Effect

Fig 5 is a graphical representation of the avalanche effect of different algorithms.

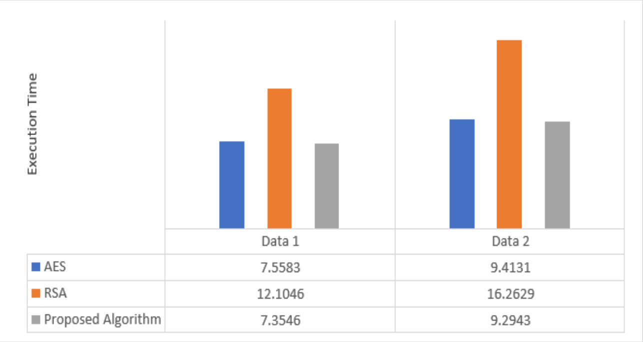
8.2. Execution Time

Time needed for encryption and decryption of data.

Table 4 shows the execution time of the algorithms. First data 1 was run on all three algorithms and its execution time was noted and hen did the same data with 2 The proposed algorithm has a better performance compared to existing algorithms.

Table 4. Execution Time

Algorithms	Execution Time (Data 1)	Execution Time (Data 2)
AES	7.5583	9.4131
RSA	12.1046	16.2629
Proposed Algorithm	7.3546	9.2943



	Data 1	Data 2
■ AES	7.5583	9.4131
■ RSA	12.1046	16.2629
■ Proposed Algorithm	7.3546	9.2943

Fig.6. Execution times

From fig 6 it is clear that the proposed algorithm has better performance. The execution time of the proposed algorithm is not constant rather it is variable.

8.3. Security Attacks

When the same data gets encrypted by the AES then it always generates the same ciphertext for it. Hence, for the passive attacker that is an advantage because when the same ciphertext is being transmitted over and over again, then the attacker will understand that it is the same type of data: and it can also decrypt it easily. Whereas in the case of RSA, it does not generate the same ciphertext for the same data but after few iterations it but after some time it starts repeating the patterns.

So, in the proposed algorithm, a special type of feature: that every time the same data gets encrypted, it will always give different ciphertexts. Hence making it fully secure from active as well as from passive attacks.

9. Conclusion and Future Scope

The advantages of encrypting data clear themselves in the form of security & confidentiality in real-time applications. Encryption of data is of specific significance in applications like email, e-commerce, e-cash where highly vulnerable communication lines are accessed for transmission of highly volatile data.

It is identified the importance of multiple parameters like keys and plaintext block size used in algorithms in terms of its security & strength. As the security of the encrypting algorithm is directly related to the key length, the more the key length the more will be the security of the algorithm.

The proposed algorithm is efficient and provides better security compared to existing algorithms. It has better results as compared to AES and RSA. Its implementation is easy, someone knowing MATLAB can easily implement this. It has features (like speed and security) of both AES and RSA algorithms with some additional features. Security is an important concern in today's date so, this proposed algorithm is the best option. The important feature of the proposed algorithm is that it is almost impossible to break the ciphertext because data goes to the dual encryption process. This proposed algorithm can be applied for any type of public application or in commercial areas for sending confidential data. So, it provides valuable application in the field of information security.

The proposed model for cybersecurity competence formation will contribute towards improving the excellence of educators and academics in the Ukrainian HEIs and increase competitiveness of educational programmes on cybersecurity and ICT among similar HEIs in the EU countries by introducing new courses that align the university context to the European values.

From performance and security points of view, performance can be increased and some new security features can also be added to it.

References

[1] D. Russell and G. T. F Gangemi Sr., “COMPUTER SECURITY BASICS,” O’Reilly and Associates, Inc., 1991.
[2] J. Katz and Y. Lindell, “INTRODUCTION TO MODERN CRYPTOGRAPHY,” Taylor & Francis Group, 2015.
[3] S. Nagaraj, G. S. V. P. Raju and K. K. Rao, “Image Encryption Using Elliptic Curve

[4] Cryptography and Matrix," in International Conference on Intelligent Computing, Communication & Convergence, pp. 276-281, 2015.

[5] A. Khate, "Cryptography and Network Security," Tata McGraw Hill Education Private Limited, pp. 14-16, 2003.

[6] 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.

[7] A. Anand, A. Raj, R. Kohli and V. Bibhu, "Proposed Symmetric Key Cryptography Algorithm for Data Security", in 1st International Conference on Innovation and Challenges in Cyber Security, 2016.

[8] M. Marwaha, R. Bedi, A. Singh and T. Singh, "Comparative Analysis of Cryptographic Algorithms," International Journal of Advanced Engineering Technology, Vol. 4, No. 3, pp. 16-18, 2013.

[9] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in International Conference on Electronics, Communication and Computational Engineering, Nov 2014.

[10] I. Alam, and M. E. R. Kahn, "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.

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

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

[13] 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.

[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] 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

[16] 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.

[17] S. Gupta and J. Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellam," in IEEE International Conference on Computational Intelligence and Computing Research, 2012.

[18] A. V. S, A. Rajan, N. B, P. Madhusoodanan and R. J. A. S, "Implementation of AES Algorithm on Text and Image using MATLAB," in Third International Conference on Trends in Electronics and Informatics, 2019.

[19] A. R. Reddy and J. S. A. K, "Implementation of 128-bit AES algorithm in MATLAB," International Journal of Engineering Trends and Technology, Vol. 33, No. 3, March 2016.

[20] Z. Hercigonja and D. Gimnazija, "Comparative Analysis of Cryptographic Algorithms," International Journal of Digital Technology & Economy, Vol. 1, No. 2, 2016.

[21] N. Settia, "Cryptanalysis of Modern Cryptographic Algorithms," International Journal of Computer Science and Technology, Vol. 1, No.2, 2010.

[22] Zuhi Subedar, Ashwini Araballi. " Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication ", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.4, pp.35-41, 2020. DOI: 10.5815/ijmsc.2020.04.04

[23] Qasem Abu Al-Haija, Mohamad M.Asad, Ibrahim Marouf,"A Systematic Expository Review of Schmidt-Samoa Cryptosystem", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.4, No.2, pp.12-21, 2018.DOI: 10.5815/ijmsc.2018.02.02

[24] Ritu Goyal, Mehak Khurana,"New Design of Tiny-Block Hybridization in AES", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.46-53, 2017.DOI: 10.5815/ijcnis.2017.09.06

[25] M. Sonar. Available [Online]: https://www.geeksforgeeks.org/visual-cryptography- introduction. Accessed on 28/03/2020 at 10:32 AM.

[26] L. Elbaz and H. Bar-El, "Strength Assessment of Encryption Algorithms," Available [Online]: http://www.discretix.com/PDF/Strength%20Assessment%20of%20Encryption%20Algorithms.pdf Accessed on 29/03/2020 at 01:22 PM.

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

Authors' Profiles

Rohit Verma has received his Master of Computer Science from Department of Computer Science at Himachal Pradesh University (HPU), Summerhill, Shimla, India. He received his Bachlors of Technology in Information Technology from University Institute of Information Technology at Himachal Pradesh University, Summerhill, Shimla, India. His research Interest includes Cryptography, Network/Data Security, Networking Protocols.

Jyoti Dhiman is pursuing her Bachlors of Technology in Computer Science from University Institute of Information Technology at Himachal Pradesh University (HPU), Summerhill, Shimla, India. Her research Interest includes Cryptography.

How to cite this paper: Rohit Verma, Jyoti Dhiman, "Implementation of Improved Cryptography Algorithm", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.2, pp.45-53, 2022. DOI: 10.5815/ijitcs.2022.02.04