ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 3, 25-30 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

An Immutable Algorithm Approach to Improve the Information Security of a Process for a Public Organization of Ecuador

Segundo Moisés Toapanta Toapanta*[1], Andrés Javier Bravo Jácome [1], Maximo Giovanny Tandazo Espinoza[1], Luis Enrique Mafla Gallegos[2]

[1] *Departament of Engineering Systems, Universidad Politécnica Salesiana(UPS), Guayaquil, Ecuador*

[2] *Faculty of Engineering Systems, Escuela Politécnica Nacional del Ecuador (EPN), Quito, Ecuador*

ARTICLE INFO

Article history:
Received: 28 March, 2019
Accepted: 22 April, 2019
Online: 07 May, 2019

Keywords:
Algorithms
Cryptography
Security

ABSTRACT

Currently, information security is among the main characteristics that must be achieved within the security of private and public organizations worldwide. For this reason, globally recognized algorithms such as the AES, IDEA, RC5, DES, RSA are researched with the aim of identifying the most suitable and obtaining a greater degree of security and speed of encryption in order to mitigate the information vulnerabilities between processes and be applied as a feasible alternative in an electoral process. The deductive method was used to analyze the information obtained in the references. After the study it is possible to conclude that to improve security in the processes of public organizations in Ecuador it is necessary to implement cryptographic mechanisms.

1. Introduction

The arrival of Information Technologies for the digital communications of the organizational processes, security problems have increased in an increasing way, that is why it is important to know about the different existing algorithms in order to reduce security problems of the information[1]. In the last decade there have been incidents where computer systems are vulnerable in the presence of hackers, cybercriminals and hacktivists, for such events governments have analyzed the negative effects that can cause these attacks and have developed different defense strategies to deal with the different attempts of intrusions. Most private and public organizations implement the use, creation or customization of cryptographic algorithms specialized in safeguarding the security of digital communications.

Why is it imperative to implement immutable algorithms in the processes of public organizations in Ecuador?

It is necessary to ensure the security of the information of possible attacks of theft, and to guarantee the security in the communications between the processes of the public organizations of Ecuador.

The general objective of the research is to establish a cryptographic algorithm could use a public institution of the Ecuadorian state that provides greater security in the communication and treatment of information.

The articles analyzed in relation to the subject are:

Performance analysis of encryption algorithms for security[1], A Comparative and Analytical Study on Symmetric[2], Dessign of new security algorithm[3], Comparative Analysis of NPN Algorithm & DES[4], Proposed Symmetric Key Cryptography Algorithm[5], Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms[6], Performance Evaluation of Cryptographic Algorithms: DES and AES[7], DES and AES Performance Evaluation[8], Differential fault analysis against AES-192 and AES-256 with minimal faults[9] ,Implementing the IDEA Cryptographic Algorithm in Virtex-E and Virtex-II FPGAs[10], User Defined Encryption Procedure for IDEA Algorithm[11], Performance evaluation for CAST and RC5 encryption algorithms[12], Selection of parameter 'r' in RC5 algorithm on the basis of prime number [13] , Design and implementation of algorithm for des cryptanalysis [14], A-RSA: Augmented RSA [15], High speed implementation of RSA algorithm with modified keys exchange[16].

The deductive method was used to analyze the information obtained in the references and identify the characteristics of each of the security algorithms; that allow improving the security of organizations. This method is taken in view of the fact that the

*Segundo Moisés Toapanta Toapanta, Email: stoapanta@ups.edu.ec

information obtained must be analyzed to consider the qualities presented by each of the algorithms.

In this research phase it can be obtained that AES cipher algorithm is the most efficient due to its features, working together with hardware and software for the application of cryptography in digital communications processes.

2. Materials and Methods

2.1.1 Materials

Cryptography is the skill of writing in an enigmatic way, that is, it is a process of transformation of any data readable to an encrypted data. This ensures that the data can't be objective of any attack coming from the organization or outside it. For the interaction of processes applying cryptography it is necessary to apply the encrypted method and decrypted method[2].

This science allows the secure transmission of sensitive information in unsafe processes so that it can't be interpreted by third parties[3].

Cryptography, in addition to providing confidentiality and privacy, within its main features that it provides are: authentication, data integrity, non-repudiation, etc[4,5]. The two main methods are Symmetric Key Cryptography and Asymmetric Key Cryptography[6].

Immutable Algorithm refers to the fact that the data it handles within its encryption process are not going to be modified or altered, the immutable algorithms are algorithms that work in blocks, for that reason not even a single bit of each output of the round.

2.1.2 Definition AES Algorithm

AES is used as a standard algorithm for US federal organizations. AES consists of a key mechanism of 128 bits, 192 bits and 256 bits. Starting from an initial key of 16 bytes (128 bits), which we can show as a block or matrix of 4x4 bytes, 10 keys are generated, these resulting keys plus the first key are called subkeys[7,8].

The algorithm is classified into AES-128, AES-192 and AES-256 which have 10 rounds, 12 rounds and 14 rounds respectively. Each of the rounds is composed of 4 transformations, unlike the last round. These transformations are: SubBytes, ShiftRows, MixColumns and AddRoundKey, as mentioned the last round lacks a transformation which is MixColumns[9].

- SubBytes: It consists of 16 identical boxes (8x8). In this step, a non-linear substitution is performed where each byte is replaced with another, that is, $Sb_{ij} = S(a_{ij})$. The denotative is SB.
- ShiftRows: In this step a transposition is carried out, each row of the box moves cyclically in different displacements. Row 0 does not scroll, row 1 moves by 1 byte, row 2 moves by 2 bytes and row 3 by 3 bytes. The denotative is SR.
- MixColumns: This is a mixing operation that runs in the columns of the box, coupling the 4 bytes in each column using a linear transformation. The denotative is MC.
- AddRoundKey: This is an XOR operation bit by bit with the key of the round.

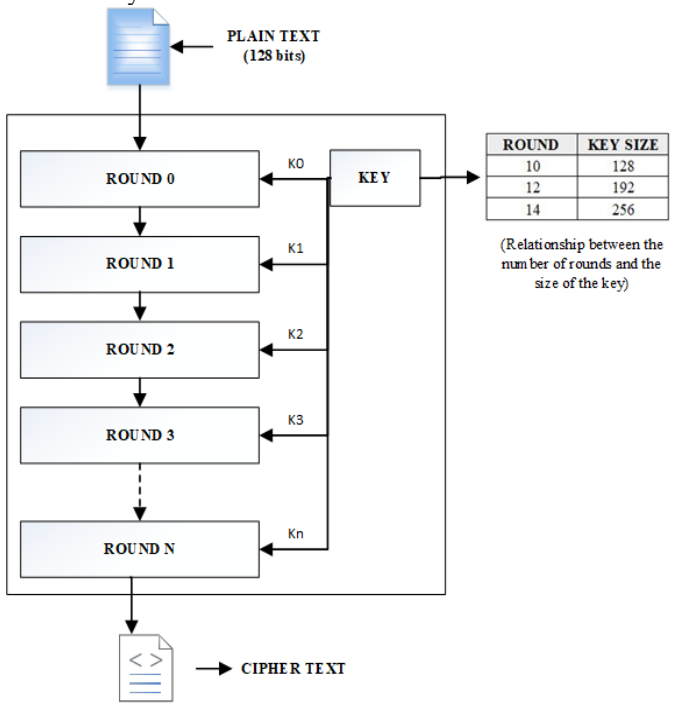

Figure 1: Process AES (Advanced Encryption Standard).

2.1.3 Definition IDEA Algorithm

IDEA is an encryption algorithm that works with a block of 64-bit flat text. It implements a 128-bit input key that it uses to generate 52 subkeys of 16 bits each. The decryption process is the same encryption process but applied in reverse[10].

The encryption stream contains a total of 8 rounds, after the round number 8 performs a transformation in the output. Its operation consists of the first four sub-blocks are 16 bits of key which combines them with four blocks of 16-bit flat text. The exit of each round is the entrance of the next round[11].

IDEA is an encryption algorithm that is based on the concepts of confusion and diffusion, implementing elementary operations, are the following:

- XOR
- Sum of module 2^{16}
- Module product $2^{16} + 1$

In a round of IDEA:

1. Multiply X1 by sub-key Z1.
2. Add X2 with sub-key Z2.
3. Add X3 with sub-key Z3.
4. Multiply X4 by sub-key Z4.
5. XOR between step 1 and step 3.
6. XOR between step 2 and step 4.
7. Multiply step 5 by subkey Z5.

8. Add the step 6 and step 7.
9. Multiply step 8 by subkey Z6.
10. Add the step 7 and step 9.
11. XOR between step 1 and step 9.
12. XOR between step 3 and step 9.
13. XOR between step 2 and step 10.
14. XOR between step 4 and step 10[11].

Transformation of the output:

1. Multiply X1 by sub-key Z1.
2. Add X2 with sub-key Z2.
3. Add X3 with sub-key Z3.
4. Multiply X4 by sub-key Z4[11]

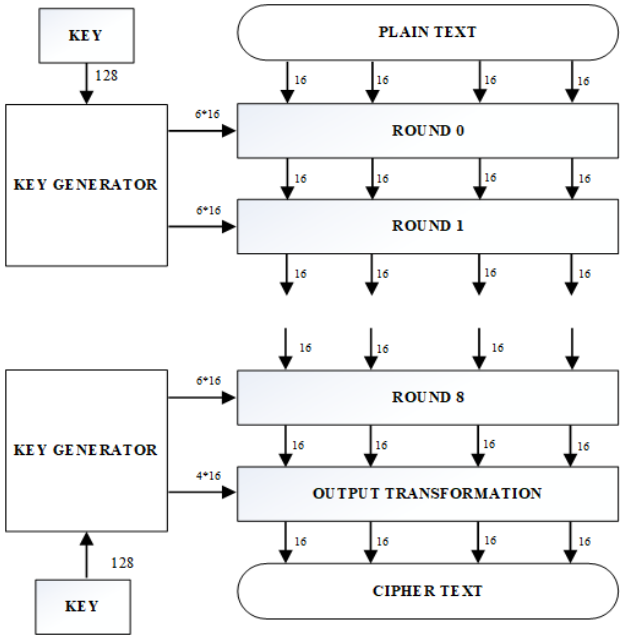

Figure 2: Process IDEA (International Data Encryption Algorithm)

2.1.4 *Definition RC5 Algorithm*

RC5 was created by the cryptographer Ronald Rivest and is a symmetric method block cipher algorithm. Its operation is simple and very fast since it only implements three classes of computational operations (such as XOR, shift, etc.) and a minimum memory consumption[12].

To encrypt the entry of the block is a plain text that is divided into 2 sub-blocks A and B, the output of this block is an encryption text of 2 w-bit length. Equation(1) shows the operations to encrypt[13].

$$
\begin{aligned}
&A = A + S[0];\\
&B = B + S[1];\\
&\text{For } i = 1 \text{ to } r \text{ do}\\
&A = ((A \text{ XOR } B) << B) + S[2*i];\\
&B = ((B \text{ XOR } A) << A) + S[2*i+1];
\end{aligned}
\qquad (1)
$$

To decrypt the cipher text, it is treated as a data block and again divided into two sub-blocks. Therefore, one can arrive at the deduction that the decryption method is the inverse of encrypting. Equation(2) shows the operations to encrypt[13].

$$
\begin{aligned}
&\text{For } i = r \text{ downto } 1 \text{ do}\\
&B = ((B - S[2*i+1]) >> A) \text{ XOR } A;\\
&A = ((A - S[2*i]) >> B) \text{ XOR } B;\\
&B = B - S[1];\\
&A = A - S[0];
\end{aligned}
\qquad (2)
$$

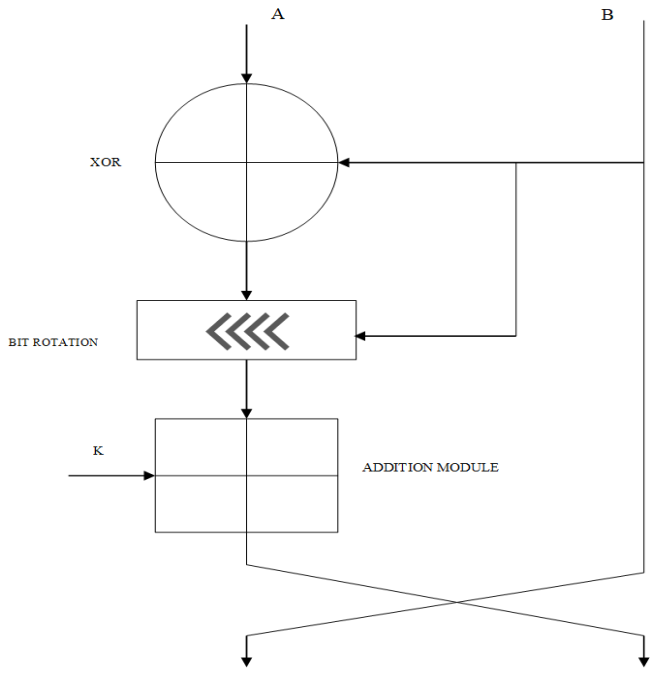

Figure 3: Process RC5 (Rivest Cipher 5)

2.1.5 *Definition DES Algorithm*

DES is a symmetric key encryption algorithm, it is among the first encryption methods that was implemented commercially, it was mainly used as a security standard for the processing of federal information in the US. It is an encryption algorithm that operates on data bocks, 64-bit blocks, with a 56-bit secret key. It has 16 rounds each with two permutations[14].

The encryption process consists of two permutations called P boxes, which correspond to preliminary permutation and last permutation, and sixteen rounds of Feistel. Each of the 16 round uses a different 48-bit key-key generated by the encryption key that implements a predefined algorithm.

The f function of Feisnel is composed of four sections:

1. Box expansion P
2. Mix of box P.
3. Replacement
4. Permutation

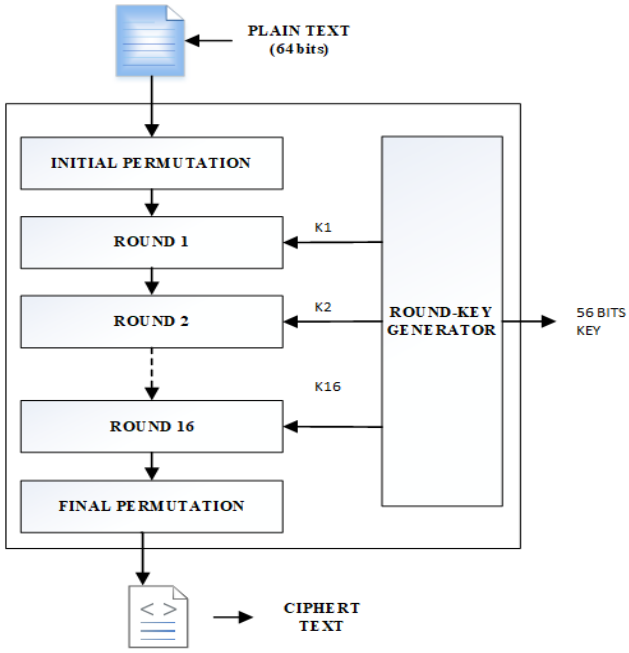

Figure 4: Process DES (Data Encryption Standard)

2.1.6 *Definition RSA Algorithm*

RSA was founded in 1978 and is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir and Adelman[15]. It is one of the most popular and recognized for the exchange of keys, digital signatures, encryption of data blocks. RSA uses an encryption of variable size of blocks and a key of variable size.

It uses 2 prime numbers to generate the public key and private keys, its size is from 128 to 4096 bits. These two different keys are used in order to encrypt and decipher[15]. It should be noted that RSA is absolutely slow in its methods of encrypting and decrypting; therefore, it is not recommended for large data[16].

RSA encryption is simply a modular expression. The module "n" is not more than the product of 2 large prime numbers (between 100 and 300 digits) chosen at random, both the public key and the private key is obtained from the following equation (3).

$$e = d\text{-}1 \bmod Ø(n) \quad (3)$$

The encryption operation is performed by public keys "n" and "e" of the following equation (4).

$$C = M^e \pmod n \quad (4)$$

While to recover the original message from the encrypted message is done with the equation (5).

$$M = C^d \pmod n \quad (5)$$

2.1.7 *Methods*

We analyzed the available data of the different cryptographic algorithms AES, RC5, IDEA, DES and RSA and it was deduced from the analysis which would be the best to apply it within the public organizations of Ecuador and as a possible alternative of security in digital electoral processes.

Secondly, the following characteristics have been considered as the relevant points to proceed to evaluate the cryptographic algorithms AES, IDEA, RC5, DES and RSA.

Table 1: Selected features for the evaluation of the AES, IDEA and RC5 algorithms

Characteristic	AES	IDEA	RC5	DES	RSA
Type	Symmetric Algorithm	Symmetric Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Key length (bits)	128 bits 192 bits 256 bits	128 bits	128 bits 192 bits 256 bits	56 bits	128, 256, 1024, 2048 y 4096 bits
Block size	128 bits	64 bits	32 bits 64 bits 128 bits	64 bits	-
Number of Rounds	10, 12 o 14	8	12	16	-

Then algorithms were implemented using Netbeans 8.2 as a development environment. The algorithms are programmed in JAVA language under OS Windows 10. The test platform is a laptop (ASUS Q504U) with Intel Core i5-7200U CPU 2.5GHZ 2.71GHZ and 12GB of RAM.

The speed test consists of the time that an encryption algorithm takes to transform a plain text. The speed test helps us measure the performance in units of time. In this paper we also consider the decryption speed for the algorithms to be evaluated.

3. Results

3.1. Cipher Test

In this test we have used 3 files of different sizes, 1 Mb, 10 Mb, and 100 Mb; which will be the files to be encrypted in order to obtain the times when encrypting the file. We have to keep in mind that each cryptographic algorithm uses different key sizes.

Table 2: Results of the cipher times obtained for the cryptographic algorithms with their different keys.

FILE (MB)	AES 256 BITS	IDEA 128 BITS	RC5 256 BITS	DES 256 BITS	RSA 128 BITS
1 MB	21 ms	40 ms	67 ms	70 ms	-
10MB	59 ms	242 ms	617 ms	418 ms	-
100MB	1489 ms	1920 ms	1874 ms	3804	-

3.2. Decryption Test

In this test we perform the decryption of the files of the previous test in order to obtain the time it takes for each algorithm to decrypt.

Table 3: Results of decryption times obtained for cryptographic algorithms.

FILE (MB)	AES 256 BITS	IDEA 128 BITS	RC5 256 BITS	DES 256 BITS	RSA 128 BITS
1 MB	36 ms	46 ms	67 ms	56 ms	-
10MB	230 ms	390 ms	617 ms	474 ms	-
100MB	2125 ms	2269 ms	2745 ms	3825	-

3.3. Analysis of result

In the following table we show a weighting assigned to each cryptographic algorithm by the characteristics of key strength and encryption speed. The assigned value corresponds to the value obtained by each algorithm (1 to 3, with 3 being the highest value and 1 being the lowest). As a result, we can show that the AES algorithm provides greater security and the IDEA gives us less security compared to the RC5 algorithm, and as the algorithms of less security this DES and finally we have the RSA algorithm.

Table 4: Analysis of the results.

Characteristic	Cryptographic Algorithm				
	AES	IDEA	RC5	DES	RSA
Key strength	3	2	3	1	3
Encryption speed	3	1	2	2	-
Decryption speed	3	2	3	1	-
Total	**9**	**5**	**8**	**4**	**3**

In the following figure we can compare the weights and show that the algorithm AES has better results in comparison with the algorithms IDEA, RC5, DES and RSA. It is worth noting that the RSA algorithm could not be performed because it is only capable of encrypting data of less than 254 bytes and the files under test exceeded its maximum quota.

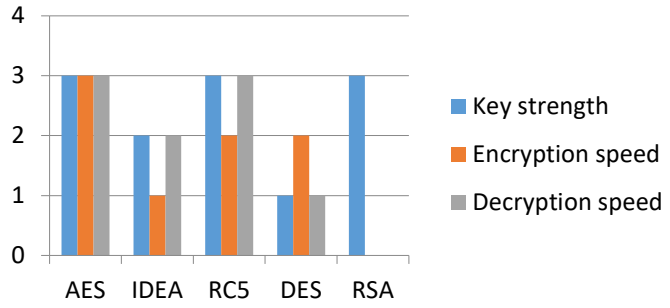

Figure 5: Analysis of results. The evaluation diagram by characteristic of each cryptographic algorithm is shown

a. The AES cryptographic algorithm has a value of 3 in the key strength characteristic, this indicates that it has a greater number of combinations among the other analyzed algorithms IDEA and RC5.
b. AES cryptographic algorithm has a greater number of stages (rounds), this means that its design is more complex than the IDEA and RC5 algorithms.
c. The cryptographic algorithm AES has the highest number in encryption speed however it has the same value in deciphering as algorithm RC5. This means that both are fast, however, the AES cryptographic algorithm is faster at the time of encrypting.

4. Discussion

The majority of developed countries adopt the use of proprietary algorithms since these are designed to their needs and vulnerabilities, there are developing countries which implement the use of immutable algorithms, with the observations made on the cryptographic algorithms it is possible to show that the cryptography has a fundamental role in information security.

The results obtained in this investigation were the criteria of the authors on the importance of the information; it is considered that the AES algorithm can be an alternative to improve the security of the information for a process of a public organization of Ecuador or any other organization.

For this, it was obtained as a result that the AES cryptographic algorithm is the most optimal, according to the score obtained; Within the research, the variables that characterize it were identified: key strength, block size, number of rounds and encryption speed; characteristics mentioned by the authors of the references(1-16).

AES exceeds the algorithms DES, RC5, IDEA, RSA; both in hardware and in software, it is considered as a combination of security, speed, performance and applicability. It also provides greater security by its multiple possible combinations between block sizes, as well as in the use of longer keys and its 3 possible numbers of rounds.

Can speak of immutability on the AES encryption algorithm; its method of encryption of rounds provides us with the security that the exit data of each round can't be altered on the way to the entrance of the next round.

The implementation of the AES cipher can be considered as a reference for the design of the security of the processes of public organizations of Ecuador, as well as possible viable alternative for an electoral process.

It is concluded that with the implementation of the AES cipher algorithm to improve the security of the information and the treatment thereof, guaranteeing the availability, integrity and confidentiality of the communications and services offered by the public organizations of Ecuador.

5. Conclusion and Future Work

The cipher algorithms play a very important role in the security of the processes inside and outside the organizations, our work in the research was to study the algorithms AES, IDEA, RC5, DES and RSA. By implementing the AES Algorithm, it was obtained that it is the fastest algorithm and gives us greater security.

It is advisable to achieve a degree of security in the keys, for this it is necessary to take into consideration the use of extensive keys, alphanumeric keys, keys with the use of uppercase and lowercase, use of special characters; this way we can delay the time in which he performs a brute force attack on a cryptographic algorithm.

The training of IT staff in cryptology, since in the future they could be responsible for technological advancement and implement their own cryptographic algorithms. Reinforcing information security policies in organizations, since the established rules could be violated due to ignorance or negligence.

It is recommended as future works the analysis of algorithms with the use of Hash methods to guarantee the integrity of the data against brute force attacks.

6. Acknowledgment

The authors thank the Salesian Polytechnic University of Ecuador, the research group of the Guayaquil Headquarters "Information Technology, Security and Information for a Globalized World" (CSITGW) created in accordance with resolution 142-06-2017-07-19 and the Secretariat of Higher Education Science, Technology and Innovation (Senescyt).

References

[1] M. Panda, "Performance analysis of encryption algorithms for security," *Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016 - Proc.*, pp. 278–284, 2017.

[2] B. Mandal, S. Chandra, S. S. Alam, and S. S. Patra, "A comparative and analytical study on symmetric key cryptography," *2014 Int. Conf. Electron. Commun. Comput. Eng. ICECCE 2014*, pp. 131–136, 2014.

[3] M. Dubai, T. Mahesh, and P. Ghosh, "Design of new security algorithm: Using hybrid Cryptography architecture," *3rd Int. Conf. Electron. Comput. Technol. (ICECT), 2011.*, pp. 99–101, 2011.

[4] M. Sharma, R. B. Garg, and S. Dwivedi, "Comparative analysis of NPN algorithm & des Algorithm," *Proc. - 2014 3rd Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2014*, 2015.

[5] A. Anand, A. Raj, R. Kohli, and V. Bibhu, "Proposed symmetric key cryptography algorithm for data security," *2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016*, no. Iciccs, pp. 159–162, 2016.

[6] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," *2017 Int. Conf. Eng. Technol.*, pp. 1–7, 2017.

[7] S. Kansal and M. Mittal, "Performance Evaluation of Various Symmetric Encryption Algorithms," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no, pp. 105–109, 2014.

[8] B. Bhat, A. W. Ali, and A. Gupta, "DES and AES performance evaluation," *Int. Conf. Comput. Commun. Autom. ICCCA 2015*, pp. 887–890, 2015.

[9] C. H. Kim, "Differential fault analysis against AES-192 and AES-256 with minimal faults," *Fault Diagnosis Toler. Cryptogr. - Proc. 7th Int. Work. FDTC 2010*, pp. 3–9, 2010.

[10] J. M. Granado, M. A. Vega, J. M. Sanchez, and J. A. Gomez, "Implementing the IDEA Cryptographic Algorithm in Virtex-E and Virtex-II FPGAs," vol. 03, pp. 109–112, 2006.

[11] V. S. Prajwal and K. V. Prema, "User Defined Encryption Procedure for IDEA Algorithm," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 1668–1671, 2018.

[12] T. Nie, Y. Li, and C. Song, "Performance evaluation for CAST and RC5 encryption algorithms," *2010 Int. Conf. Comput. Control Ind. Eng. CCIE 2010*, vol. 1, pp. 106–109, 2010.

[13] H. S. Gill, "Selection of parameter 'r' in RC5 algorithm on the basis of prime number," *2014 Recent Adv. Eng. Comput. Sci. RAECS 2014*, pp. 1–4, 2014.

[14] H. D. Zodpe, P. W. Wani, and R. R. Mehta, "Design and implementation of algorithm for des cryptanalysis," *Proc. 2012 12th Int. Conf. Hybrid Intell. Syst. HIS 2012*, pp. 278–282, 2012.

[15] A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," *Proc. 2016 SAI Comput. Conf. SAI 2016*, pp. 1016–1023, 2016.

[16] S. A. Nagar and S. Alshamma, "High speed implementation of RSA algorithm with modified keys exchange," *2012 6th Int. Conf. Sci. Electron. Technol. Inf. Telecommun. SETIT 2012*, pp. 639–642, 2012.