A New Improved Encryption Technique Using Dict Substitution and AES: Dict-AES

Manjinder Singh
Student, Master of Technology
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University Fatehgarh Sahib

Kamaljit Kaur
Assistant Professor
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University Fatehgarh Sahib

***Abstract*: In the present time, data is wealth. One with billions of bucks cannot be assumed as the wealthiest in the world. But one with data in its hand may be the richest in the world. So as to safeguard this information, we tend to use numerous cryptography techniques. Encryption is that the most generally used technique to secure the info from intrusions. In this paper, we propose a new encryption technique named as Dict-AES. In this, we implement a new substitution technique named as Dict substitution with Advance Encryption Standard. The proposed encryption technique Dict-AES gives better performance than other known encryption schemes. It may be proposed as an encryption technique to overcome from the known attacks against AES, especially Brute Force attack.**

***Keywords*: Cryptography, Data Security, Symmetric-key Cryptography, Data Compression, Lossless Compression, Lossy Compression, Public-key Cryptography**

I. INTRODUCTION

Protecting the info from intruders is extremely vital during this era of the web. Everyone has to share his/her data with another by means of the internet. The security of data is the area of major concern as data is conveyed from one place to another. With the speedy advancement within the technologies, it's troublesome to secure the info from unauthorized persons. Cryptography is sort of connected to the disciplines of cryptanalysis and cryptanalytic. Cryptography contain some techniques like microdots, merging words with images and another way to hide information in storage and transactions. Though, cryptography is usually connected with scrambling plaintext (ordinary text or clear text) into cipher text (a technique referred to as encryption) and reverse process (known as decryption) [1]. Further cryptography will be divided into two parts:

- **Private Key Cryptography:** In this, same key is used for encryption as well as for decryption.
- **Public Key Cryptography:** In this cryptography, different keys are used for encryption as well as for decryption.

II. RELATED WORK

In [3] Modified Vigenere Encryption Algorithm (MVEA) has been proposed and then Hybrid encryption algorithm have been used which integrates MVEA, Base64 and AES algorithm to improve the security of data. In [4] discussed three techniques AES, Blowfish and Twofish and then make two hybrid techniques AES with Blowfish and AES with Twofish. In [4] AES with Twofish gives better results than AES with Blowfish. In
[5] discuss about Brute Force Attack and other security issues in wireless networks. Then he implement Brute Force Attack on AES with work factor of 2^{128}. It shows that AES algorithm is more secure against brute force attack as compare to A5 and DES algorithm and suggests that AES algorithm would be used in GSM network. In [6] combining two algorithms called RSA and AES. It shows that hybrid of two encryption algorithms makes a reliable and efficient encryption technique and proposed hybrid technique in [6] is resistant to linear attacks. [7] integrates the AES algorithm with SHA-2 hash function and it complexes the architecture and gain high security. In [8] hybrid AES and RSA algorithms is used for encryption and SHA-256 is used to generate the signature with hybrid algorithm. Adding a hash function will achieve the integrity along with encryption algorithm. In [9] proposes a hybrid algorithm of AES and ElGamal and proposed hybrid algorithm is better than AES and ElGamal in terms of security. [10] makes a new hybrid algorithm by using three encryption algorithms: AES, DES and RSA. In this, possibilities of brute force attack are reduced by great extent.
Some researchers have applied hybrid methodology to beat weakness of encryption algorithms. In [11] hybrid AES and Blowfish is used for encryption and SHA-256 is used for hashing the plaintext. In this, RSA and ECC are used for generating the public and private keys. It conjointly provides a technique to induce protocol implementation and high speed key authentication. [12] is a hybrid combination of four existing cryptosystems Chaos-Based, AES, RSA and ElGamal. It provides security against known attacks and it makes hard for intruders to break such encryption. In [13] hybrid RSA and AES is used for encryption of plaintext and SHA-256 to ensure data integrity. The proposed solution is implemented in live scenarios. In [14] hybrid RSA and AES is implemented. It provides security over interpolation attacks against AES.

III. DICT SUBSTITUTION

Substitution is the process of interchange the alphabet with another alphabet using simple substitution table or by doing some mathematical calculations on it. However, today there are various substitution techniques are available from simplest one to complex. The substitution technique used in our proposed method is known as Dict substitution. In this, we interchange the most common alphabet pair with the predefined key stored in the indexed dictionary. The following diagram shows the working of the indexed dictionary substitution.

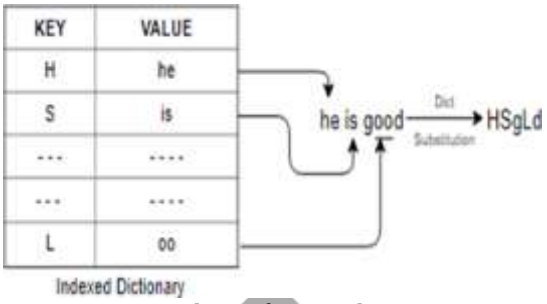


Fig.1 Working of Dict Substitution

In this substitution, the character pair that are matched with dictionary values are replaced with a predefined key stored in the dictionary. For example, if the word 'soon' will occur in our data string the characters 'oo' are replaced by the dictionary key 'L'. The word 'soon' will be encrypted as 'sLn'. However, choosing the best dictionary key pairs is very difficult and complex process. As much as the dictionary is more efficient, the encrypted cipher text is more difficult to break by intruders. Find the best suitable indexed dictionary is again a wide research field of Information retrieval. As much as values from plane text will be matched with the dictionary smaller will be the size of the encrypted output. Thus Dict substitution provides compression as well as encryption of plaintext.

IV.ADVANCED ENCRYPTION STANDARD

AES (Advance Encryption Standard) is the successor of outdated DES. AES was developed by Joan Daemen and Vincent Rijmen in 2001, who were from Belgian [2]. The length of the key for AES should be 128, 192 and 256 bits. AES has a fixed block size that is of 128 bits. Number of rounds for AES depends upon the key size i.e. 10 rounds, 12 rounds and 14 rounds for 128 bits keys, 192 bits keys and 256 bits keys respectively [13]. US government is employed AES to shield sensitive data and implemented across the planet for encryption purposes in the form of software and hardware [17]. In AES, 128 bits input block is organized as 4x4 matrix is known as state array. In both encryption and decryption process, the state array will modified by round function. The round functions defined as below [3]:

1. **SubBytes Transformation:** It is a non-linear substitution step, in which each byte is take place of another byte according to the S-Box (Substitution Box).
2. **ShiftRows Transformation:** In this step, each row of state array is shifted by a certain number of steps.
3. **MixColumns:** In MixColumns, a mixing operator is applied to the columns of the state array. By applying MixColumns, we can combining the four bytes in each column of the state array. It is applied only on first n-1 rounds where n is total number of rounds of AES.
4. **Add Round Key:** It is a simple XOR operation applied on bytes of the state array and round key. The round key is generated from the cipher key by using Rijndael key schedule algorithm.

Let us explain the encryption and decryption process of AES with help of an example. Suppose we have 128 bits cipher key. For cipher key of 128 bits, AES will process 10 rounds on the plaintext to encrypt it into ciphertext. The following diagram shows the process of AES for 128 bits cipher key.

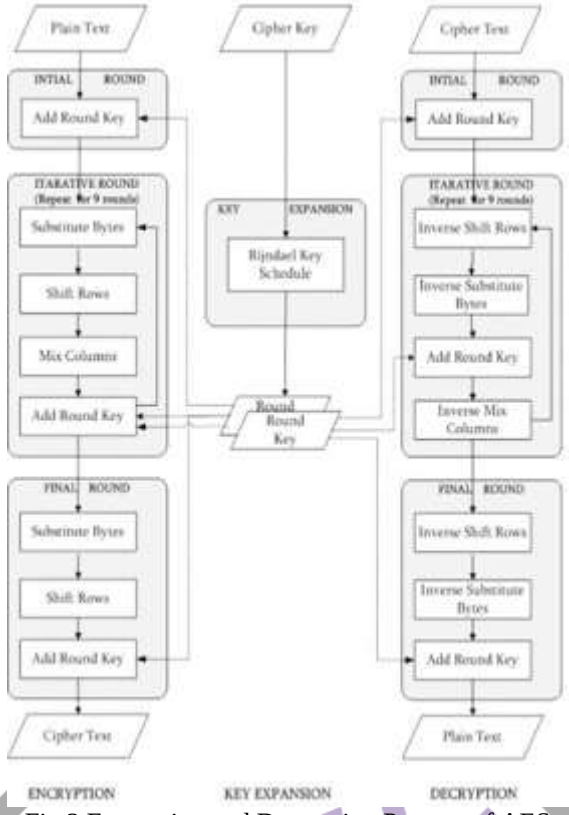


Fig.2 Encryption and Decryption Process of AES

The input from the user to the AES is plaintext which is original data which user wants to protect from unauthorized access. Along with plaintext user also input the secret key to the AES algorithm which of either size 128 bits or 196 bits or 256 bits. From round 1 to 9 all the four function of AES i.e. SubBytes Transformation, ShiftRows Transformation, Mixcolumns and Add Round Key are processed on the plaintext. In 10^{th} round of AES, the MixColumns step is skipped.

V. PROPOSED WORK

In our proposed technique, the input data is passes through Indexed-Dict phase which indexed the input data according to the occurrences. After that AES algorithm is applied on the indexed data and data encrypted with the proposed technique. Flow of work how data is taken as input, how it is been processed, and what is the outcome after all processing, is shown in the following diagram

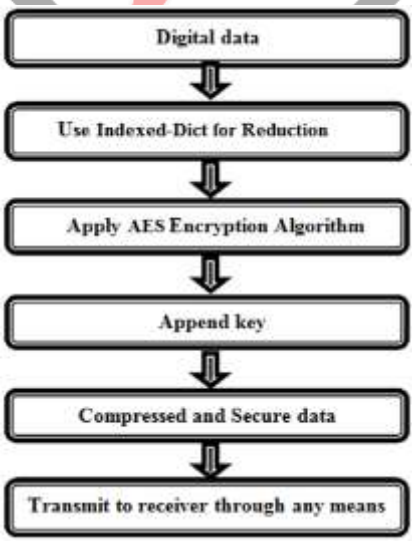


Fig.3 Architecture of Proposed Methodology

i. Encryption Phase

Encryption phase of the proposed technique will consist of two algorithms named as Algorithm_1 and Algorithm_2. The Algorithm_1 do the substitution process with the help of indexed dictionary. The Algorithm_2 will apply the various steps of AES on the output provided by the Algorithm_1. Plaintext will be provided to the Algorithm_1 as input. It will doing the substitution on that plaintext and pass it to the Algorithm_2 as input. Then Algorithm_2 will encrypted it into cipher text with the help of AES.

Following figure shows the working of the encryption phase of our proposed technique

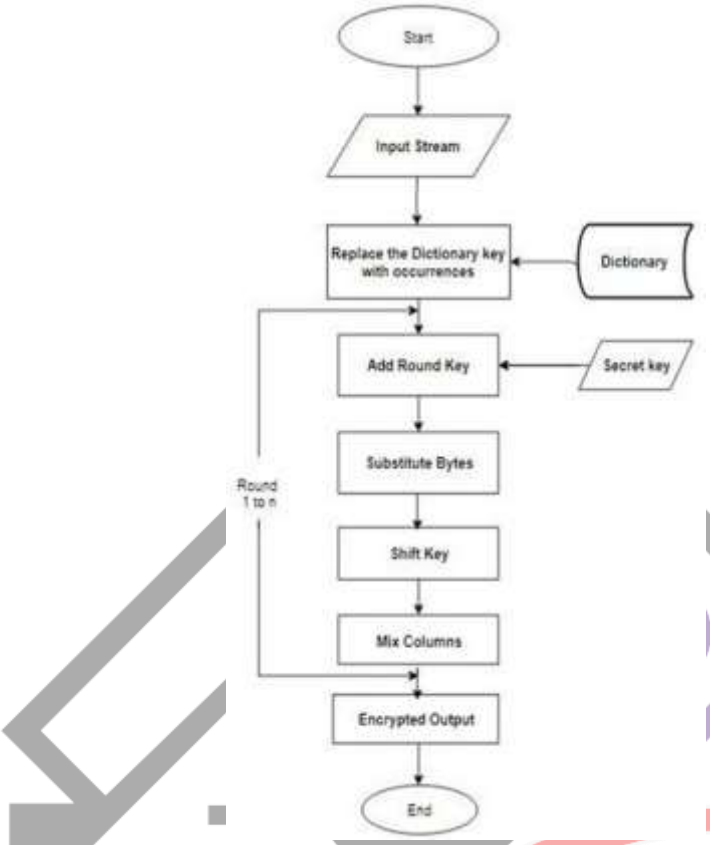


Fig.4 Working of Encryption Phase

It is shown in Fig. 4.6 that the plaintext will be provided as input to the Dict-AES algorithm. Firstly, it will doing substitution on it with the help of indexed dictionary. Then it will encrypted it with the Advance Encryption Standard into the cipher text.

ii. Decryption Phase

As long as data is in encrypted form i.e. it is a ciphertext it is protected but is no longer usable until it will decrypted into the original plaintext form. Decryption phase is composed of algorithm_3 and Algorithm_4. Algorithm_3 done the inverse operation of AES. Algorithm_4 make the substitution of keys with the original values with the help of indexed dictionary. The decryption phase is just the inverse of encryption phase. The encryption phase will convert plain text into cipher text while decryption phase will convert cipher text into plain text. The figure shows the working of the decryption phase

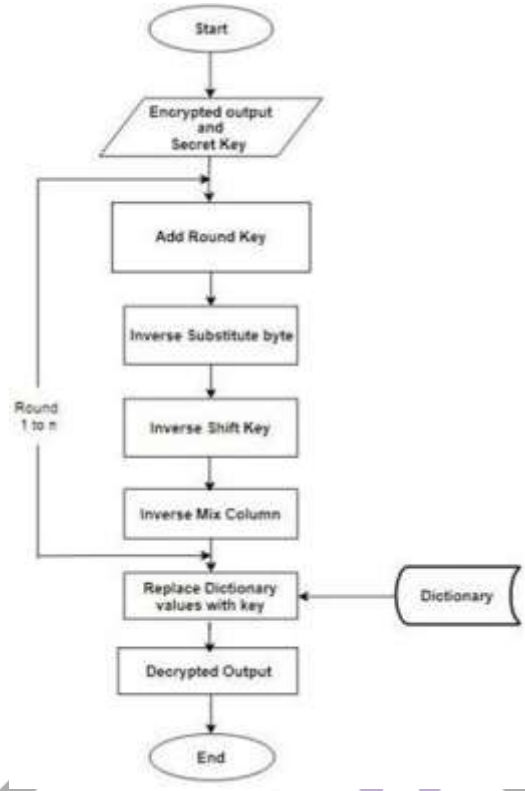


Fig.5 Working of Decryption Phase

Decryption phase makes the ciphertext into a user understandable form i.e. into its original form. In decryption phase all four AES round function will applied but in a reverse manner as Inverse Substitute Byte, Inverse ShiftRows and Inverse MixColumns. After apply all these round function of AES inreverse manner, the inverse of Dict Substitution is applied. In inverse of Dict Substitution, all the key that are substituted with matching value pairs in indexed dictionary are again substituted in their original place. After applying AES in inverse manner and inverse of the Dict substitution we will make the decryption phase of our proposed technique.

RESULTS AND DISCUSSION

For our proposed technique we need a data set to find the result of our proposed technique. For this we get a data set from banking system. The data is in the form of CSV (Comma Separated Values). We can further divide our data set into six data cases named as datacase1, datacase2, datacase3, datacase4, datacase5 and datacase6 for better results.
For the testing purpose of the algorithm designed in this research work, textual data base based on the Bank records is used as for input. It includes the textual format of the records kept by the bank. After getting the data in text form, it is transformed into digital equivalent form using java coding in the Net beans IDE. After that DICT-AES algorithm is applied to each of the data cases and there bits are recorded as were in the original file and number of bits consumed after applying the Dict-AES algorithm. The results are displayed under the following table and discussed afterwards.

File size in bits	Dict-AES	Blowfish	DES	3 DES	AES
1298	1560	1628	1740	1700	1592
1232	1664	1656	1656	1606	1664
1225	1452	1592	1660	1674	1644
1238	1472	1656	1650	1656	1664
1228	1472	1644	1670	1628	1644
1236	1472	1636	1644	1694	1664

Table.1 Number of Bits after Encryption

There numerous parameters like execution time of an algorithm, Avalanche effect and many more parameters which are used to measures the performance of various encryption algorithms.
However we choose only two parameters

i. Compression Ratio

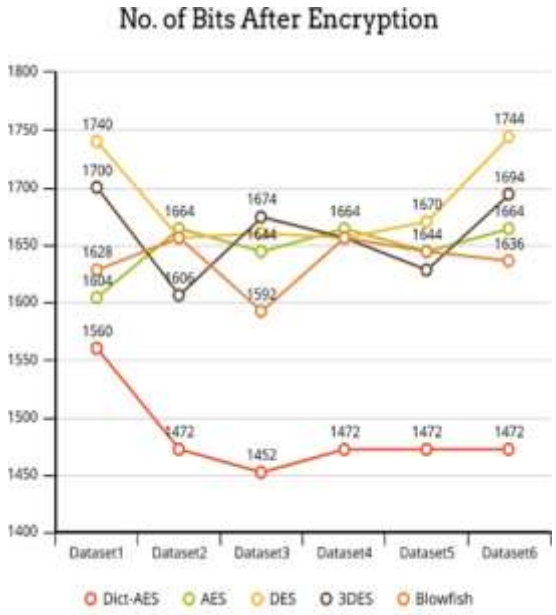
It has been seen in various algorithms after the encryption of data, the size of the encrypted data will become larger than the original data. In our proposed technique, the size of decrypted data will be slightly increase than the original data. Compression ratio defined as the ratio of total bits in any file after encryption/compression to the total number of bits in that original file. The formula for calculating the compression ratio is given as below

$$\text{Compression Ratio} = \frac{Number\ of\ bits\ after\ encryption}{Number\ of\ bits\ in\ original\ file}$$

The following graph shows the compression ratio for Dict-AES, AES, DES, 3DES and Blowfish algorithms.

Graph 1 Compression Ratio of Encryption Algorithms

Some encryption techniques provide better security than other encryption techniques but they cannot be implement due some drawbacks. For an encryption technique to implement successfully, it is mandatory that the size of ciphertext should not much larger than the plaintext. If so, then we need more effort to send that ciphertext to another node. From Graph 1, it is clear that our proposed encryption technique has smallest compression ratio in all datasets except dataset2. As much as value of compression ratio is greater than 1, this means that much percentage size of plaintext is increased after the encryption process. For example, in dataset 1 for Dict-AES algorithm, the compression ratio is 1.20. This means that the encrypted cipher has 20% larger than original plaintext. Here is another graph shows the number of bits after applying the encryption process by various algorithms.



Graph 2 No of Bits after encryption

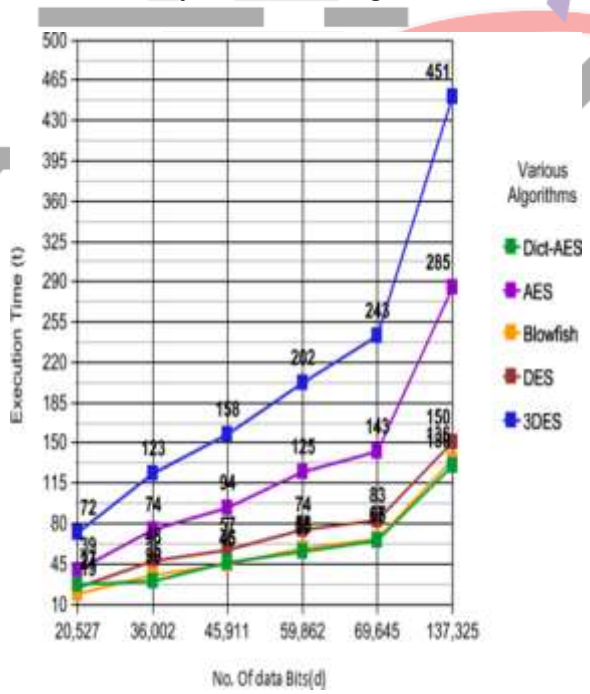
In Graph 2, it clearly shown that number of bits after applying the encryption process by Dict-AES is smaller than AES, DES, 3DES and Blowfish.

Execution Time

The time taken by an algorithm from the initialization of first step to the completion of last step is known as the execution time. In the fast speed data communication, it is every important to keep in mind that the execution time required by an algorithm should be minimum. The execution time is calculated from the formula given below

Execution time = *Time at the end of execution of algorithm – Time at the start of execution of algorithm*

The following graph shows the execution time taken by our Dict-AES algorithm is little bit better than other algorithms.



Graph 3 Execution Time of Various Algorithms

In this graph, we input six data file varying in size from 20kb to 200kb. The output of this graph shows that the proposed technique takes smaller execution time than the other algorithms compared with it. Smaller the execution time of an algorithm, smaller will be its time complexity. The proposed technique will efficient in manner of time complexity as well as space complexity.

ii. Security against Brute Force Attack

Brute force attack is widely used by attack to find the key of any private key encryption algorithm. In this, attacker will try to apply the every possible combination of the key to the encryption algorithm. However, it is very complex and time consuming method but it is most successful method which applied on various algorithms like DES, 3DES, RSA, AES etc. In our proposed technique, if outsider will find the private key then he/she will not able to decrypt the cipher text to plain text because he/she will further needed indexed dictionary to decrypt the data to its original form which gives any extra layer of security to our cipher text. To fully decrypt the data to its original form one will needed private key as well as indexed dictionary.

CONCLUSION

In modern era, every new development or invention of electronic equipment is based on digital signals, due to wide advantages of digital data. As there are numerous pros of internet, digital data, electronic equipment, there are lots of vulnerabilities that need to be taken care of. In the field of Data Security, the attacks on data transmission are getting popularity. Attacks like eavesdropping, traffic analysis, spoofing are very difficult to control and check. This research work propose an efficient and secure data encryption scheme, which leads to make the message meant to be read by such users that have access privileges. Moreover, a protocol to secure the data transmission between the sender and the receiver is also provided. As it is shown through the results and discussion proposed algorithm achieves data compression as well as encryption and performs best when the data bits are in huge number. It also plays handy approach when applied for data having short lengths.

REFERENCES

[1] Sangeeth Rajan "CRYPTOGRAPHY: CONCEPTS, BACKGROUND AND METHODS" International Journal of Emerging Technology and Innovative Engineering Volume 4, Issue 12, December 2018
[2] Gurpreet Singh, Supriya "Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base64 and AES" Second International Conference on Advanced Computing, Networking and Security, 2013
[3] Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" International Conference on Convergence and Hybrid Information Technology, 2008
[4] Neha, Mandeep Kaur 'Enhanced Security using Hybrid Encryption Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2016
[5] Neeraj Kumar "Investigations in Brute Force Attack on Cellular Security Based on DES and AES" International Journal of Computational Engineering & Management, Vol. 14, October 2011
[6] Shashikant Kuswaha, Praful B.Choudhary, Sachin Waghmare, Nilesh Patil "Data Transmission using AES-RSA Based Hybrid Security Algorithms" International Journal on Recent and Innovation Trends in Computing and Communication, Volume 3 Issue 4, April 2015
[7] *Vanishreeprasad. S, Mrs. K N Pushpalatha "Design and Implementation of Hybrid Cryptosystem using AES and Hash Function" Journal of Electronics and Communication Engineering, Volume 10, Issue3, May 2015*
[8] *Noha MM. AbdElnapi, Fatma A. Omara, Nahla F.Omran "A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing" International Journal of Computer Science and Information Security, Volume 14, Issue 4, April 2016*
[9] *Sonia Rani, Harpreet Kaur "Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal" International Journal of Advanced Research in Computer Science, Volume 8,Issue 3, March – April 2017*
[10] *Prof.S.N.Ghosh, Deepak T Biradar, Ganesh C Shinde, Sarika D Bhojane , Manojkumar R Shirapure "Performance Analysis of AES, DES, RSA And AES- DES-RSA Hybrid Algorithm for Data Security" International Journal of Innovative and Emerging Research in Engineering, Volume 2, Issue 5, 2015*
[11] *Amir Mahmud H, Bayu Angga W, Tommy, Andi Marwan E, Rosyidah Siregar "Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data" IOP Conf. Series: Journal of Physics: Conf. Series 1007, 2018*
[12] *Michael Enriquez, Den Whilrex Garcia, Edwin Arboleda "Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA and ElGamal Cryptosystems" Indian Journal of Science and Technology, Volume 10, July 2018*
[13] *Kalyani Ganesh Kadam, Prof. Vaishali Khairnar "HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES" International Journal of Technical Research and Applications, Special Issue 31, September 2015*
[14] *Palanisamy, Jeneba Mary "HYBRID CRYPTOGRAPHY BY THE IMPLEMENTATION OF RSA AND AES" International Journal of Current Research Vol. 33, Issue, 4, April, 2011*
[15] *Jignesh R Patel, Rajesh S. Bansode, Vikas Kaul "Hybrid Security Algorithms for Data Transmission using AES-DES" International Journal of Applied Information Systems, Volume 2, Issue 2, February 2012*
[16] *Daniel J. Bernstein "Understanding brute force" http://citeseerx.ist.psu.edu/viewdoc/download?doi=1 0.1.1.139.4510&rep=rep1&type=pdf*
[17] *Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris "A Survey on the Cryptographic Encryption Algorithms" International Journal of Advanced Computer Science and Applications, Volume 8, Issue 11, 2017*