IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 3, Ser. I (May. – June. 2023), PP 21-27
www.iosrjournals.org

Comparative Analysis Of Selected Symmetric And Assymetric Key Encryption Algorithms: A Review

Mohammad Shohel Rana[1]
[1](*Department of CSE, Southeast University, Bangladesh*

Abstract :
The scope of the establishment of internetworking security is large enough that requires special attention to details to realize its ultimate wholesome state. As soon as the Data/Information is placed in a medium to transmit over to the next hop, it is at risk of being fabricated by the Man-in-the-middle. Over the years many encryption/decryption algorithms were invented to ensure the integrity and authenticity of the content co compiled at the sender end. Cryptography is a subset of cryptography that only deals with encrypting data that can be passed through secure channels along with keys to ensure security. Where cryptology deals with both encryption and decryption processes. Cryptographic algorithms are primarily categorized into two types - Symmetric and Asymmetric. The main objective of this review paper is to identify how some public (asymmetric) and private (symmetric) keys algorithms fare against each category with respect to attack resistance, efficiency, and other relative measures. Two symmetric algorithms namely Hill Cipher and Data Encryption Standards (DES) were compared against two well known asymmetric key algorithms namely RSA and Diffie-Hellman Key Exchange in this study. The computational and implementation complexities of the algorithms were parts of the discussion as well.

Keywords : *Cryptology, Cryptography, Crptanalysis, Symmetric Key Encryption, Assymetric Key Encryption, Man-in-the-middle.*

Date of Submission: 28-04-2023 Date of Acceptance: 09-05-2023

I. Introduction

When the same key is used for both encryption and decryption, it is known as symmetric encryption whereas if participating agents each use a pair of keys named public and private for encryption and decryption, it is known as asymmetric key or public key encryption method. This is a review paper where multiple symmetric and asymmetric algorithms will be compared to see which one is really better in terms of their security features, time complexities, and performance. General rule of thumb is that public key encryption is better; this paper will clarify the truth behind the general belief and enlighten techno savvy people how we could be just as secure using symmetric or same key encryption. Over the years many algorithms came in to ensure the security; this paper will consider three well known public and three private key encryption algorithms to enlighten the general understandings of cryptology and its significance in the secure communication. This paper presents a detailed study of four popular En/Decryption algorithms, and they are DES, Hill Cipher, RSA, and Diffie-Hellman. The use of the internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, the existing work on the Encryption and decryption techniques has been done. Each algorithm technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that asymmetric algorithms are most efficient in terms of speed, time, throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. This paper will contribute important information To setup a more secure environment for data storage and retrieval.

Basic Encryption/Decryption Process

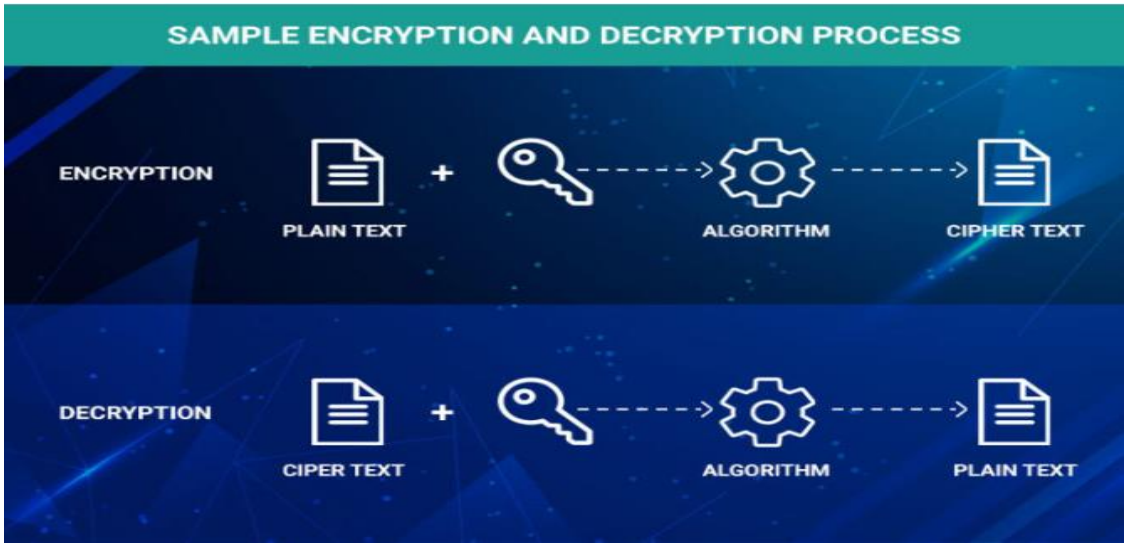

Fig 1.1 - ref: [1]

Plain Text: it is the text which is readable and can be understood by all users.
Cipher Text: the message obtained after applying cryptography on plain text is Cipher text.
Encryption: the method of converting plain text to cipher text is named encryption. It is also called encoding.
Decryption: the method of converting cipher text to plain text is named decryption. It is also termed decoding.

Basic Priciples of Cryptography

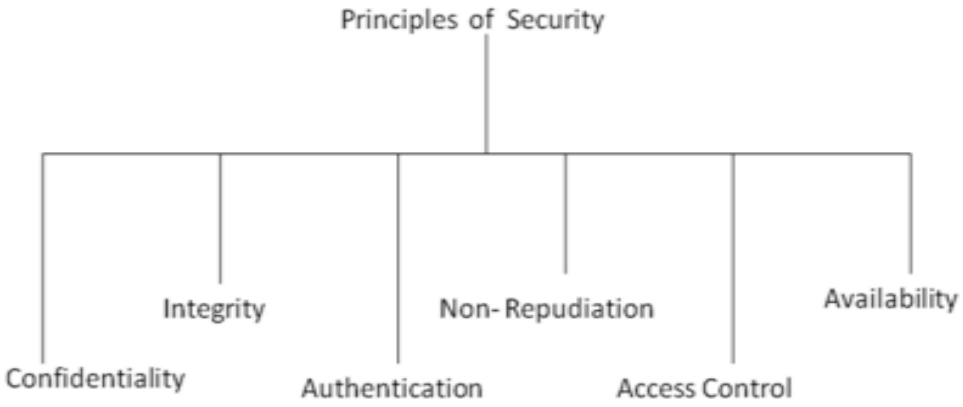

Fig - 1.2 - Basic principles of Cryptography [16]

II. Literature Review

Maqsood, F., Ahmed, M., Ali, M. M., & Shah, have evaluated the performance of different symmetric and asymmetric algorithms by covering multiple parameters such as encryption/decryption time, key generation time and file size [2]. For evaluation purpose, they also have performed simulations in a sample context in which multiple cryptography algorithms have been compared. Hercigonja, Z. (2016) identified the implementation limitations of existing cryptographic algorithms such as DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6 of symmetric techniques and RSA of asymmetric techniques [3]. This paper also analyzes parameters like key exchange, flexibility and security issues of the algorithms which determines the efficiency of the cryptosystem. Jeeva, A. L., Palanisamy, D. V., & Kanagaram, K. (2012) provides a fair performance comparison between the various cryptography algorithms such as the AES, RSA, RC2, DES, 3DES, DSA where both types of symmetric and asymmetric techniques [4]. The authors have compared these parameters for both the symmetric key encryption and for the asymmetric key encryption. The parameters such as the tunability, key length, computational speed, and the type of attacks on the security issues were also discussed. Thambiraja, E., Ramesh, G., & Umarani, D. R. (2012) discussed some of the recent existing encryption techniques and their

security issues [5]. The performance of all those encryption techniques including UMARAM and UR5. Ebrahim, M., Khan, S., & Khalid, U. B. (2014) presents a comprehensive comparative analysis of different existing cryptographic symmetric algorithms based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secure communication over wired and wireless networks [6]. Mitali, V. K., & Sharma analyzed the encryption and decryption time of various algorithms on different settings of data [7]. Mohammad, O. K. J., Abbas, S., El-Horbaty, E. S. M., & Salem, A. B. M. (2013, December) provides a comparative study that represents the differences between modern encryption algorithms in cloud computing [8]. The study also encompasses the key size, the performance and the size of the output encrypted file based on both symmetric and asymmetric algorithms. Al Hasib, A., & Haque, A. A. M. M. (2008, November) presents the fundamental mathematics behind the AES and RSA algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security [9]. It also includes several computational issues as well as the analysis of AES and RSA security aspects against different kinds of attacks including the countermeasures against these attacks. Semwal, P., & Sharma, M. K. (2017, September) discusses the comparison of various cryptographic encryption algorithms with respect to its various key features & then later discusses their performance cost based on the some selected key criteria's [10]. Some of the algorithms chosen for the purpose are DES, 3DES, IDEA, CAST128, AES, Blowfish, RSA, ABE & ECC were also parts of the discussion. Fatima, A., & Nishchal, N. K. (2016) presents two different aspects of cryptanalysis of the optical phase-truncated Fourier transform (PTFT)-based cryptosystem [11]. In the first part, a comparative study is carried out for a specific attack on the PTFT-based scheme in different optical transformation domains. In the second part, a new attack algorithm is proposed. The existing attack algorithms devised for the PTFT-based cryptosystem require knowledge of both the encryption keys for successful retrieval of phase through phase-retrieval algorithms to extract information about the plaintext. Hamouda, B. E. H. H. (2020) analyzed comparative encryption algorithms in performance, three most useful algorithms: Data Encryption Standard (DES), Triple DES (3DES) also known as Triple Data Encryption Algorithm (TDEA), and Advanced Encryption Standard (AES) [12]. They have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. The performance of different algorithms differs according to the inputs. Prajapati, P., Patel, N., Macwan, R., Kachhiya, N., & Shah, P. (2014) accomplishes comparative analysis of encryption standards DES, AES and RSA considering various parameters such as computation time, memory usages [13]. A cryptographic tool is used for performing experiments. Experiments results are given to analyses the effectiveness of symmetric and asymmetric algorithms. Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010) worked on The New Comparative Study between DES, 3DES and AES within Nine Factors achieving an efficiency, flexibility and security, which is a challenge of researchers [14]. Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December) presents the implementation and comparison of RSA, Elgamal and Paillier for variable text files sizes [15]. Their goal was to calculate encryption time, decryption time, throughput, encrypted file size, and decrypted file size for each algorithm to identify which algorithms outperforms others in term of evaluation parameters.

III. Algorithms

Symmetric Encryption - Hill Cipher

In classical cryptography, the **Hill cipher** is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The following discussion assumes an elementary knowledge of matrices. Each letter is represented by a number modulo 26. Though this is not an essential feature of the cipher, this simple scheme is often used:

Encryption:

To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT', and the key below (or GYB/NQK/URP in letters):

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

Thus the enciphered vector is given by:

which corresponds to a ciphertext of 'POH'. Now, suppose that our message is instead 'CAT', or:

This time, the enciphered vector is given by:

which corresponds to a ciphertext of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption:

In order to decrypt, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFK/VIV/VMI in letters). (See matrix inversion for methods to calculate the inverse matrix.) We find that, modulo 26, the inverse of the matrix used in the previous example is:
Taking the previous example ciphertext of 'POH', we get:
which gets us back to 'ACT', as expected.

Two complications exist in picking the encrypting matrix:
1. Not all matrices have an inverse (see invertible matrix). The matrix will have an inverse if and only if its determinant is not zero.
2. The determinant of the encrypting matrix must not have any common factors with the modular base.

Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.
For our example key matrix:
So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher.

The risk of the determinant having common factors with the modulus can be eliminated by making the modulus prime. Consequently, a useful variant of the Hill cipher adds 3 extra symbols (such as a space, a period and a question mark) to increase the modulus to 29.

Symmetric Encryption – DES

The data encryption standard (DES) is a symmetric-key block cipher published by the national institute of standards and technology (NIST).

In 1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal information processing standard (FIPS)

Overview:

Fig 1.3 - DES Encryption Decryption [17]

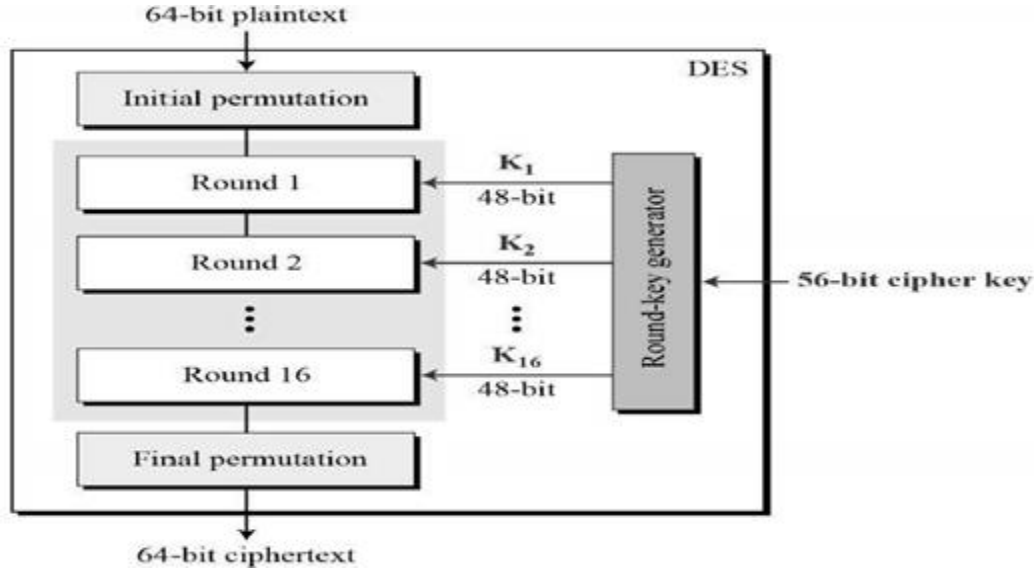

Fig 1.4 - Structure of DES [18]

How Does DES Work

- DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64 bit blocs of cipher text come out.
- It is also a symmetric algorithm, meaning the same key is used for encryption, meaning the same key is used for encryption and decryption.
- It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity
- When the DES algorithm is applied to data it divides the message into blocks and operates on them one at a time.
- The blocks are put through 16 rounds of transposition and substitution functions.
- The result is 64 bit blocks of cipertext.

Asymmetric Encryptions - RSA

RSA - Key Setup :

1. Select primes: p=17 & q=11
2. Compute $n = pq$ =17 x 11=187
3. Compute ø(n)=(p–1)(q-1)=16 x 10=160
4. Select e: gcd(e,160)=1; choose e=7
5. Determine d: d= e^{-1} mod 160 (d = multiplicative inverse of e mod 160) and d < 160 Value is d=23 since 23x7=161=1mod160
6. Public key (e, n) =(7,187)
7. Private key (d, n) =(23,187)

Encryption & Decryption :

- To encrypt a message M (given message M = 88):
  obtains public key of recipient (e,n)
  computes: C = M^e mod n
  C = 88^7 mod 187 = 11
- To decrypt the ciphertext C:
  uses their private key
  (d,n)
  computes:M=C^dmodn
  M=11^{23}mod187=88

Assymetric Diffie-Hellman key exchange algorithm:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables one prime P and G (a primitive root of P) and two private values a and b

P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly, the opposite person received the key and from that generates a secret key after which they have the same secret key to encrypt.

IV. Comparative Analysis

RSA

One of the reason RSA has become most widely used is because it allows either of the two keys to encrypt a message and the opposite key to decrypt it, thus promising confidentiality, integrity, authenticity and non-reputability of data and electronic communications. It's important to note that a weak key generation will make RSA very vulnerable to attacks therefore care must be taken to ensure that two large random prime numbers are used to calculate the modulus, n [10], which will become the public key and the private key will consist of those two primes themselves. The effectiveness of RSA algorithm comes from the fact that it's difficult to computationally factor large integers into primes [12].

Multiplying the two primes is easy but performing the reverse in the form of factoring is actually hard and gets even harder as the values of p and q gets bigger. Take for instance, the RSA Factoring Challenge enacted by RSA Laboratories in 1991, has many moduli still pending to be factored. On 12 December 2009, a 768-bit RSA modulus containing a 232 decimal digit number was factored by a total of 13 researchers over a span of two years using hundreds of parallel computers, a task equivalent to approximately 2000 years of computing on a single-core 2.2 GHz AMD processor [12]. The larger the key length of the modulus, the more time it takes to be factored. The Federal Information Processing Standards Publication (FIPS PUB) 186-4 specifies three choices for the length of the modulus, n, to be 1024, 2048 and 3072 bits. RSA's strength lies in its key size, since it's not easy to factor large primes.

Analysis of Hill Cipher

The basic Hill cipher is vulnerable to a known-plaintext attack because it is completely linear. An opponent who intercepts {\displaystyle n} plaintext/ciphertext character pairs can set up a linear system which can (usually) be easily solved; if it happens that this system is indeterminate, it is only necessary to add a few more plaintext/ciphertext pairs. Calculating this solution by standard linear algebra algorithms then takes very little time.

While matrix multiplication alone does not result in a secure cipher it is still a useful step when combined with other non-linear operations, because matrix multiplication can provide diffusion. For example, an appropriately chosen matrix can guarantee that small differences before the matrix multiplication will result in large differences after the matrix multiplication. Indeed, some modern ciphers use a matrix multiplication step to provide diffusion. For example, the MixColumns step in AES is a matrix multiplication. The function *g* in Twofish is a combination of non-linear S-boxes with a carefully chosen matrix multiplication (MDS).

S.No	Comparison		
	Parameter	***AES***	***RSA***
1.	Approach	Symmetric	Asymmetric
2.	Encryption	Fast	Slow
3.	Decryption	Fast	Slow
4.	Key Distribution	Difficult	Easy
5.	Complexity	O(log N)	$O(N^3)$
6.	Security	Moderate	Highest
7.	Nature	Closed	Open
8.	Secure Services	Confidentiality, integrity, non-repudiation	Confidentiality

Fig 1.3 - Comparison Between Symmetric and Asymmetric Algorithms [16]

V. Future Works

This paper presents a detailed study of four popular En/Decryption algorithm, and they are DES, Hill Cipher, RSA and Diffie-Helman. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, the existing works on the Encryption and decryption techniques has been done. Each algorithm technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that algorithm is most efficient in terms of speed, time, throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. This paper will contribute important information To setup a more secure environment for data storage and retrieval.

VI. Conclusion

Major finding of the study is that- Symmetric encryption algorithms are still widely used algorithms ensuring transmission security. Public key which is also known as asymmetric key encryption is comparatively better in terms of providing security, but it comes with baggage. The asymmetric key encryption process has overhead in terms of time and money associated with the process. Yet, for today's digital nation it is a must have to ensure the best security irrespective of any factor. With that consideration, we can conclude that it is best to use asymmetric key encryption for financial transactions while using assymmtric can best be sured for general encryption security.

References

[1]. https://techblogs.42gears.com/encrypt-and-decrypt-a-message-using-des-algorithm-in-python/
[2]. Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: a comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications, 8(6).
[3]. Hercigonja, Z. (2016). Comparative analysis of cryptographic algorithms. International Journal of Digital Technology & Economy, 1(2), 127-134.
[4]. Jeeva, A. L., Palanisamy, D. V., & Kanagaram, K. (2012). Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications (IJERA), 2(3), 3033-3037.
[5]. Thambiraja, E., Ramesh, G., & Umarani, D. R. (2012). A survey on various most common encryption techniques. International journal of advanced research in computer science and software engineering, 2(7).
[6]. Ebrahim, M., Khan, S., & Khalid, U. B. (2014). Symmetric algorithm survey: a comparative analysis. arXiv preprint arXiv:1405.0398.
[7]. Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(4), 307-312.
[8]. Mohammad, O. K. J., Abbas, S., El-Horbaty, E. S. M., & Salem, A. B. M. (2013, December). A comparative study between modern encryption algorithms based on cloud computing environment. In 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013) (pp. 531-535). IEEE.
[9]. Al Hasib, A., & Haque, A. A. M. M. (2008, November). A comparative study of the performance and security issues of AES and RSA cryptography. In 2008 third international conference on convergence and hybrid information technology (Vol. 2, pp. 505-510). IEEE.
[10]. Semwal, P., & Sharma, M. K. (2017, September). Comparative study of different cryptographic algorithms for data security in cloud computing. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-7). IEEE.
[11]. Fatima, A., & Nishchal, N. K. (2016). Discussion on comparative analysis and a new attack on optical asymmetric cryptosystem. JOSA A, 33(10), 2034-2040.
[12]. Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. Journal of Information Security, 11(3), 138-148.
[13]. Prajapati, P., Patel, N., Macwan, R., Kachhiya, N., & Shah, P. (2014). Comparative analysis of DES, AES, RSA encryption algorithms. International Journal of Engineering and Management Research (IJEMR), 4(1), 132-134.
[14]. Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085.
[15]. Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December). An experimental study on performance evaluation of asymmetric encryption algorithms. In Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12) (pp. 121-124).
[16]. https://ijsrcseit.com/paper/CSEIT1833191.pdf
[17]. https://slideplayer.com/slide/224292/
[18]. https://www.researchgate.net/figure/General-structure-of-DES-algorithm_fig1_323873117