A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms

Shiraz Saptarshi Ghosh
Computer Engineering
Mukesh Patel School of Technology Management and Engineering, NMIMS
Thane, India
shirazghosh@gmail.com

Harshwardhan Parmar
Computer Engineering
Mukesh Patel School of Technology Management and Engineering, NMIMS
Mumbai, India
harshwardhanparmar55@gmail.com

Prasham Shah
Computer Engineering
Mukesh Patel School of Technology Management and Engineering, NMIMS
Mumbai, India
prashamshah88@gmail.com

Krishna Samdani
Assistant Professor
Mukesh Patel School of Technology Management and Engineering, NMIMS
Mumbai, India
krishna.samdani@nmims.edu

***Abstract*— In today's world, data is termed as the new gold. The need for providing security to the data stored on local storage or at a remote location is a must. Various methods and algorithms are used for securing data one of which is using symmetric key cryptography. It is an encryption technique which uses a single key for the encryption and decryption process. This paper provides an extensive literature survey and puts forth a comparative analysis of the existing symmetric cryptography algorithms (Caesar, Vigenère, Data Encryption Standard, Triple Data Encryption Standard, Extended Data Encryption Standard, Rijndael, Twofish, Blowfish, Modified Blowfish) based on their architecture, flexibility, reliability, security and also states the limitations for each that are essential for secure communication through a wired or wireless medium.**

Keywords*— *DES- Data encryption standard, AES- Advanced Encryption Standard, EDES- Extended Data Encryption standard, TDES- Triple Data Encryption Standard, Blowfish, Twofish.

I. INTRODUCTION

Nowadays it is very important to protect the data transmitted over the internet due to the increasing number of cases in which data to confidential between two parties is stolen by intruders. The sheer hostility of the network in question shows us the need to secure information before it to be transmitted over the network. The advantage key encryption is that the confidentiality of the data in question relies on the key and not the algorithm using the key. This means that even if the attacker knows the decryption algorithm, decryption isn't possible unless the attacker knows the key as well. Encryption algorithms can be primarily divided into two types, symmetric and asymmetric key algorithms. Fig. 1 shows the Encryption system Hierarchy. Symmetric encryption process uses only a single Private Key to encrypt as well as decrypt data. There are many different types of symmetric encryption algorithms such as DES [1], TDES [1], Blowfish [5], AES (aka Rijndael) [3], Twofish [4]. Asymmetric encryption uses two different keys namely the private key and the public key to help in achieving encryption or decryption. The different asymmetric encryption algorithms are PGP, RSA, SSH and many more. This paper primarily targets its research towards popular symmetric key Encryption algorithms based on specific criteria.

II. LITERATURE SURVEY

In this section, the above-mentioned symmetric algorithms shall be compared. To understand the applications of these algorithms it is necessary to understand its strengths and shortcomings. The parameters based on which the strengths and shortcomings for the algorithms shall be noted include Architecture, Security, Efficiency (in terms of speed to encryption and Memory utilization) and Drawbacks.

A. Parameters

The parameter's that affect the selection of a certain cipher for a particular application are:

1) Architecture: Defines the basic structure that encompasses how a certain algorithm their respected plain text into its corresponding ciphertext. Based on the usage of a specific key (either secret or public key) we also are able to determine if the algorithm is symmetric or asymmetric.

2) Security: Defines how strong the encryption algorithm is against an attack. Encryption systems strive to satisfy this particular criterion and hence security has become an important criterion among these parameters. Secure encryptions generally use bigger key sizes than its less secure counterparts.

3) Efficiency: A major criterion on which encryption algorithms are analysed. Efficiency basically depends on two main factors such as speed of execution and memory utilization.

4) Limitations: Defines the already known attacks that the encryption is vulnerable to. Helps to decide whether the encryption algorithm must be used or not for a specific application.

B. Encryption System Overview

1) Caesar's Cipher: also known as the shift cipher, Caesar's code or Caesar shift, is a very well-known and easy encryption technique. The name of this encryption algorithm comes after a Roman general Julius Caesar who used this encryption to send encoded data throughout his military.

2) Vigenère Cipher: In 1553 a method to encrypt alphabetic text by using a series of inter lapping Caesar's Ciphers based on a secret key.

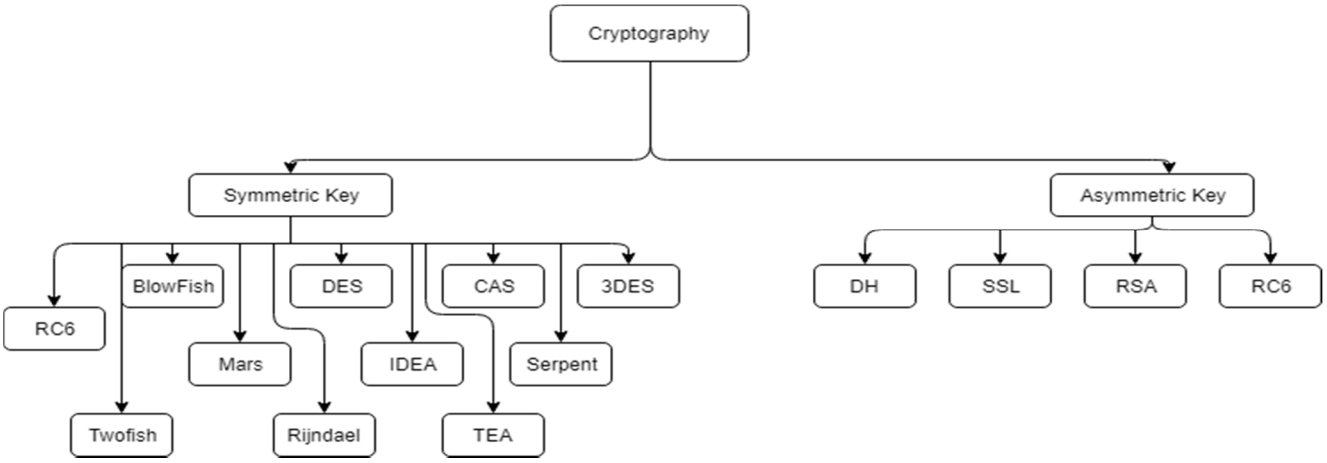

Fig. 1: A hierarchical view of various encryption systems [1]

Though the cipher is easy to understand and implement, for three centuries it resisted all the attempts to break it.

3) DES: Data Encryption Standard was developed in March 1975 by IBM. This is one of the earliest algorithms to be used at such a commercially large scale to protect data. Over the years, due to its small key size and the need to transfer data, it was phased out [1].

4) TDES: Triple Data Encryption standard developed in 1986, was created to remove some of the limitations of the original DES algorithm without making any modifications to the internal components of the DES encryption system [1].

5) Extended DES: The extended DES was designed by Rajay R Pai, Seung J. Han and Menahem Lowy and this algorithm was created to remove the security issues in the traditional DES algorithm while changing the architecture of the algorithm [2].

6) AES (Rijndael): Also known as Rijndael, was developed By Joan Daemen and Vincent Rijmen for the U.S. as its new Encryption standard in October of 2000. It proves an effective resistance against crypto-analytic attacks. AES is the actual name of the standard that was used by the United States and Rijndael is the specific algorithm, but it is most widely known as AES [3].

7) Twofish: The Twofish encryption algorithm was created by Bruce Schneier, and was one of the five finalists nominated to be the United States new encryption standard at the Advanced Encryption Standard contest, but did not get selected for standardization. Twofish is related to the earlier block cipher Blowfish. As of December 2017, Twofish has not been patented and is an open source code [4].

8) Blowfish: Blowfish is a symmetric block cipher that can Replace IDEA or DES as a drop-in replacement. Designed by Bruce Schneier in 1993 Blowfish is a free alternative to many of the present algorithms. This serves as its main advantage since the code is open to all in the public domain [5].

9) Modified Blowfish: This algorithm was developed to remove some issues related to security and processing the speed by changing the f-function calculation but keeps the structure of the algorithm the same [5].

C. Architecture

1) Caesar's Cipher: Caesar's cipher uses a key whose value determines the number of left/right alphabet shifts must be done to produce a valid string from the ciphertext. One of the easiest encryption algorithms, Caesar's is generally used in the creation of more complex ciphers such as the Vigenère cipher.

2) Vigenère Cipher: This cipher uses a textual string as a key, which then is used for doing a number of shifts on the plaintext. For example, let us assume that the key is "yellow". Each alphabet of the key has a numeric value depending on its position in the alphabetical table: In this case,

y=25, e=5, l=12, l=12, o=15 and w=23.

Thus, the key is 25 5 12 12 15 23. Apply Caesar's cipher in the following order with each alphabet in the message incremented with the value of the corresponding key the whole mod.

3) DES: Data Encryption standard is based on the Feistel structure concept. A 64-bit block goes through 16 rounds and uses a key of length 56-bits to produce a ciphertext as shown in Fig. 2. The Key originally has a size of 64-bits (equal to the block size) but in every byte, 1 bit is used as a parity bit and hence isn't used for execution. The 56-bit key is the permuted into 16 subkeys of 48-bits each, used for the 16 rounds. 8 S-boxes are used in the process and the same algorithm in reverse is used for decryption [1].

4) TDES: TDES as the name suggests, uses the DES algorithm thrice on the data block to produce an equivalent ciphertext. As no changes are made to the internal structure of the DES algorithm, TDES still follows the Feistel Structure concept. TDES uses two or three keys in an encrypt-decrypt-encrypt sequence to provide a valid ciphertext. The reverse of the operation is done to convert the ciphertext to plaintext. TDES uses a 64-bit plain text, 48 rounds and a key length of 168-bits with the use of 8 S-boxes to provide an equivalent 64-bit ciphertext [1].

5) Extended DES: The encryption algorithm for the EDES is shown in Fig. 3 Each block of data consists of 96-bits that are divided into three equal sub-blocks (A, B and C) each containing 32-bits. A different f-function is performed for each of the following three sub-blocks and the number of S-boxes generated is increased from 8 to 16. A bigger key of

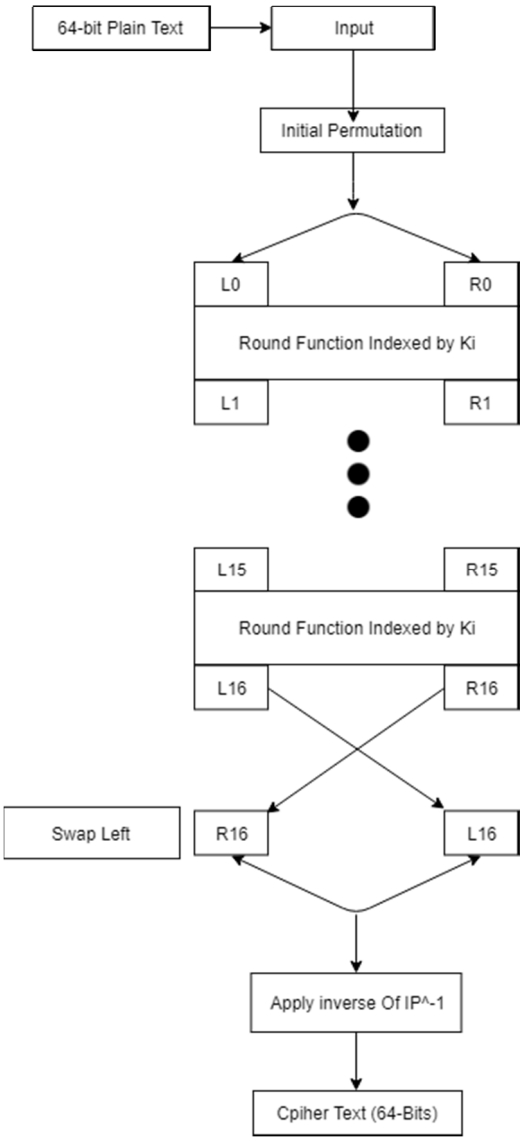

Fig. 2. Working of the DES Algorithm [1]

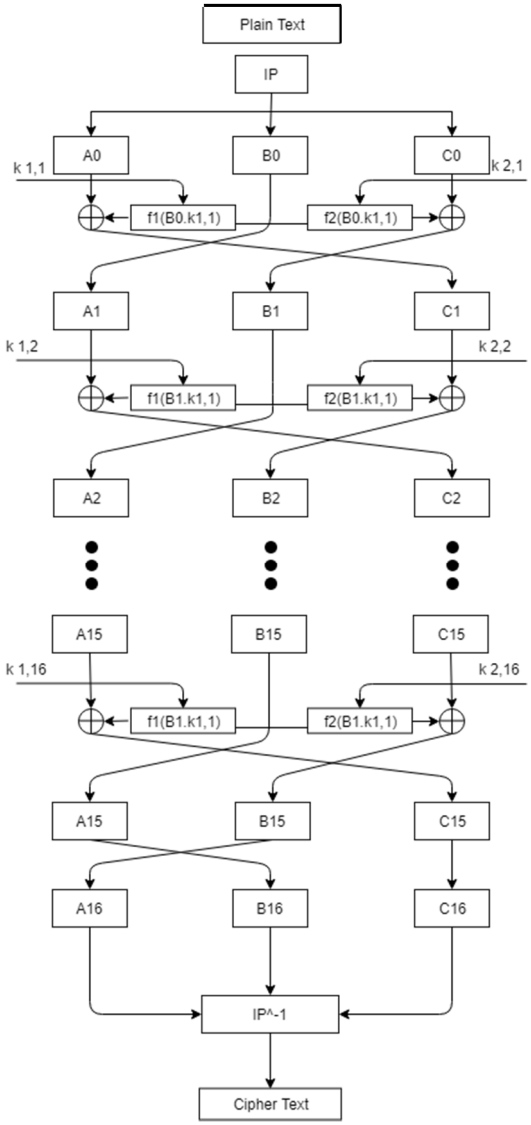

Fig. 3. Working of the EDES Algorithm [2]

each 56-bits long: K1 on the left and K2 on the right. After the first permuted choice (PC-1) each of the 56-bit keys is further divided into left and right keys both of 28 bits each and so on the process is continued for the next 15 rounds [2].

6) AES (Rijnadael): AES is another symmetric key encryption algorithm that uses a 128, 192, 256-bit, plain text that is put through a variable 10,12 or 14 rounds respectively (Default number of rounds=key- length/32+6). Fig. 4 shows this block cipher. Each round has 4 basic functions to be performed namely: 1. Sub bytes, 2. Shift Rows, 3. Mix Columns, 4. XOR nth round key. The last round is the same except for the fact that the Mix Column process is eliminated.

7) Twofish: Based on the Feistel Structure, Twofish is also another symmetric key algorithm. Fig. 5 shows this block cipher. Fig. 6 shows the Internal Round working architecture. This block cipher uses 128-bit plain text and processes it through 16 rounds using a key of variable lengths such as 128,192,256 bit. It also uses 4 S-boxes during the process. The algorithm is reversed to convert the ciphertext back into its corresponding plaintext [4] [11].

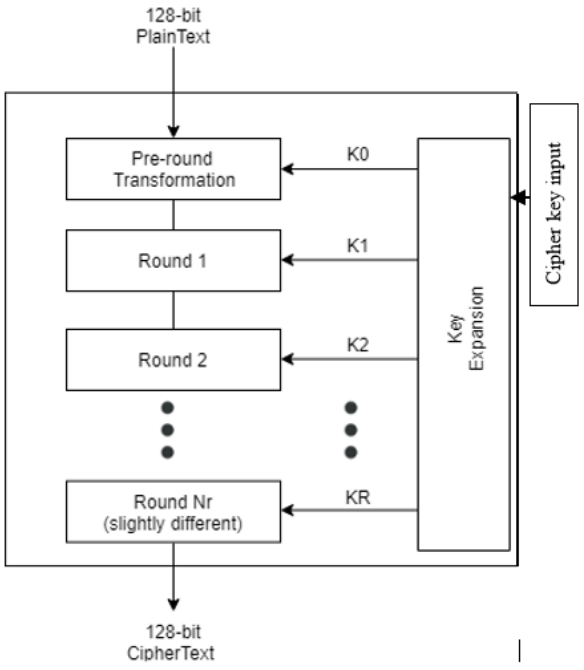

Fig. 4. Working of the AES Algorithm [1]

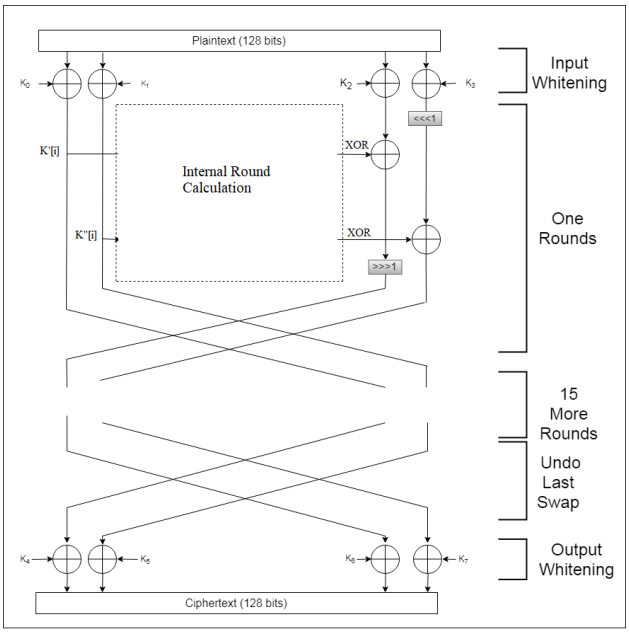

Fig. 5. Working of Twofish Algorithm [4]

8) Blowfish: The Blowfish encryption algorithm is a symmetric cipher which can be used as a replacement for IDEA or DES. It uses a key of variable length, from 32 bits to 448 bits. Fig. 7 shows the architecture of the Blowfish algorithm. The Blowfish algorithm uses the Feistel structure Architecture and is made up 16 rounds. Each of the rounds uses a key that is applied to a data dependent substitution to create a key-dependent permutation. The operation is performed on a 32- bit data set using XOR, the calculations for every round are performed in the following way:

- Divide each block into two parts.
- The new left half is made by the previous rounds right half.
- The new right half is made when XOR is performed on the left half and the result is used after applying function 'f' to the right half and the key shown in Fig. 8.
- The rounds which are prior can be obtained even if the function f is not turned upside down [5].

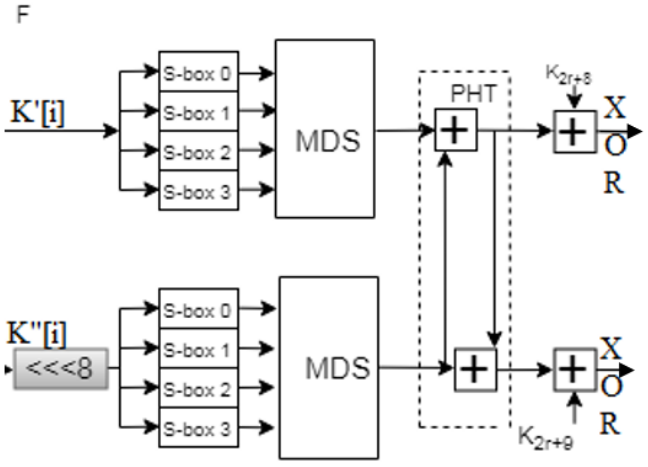

Fig. 6 Internal round calculation for Twofish [4]

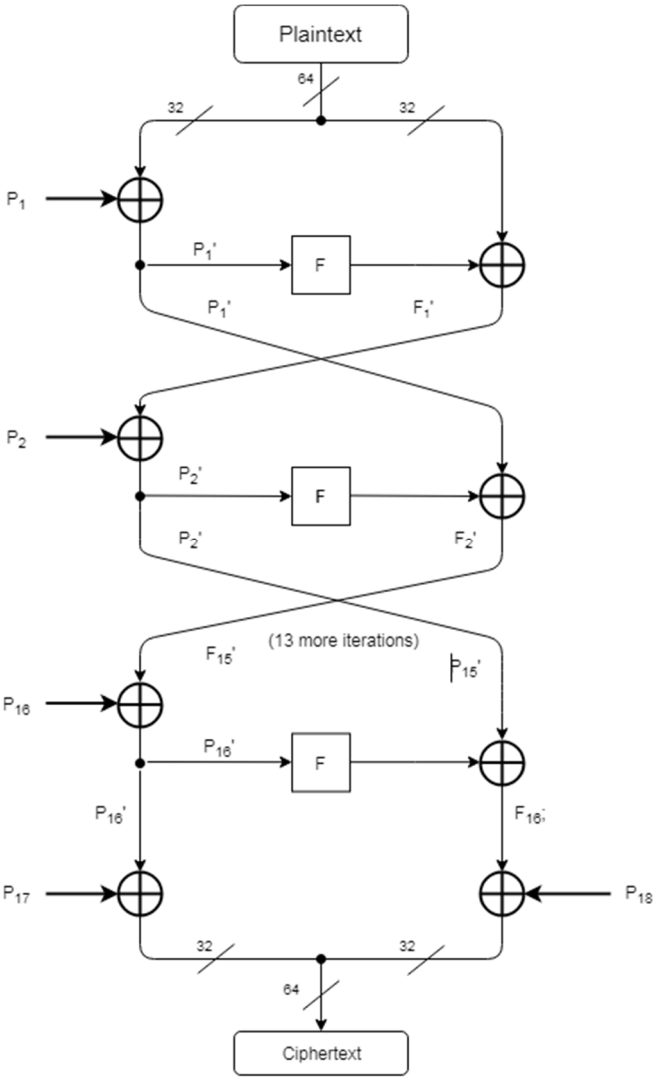

Fig. 7. Working of the Blowfish Algorithm [5]

9) Modified Blowfish: The architecture for the modified blowfish is the same the only difference is that the calculation of the f function has changed wherein the s-boxes 1 and 2 are added and then the values of s box 3 and 4 is added and the then total values of 1, 2, 3 and 4 are XORed and then the value of f function is obtained. This has been proved to be better in terms of encryption quality by some units [5]. Fig. 9 shows the modified F-function calculation described.

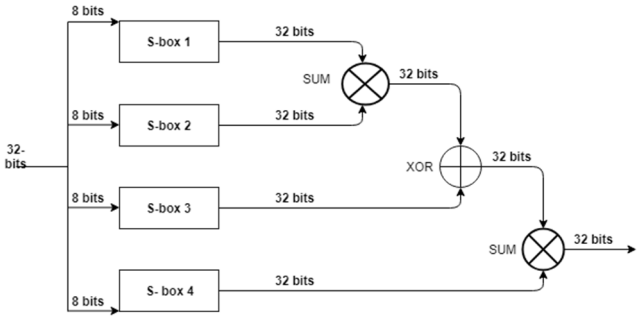

Fig. 8. F-function calculation for Blowfish Algorithm [1]

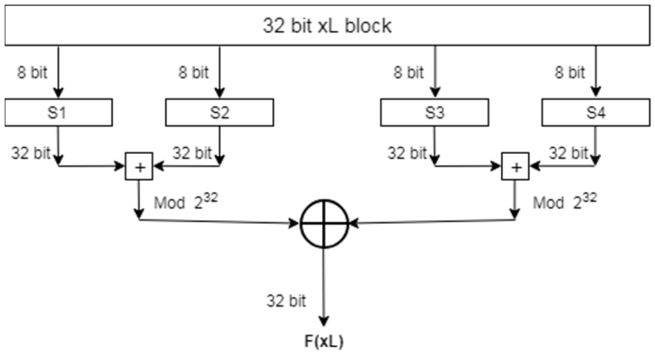

Fig 9. Working of Modified Blowfish Algorithm [5]

D. Security

1) Caesar's Cipher: The cipher with just an alphabetical shift is the easiest to crack and shall take a computer seconds to figure the real answer using brute force.

2) Vigenère Cipher: Although tougher than Caesar's cipher it is comparatively much easier to crack than the rest of the ciphers in this paper. A brute force attack comparing all the words that can be formed using a dictionary can be used to break this cipher.

3) DES: DES uses a 56-bit key size. Hence the number of possible combinations include 2^[56] making it very difficult to originate the real key amongst the others. Moreover, the DES encryption shows a very strong Avalanche effect, hence a very minor change to the data block brings about a significant change to the ciphertext and vice-versa. Initially DES was considered very difficult to crack but later on, Brute force attacks became a major reason to the downfall of this algorithm. In 1998 Electronic Frontier Foundation (EFF) created a machine that used the computing power of all the systems in the world to crack a DES coded ciphertext in one day by finding its key [6]. This proved that a DES-encoded data could no longer be used to encrypt data as it proved to be insecure. However, since it is backwards compatible and has a low cost to upgrade, DES should still be used if it outweighs the risk of exposure.

4) TDES: The key size of TDES is thrice the size of ordinary DES (56+56+56=168-bits). Furthermore, DES operations (encrypt-decrypt-encrypt) are performed thrice in 3DES with 2 or 3 different sets of keys hence providing 112-bits of added security.

5) Extended DES: The security of the extended DES lies in the data block distribution and also the different f functions performed on each of the data blocks while the number of s boxes has been increased from 8 to 16 it helps in making the encryption quality more secure [2].

6) AES (Rijndael): Rijndael has a variable amount of security due to its variable key size. Hence depending on the amount of security required, a key size of up to 256-bits can be used to provide resistance against future attacks. General attacks that were used against rounds editions of Rijndael [7] are Improved Square Attack, Square Attack, Reversed Key Schedule Attack and Impossible Differential Attack, but none of the attacks are actually practically possible.

7) Twofish: The Twofish encryption algorithm is considered very robust a highly resistive towards any key related attacks including related-key differential attack and slide attack since no keys can be used for any related key attack.

8) Blowfish: Blowfish's security lies in its variable key length which is of 32 to 448 bits after the development of the blowfish algorithm many cryptanalysis attacks were made but were not successful, Blowfish is invulnerable to differential key attacks as every bit of the master key involves many round keys which are very much independent [5] [12].

9) Modified Blowfish: Security is the same for both blowfish and modified blowfish the difference is that the quality of encryption has increased as there are certain changes made to the f function and also there are cases where the output file size after encryption has decreased to certain extent which makes the modified blowfish algorithm faster and more efficient than the original Blowfish [5].

E. Efficiency

Efficiency shall be analyzed based on encryption performance and Memory Usage. Encryption performance can be defined as the rate at which its converts a given set of plain text into cypher-text and vice-versa whereas memory usage can be defined as the number of functions that the algorithm performs in order to do its job successfully. Algorithms with high encryption rate and low memory usage are said to have a high degree of efficiency.

Fig. 10 shows a graph of the performance in terms of encryption and decryption speed between different algorithms, the analysis of these algorithms are derived from different research papers.

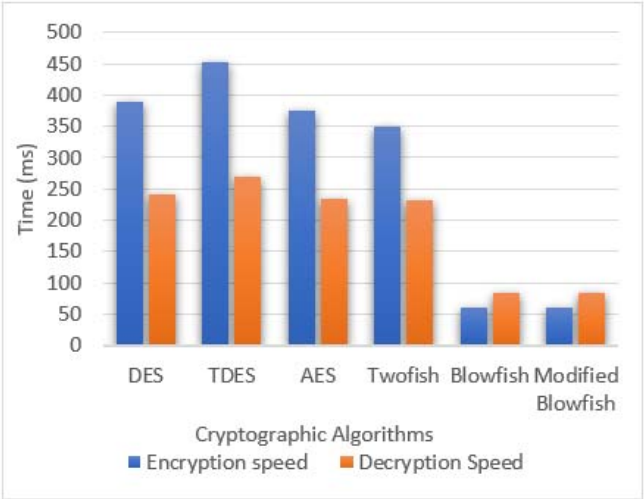

Fig. 10 Encryption and Decryption speed of Cryptographic Algorithms [6]

The paper [8] by Bruce Schneier provides a comprehensive an elaborate analysis of the performance of the five AES finalists showing approximated algorithm speed against on a huge variety of common software and hardware platforms. The papers [1-5] [13] [14] show a comprehensive analysis of all the other algorithms mentioned in this paper. In terms of rate of encryption or throughput, the Blowfish and Modified Blowfish algorithms are clear winners. Fig. 11 shows the memory utilization for the various cryptographic algorithms in question. Whilst triple DES takes the most amount of memory due to its computational algorithm being

thrice the size of a generic DES algorithm, Twofish seems to use the least amount of memory in this category. A proper compilation has led us to the conclusion that AES in terms of

encryption performance and memory utilization takes the first place as the most efficient between the selected algorithms. Whilst 3DES falls in the bottom of these encryption algorithms, in terms of efficiency.

F. Limitations

1) Caesar's Cipher: Due to the ease with which this cipher can be cracked, Caesar's Algorithm isn't used today.

2) Vigenère Cipher: Can only be used on alphabets and not on numbers, symbols or binary digits, hence not very useful.

3) DES: DES has a great vulnerability to linear cryptanalysis attacks. Weak keys also pose a great issue. The small key exposes DES to brute force attack [7].

4) TDES: 3 DES is exposed to related-key and differential attacks. It is also susceptible to certain variation of meet-in-the-middle attack [7].

5) Extended DES: The extended des is limited in the speed section because of the extra steps performed to the data blocks and also it is vulnerable to differential cryptanalysis attack [2].

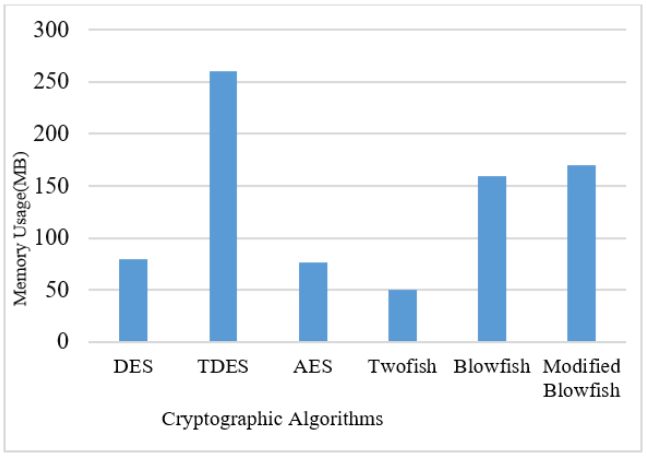

Fig. 11. Memory Utilization of Cryptographic Algorithms [6]

6) AES: AES (Rijndael) has no serious weakness; although it was observed that a certain mathematical property (not an attack) of the cipher can and might be vulnerable into an attack. Further AES (Rijndael) is inappropriate for smart card implementation due to the inverse cipher implementation [8].

7) Twofish: Twofish is susceptible to chosen-key attacks that may cause a reduction to the security of algorithm when applied to certain methods, such as a hash function [8].

8) Blowfish: As there is a range of keys from 32 to 448 there are cases where there are certain keys which are weak and also the encryption speed decreases as the size of memory increases and also it is vulnerable to differential attack hence it is not very reliable [5].

9) Modified Blowfish: The modified blowfish has the same limitations as the blowfish but adding to it can be the extra steps performed used to calculate the f function which increases the speed but it is still vulnerable to differential attack [5].

III. Inferences

Comparing the above-mentioned algorithms Table. 1 is created, showing the encryption times of the following algorithms. On an average, the AES algorithm fares as one of the best of algorithms to use with its High encryption rate and low memory utilization. The DES encryption although efficient lacks in security. TDES due to its structure may be considered one of the safest algorithms but suffers in terms of encryption rate being the slowest out of all these ciphers. Blowfish and Twofish have comparable execution speeds but don't triumph AES encryption. These encryption techniques can also be used in wireless sensor networks. One such example of an application using encryption is a money transfer application such as Paytm which uses 128-bit encryption to secure transactions from one account. Many e-commerce websites use encryption algorithm techniques to secure their payment gateway and also secure their data [10].

TABLE 1. A Comparison of execution time [9]

	A Comparison of Execution Time					
Sr.no	***Input size (Kbytes)***	***DES***	***3DES***	***AES***	***Blowfish***	***Modified Blowfish***
8	256	29	54	59	36	36
2	512	33	48	38	36	36
3	512	49	81	90	37	37
4	1024	47	111	112	45	45
5	1024	82	167	164	45	45
6	1024	144	226	210	46	46
7	2048	240	299	258	64	64
8	2048	250	283	208	66	66
9	2048	1296	1466	1237	122	122
10	2048	1695	1786	1366	107	107
Average Time (ms)		389	452	374	60.3	60.3

IV. Conclusion

In this paper we have given a detailed analysis of the symmetric block encryption on the basis of different parameters where our goal was to analyze the performance of the popular symmetric algorithms on the basis of Security, Architecture, Limitations and Efficiency and to highlight the weakness of different algorithms and it was found that AES was the best algorithm in terms of security efficiency and architecture.

References

[1] Mukta Sharma and R.B.Garg,"DES: The oldest symmetric block key Encryption algorithm", IEEE Conference Publications, November 2016.
[2] Rajay R. Pai, Seung J. Han, Menahem Lowy,"DESIGN AND IMPLEMENTATION OF THE EXTENDED DATA ENCRYPTION STANDARD", IEEE Conference Publications, October 2012.
[3] Shivlal Mewada, Pradeep Sharma, S. S. Gautam"Exploration of Efficient Symmetric AES Algorithm", IEEE Conference Publications, March 2016.
[4] Dr. S.A.M Rizvi, Dr. Syed Zeeshan Hussain, Neeta Wadhwa,"Performance Analysis of AES and Two Fish Encryption Algorithm Schemes", IEEE Conference Publications, June 2011.
[5] Tingyuan Nie, Teng Zhang,"A Study of DES and Blowfish Encryption Algorithm", IEEE Conference Publications, Jan 2015.
[6] Shashi Mehrotra Seth, Rajan Mishra,"Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011

[7] Limor Elbaz, Hagai Bar-El,"Strength Assessment of Encryption Algorithms", Discretix technologies, October 2000.
[8] Bruce Schneier, Doug Whiting, "A Performance Comparison of the Five AES Finalists", third AES Candidate Conference, April 2000, pp. 123-135.
[9] A1am, 1. M., Khan, R. M.," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research ID Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.
[10] Diaa Salama Abdul. Elminaam1, Hatem Mohamed Abdul Kader2 and Mohie Mohamed Hadhoud3," Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Sci 280 ence and Network Security, VOL.8 No.12, December 2008.
[11]Bruce Schneier, "Twofish", Website: https://www.schneier.com/academic/twofish/,October 2018.
[12] Bruce Schneier, "Blowfish", Website: https://www.schneier.com/academic/blowfish/, October 2018.
[13] Comparison of ciphers, "Summary of algorithms", Website: http://www.javamex.com/tutorials/cryptography/ciphers.shtml, October 2018.
[14] Md Imran Alam, Mohammad Rafeek Khan,"Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.