A

* + Project Report
  + on

**“Comparing Cryptography Algorithms”**

submitted in partial fulfillment of the requirement for the award of the

Degree of

Bachelor of Computer Application

**



# Submitted to: Submitted by:

# Ms.Moumita Ghosh Ranjan kumar(181279024)

**Assistant Professor BCA- 2nd Year**

**Department of Computer Applications**

**CONTENTS:**

1. INTRODUCTION

2. SYMMETRIC & ASYMMETRIC

3. POSSIBLE ATTACKS

4. COMPARING ALGORITHMS

4.1 DES

4.2 TRIPPLE -DES

4.3 AES

4.4 BLOWFISH

4.5 RSA

5. RESULT AND DISCUSSION

6. CONCLUSION

7. REFERENCES

**1. INTRODUCTION**

Data which can be read and understood without any special measures is called as plaintext. Disguishing plaintext in such a manner to conceal its actual significance is called encryption. Encoding plaintext brings about muddled drivel structure called figure content. Encryption is done to conceal the information from anybody for whom it isn't proposed. Returning the figure content to its unique plaintext is called as unscrambling. DES strategy is utilized to store touchy data or transmit data across shaky systems so it can't be perused by anybody with the exception of the expected beneficiary. Information encryption standard uses cryptographic calculation that can be utilized to secure electronic information. There are three techniques for encryption standard they are symmetric cryptography, lopsided cryptography and hash work. DES calculation utilizes symmetric cryptograph. Square figure calculation is utilized for encryption and unscrambling reason and the message is partitioned into squares of bits. DES forms the info information (Original message) of square size 64-bits and a mystery key of 64-bits to give a 64-piece figure content.

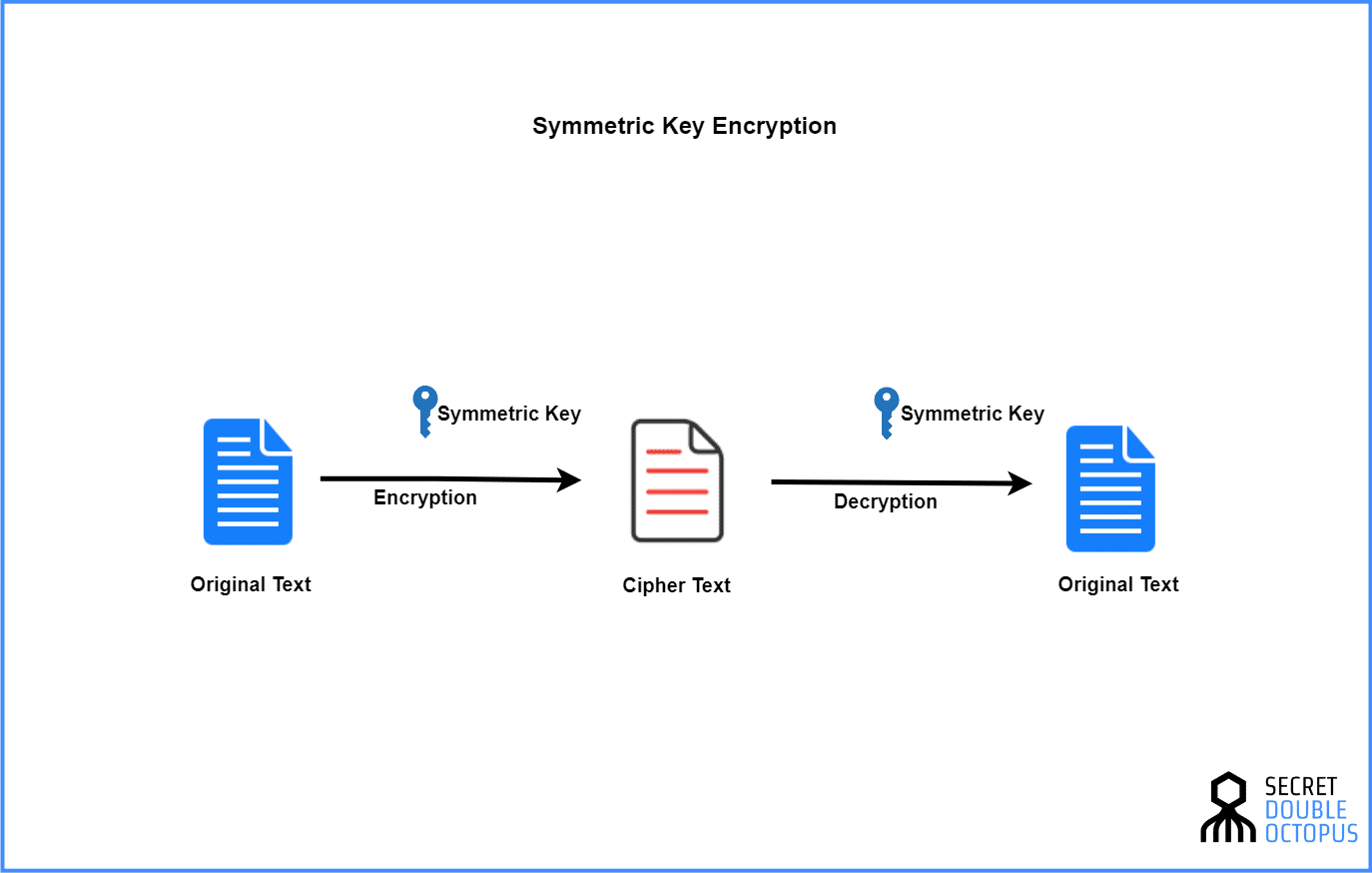
Cryptography is gotten from Greek language kryptos implies covered up and grafos significance compose or talk which means investigation of concealing data. It is the study of making sure about information. Cryptography is a study of utilizing arithmetic to encode and unscramble information. Cryptography empowers to store significant information or transmit it across shaky systems with the goal that it can't be perused by anybody aside from the expected beneficiary. Cryptography models incorporate the security of the ATM cards, PC passwords and electronic business which all rely on cryptography.

**2.** **SYMMETRIC & ASYMMETRIC**

**Symmetric** key cryptography is any cryptography calculation that depends on a common key that is utilized to encode or decode content/cypher text, in agreement to asymmetric key cryptography, where the encryption and unscrambling keys are unique.

Symmetric encryption is commonly more effective than unbalanced encryption and in this way favored when a lot of information should be traded.

Building up the mutual key is troublesome utilizing just symmetric encryption calculations, so by and large, an awry encryption is utilized to set up the common key between two gatherings.



**Fig 1.1**

**Asymmetric** cryptography, otherwise called open key cryptography, is a procedure that utilizes a couple of related keys - one open key and one private key - to encode and decode a message and shield it from unapproved access or use. An open key is a cryptographic key that can be utilized by any individual to encode a message so it must be deciphered by the proposed beneficiary with their private key. A private key - otherwise called a mystery key - is imparted distinctly to key's initiator.

AsymmetricEncryption utilizes two particular, yet related keys. One key, the Public Key, is utilized for encryption and the other, the Private Key, is for unscrambling. As inferred in the name, the Private Key is planned to be private with the goal that solitary the confirmed beneficiary can decode the message.

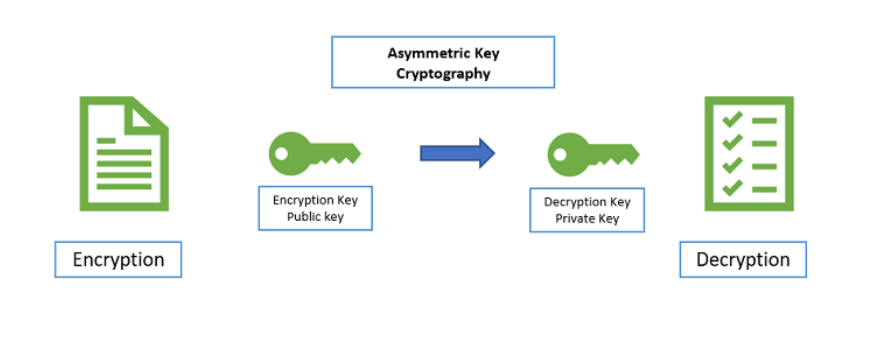


Fig 1.2

**3. POSSIBLE ATTACKS**

***Passive Attack***

The fundamental objective of a uninvolved assault is to acquire unapproved access to the data. A Passive assault endeavors to learn or utilize data from the framework yet doesn't influence framework assets. Latent Attacks are in the idea of listening stealthily on or checking of transmission.

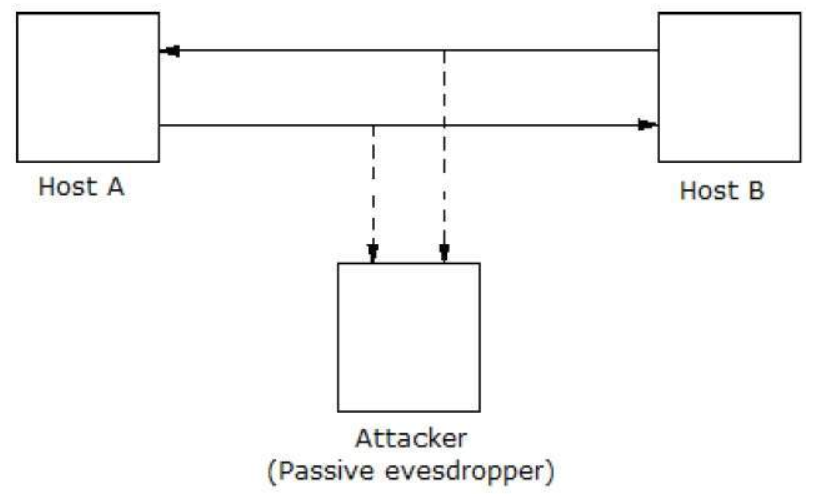


Fig 1.3

## ***Active Attacks***

A functioning assault includes changing the data here and there by leading some procedure on the data. For instance,

1.Altering the data in an unapproved way.

2.Starting unintended or unapproved transmission of data.

3.Change of validation information, for example, originator name or time stamp related with data

4.Unapproved cancellation of information.

5.Forswearing of access to data for authentic clients (disavowal of administration).

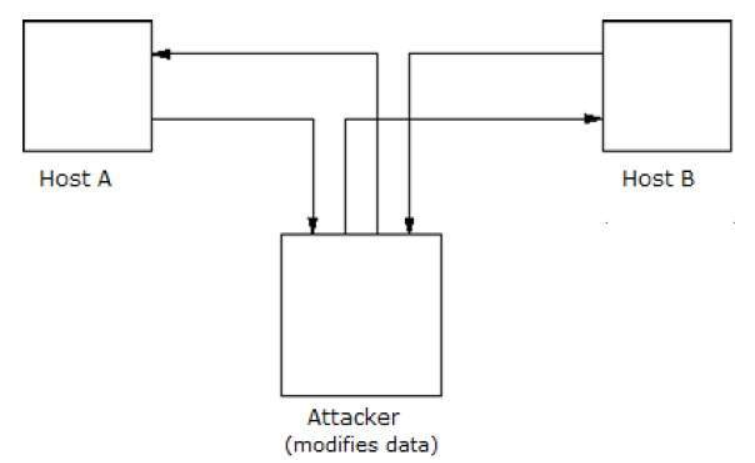


Fig 1.4

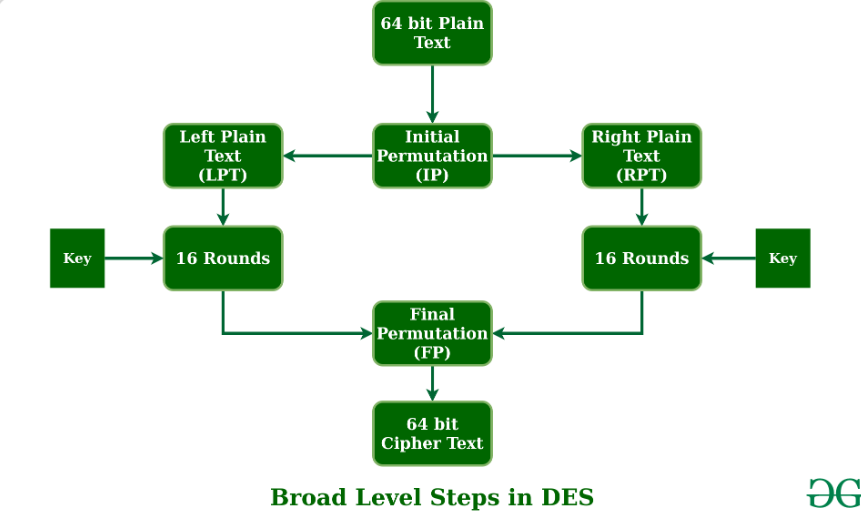
1. **COMPARING ALGORITHMS**
   1. **DES (DATA ENCRYPTION STANDARD)**

**Data Encryption Standard (DES) is a square figure calculation that takes plain content in squares of 64 bits and changes over them to figure content utilizing keys of 48 bits. It is a symmetric key calculation, which implies that a similar key is utilized for encoding and decoding information.**

***Steps for generating keys***

There are 16 rounds of encryption in the calculation, and an alternate key is utilized for each round. How keys are generated is listed below.Bits are named from 1 to 64 beginning from the most significant bit and going to the least significant bit. First we need to pack and transpose the given 64-piece key into a 48-piece key at that point partition the outcome into halves i.e C and D. C and D are left-moved circularly. For encryption adjusts 1, 2, 9, and 16 they are left moved circularly by 1 piece; for the entirety of different rounds, they are left-circularly moved by 2. In the wake of moving the outcome is compacted to 48 bits in understanding. The aftereffect of moving is the contribution for the following round of key age

## 

Fig 1.5

(<https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>)

* 1. **TRIPPLE -DES**

Triple Data Encryption Standard (DES) is a sort of electronic cryptography where square figure calculations are applied multiple times to every datum square. The key size is expanded in Triple DES to guarantee extra security through encryption capacities. Each square contains 64 bits of information. Three keys are alluded to as group keys with 56 bits for each key. There are three entering choices in information encryption guidelines:

1.All keys being free

2.Key 1 and key 2 being free keys

3.Each of the three keys being indistinguishable

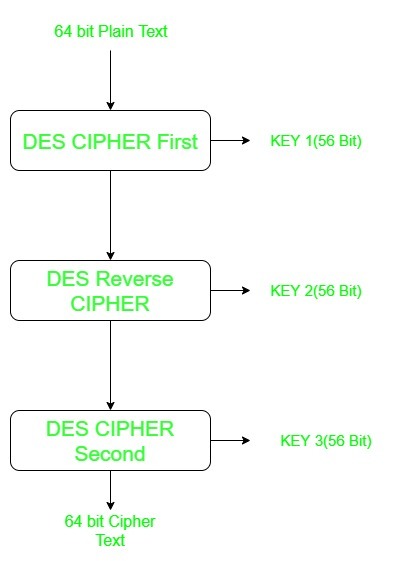


Fig 1.6

(<https://www.geeksforgeeks.org/double-des-and-triple-des/>)

**4.3 AES**

The more famous and broadly received symmetric encryption calculation liable to be experienced these days is the Advanced Encryption Standard (AES). It is found in any event six time quicker than triple DES. A swap for DES was required as its key size was excessively little. With expanding figuring power, it was viewed as defenseless against comprehensive key pursuit assault. Triple DES was intended to conquer this disadvantage yet it was discovered moderate.

AES is an iterative rather than Feistel cipher. It depends on 'substitution–permutation network'. It contains a progression of connected tasks, some of which include supplanting contributions by explicit yields (replacements) and others include rearranging bits around (stages). Strangely, AES plays out the entirety of its calculations on bytes instead of bits. Consequently, AES treats the 128 bits of a plain text obstruct as 16 bytes. These 16 bytes are orchestrated in four segments and four columns for handling as a framework . In contrast to DES, the quantity of rounds in AES is variable and relies upon the length of the key. AES was used 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds utilizes a different 128-bit round key, which is determined from the first AES key.

## 

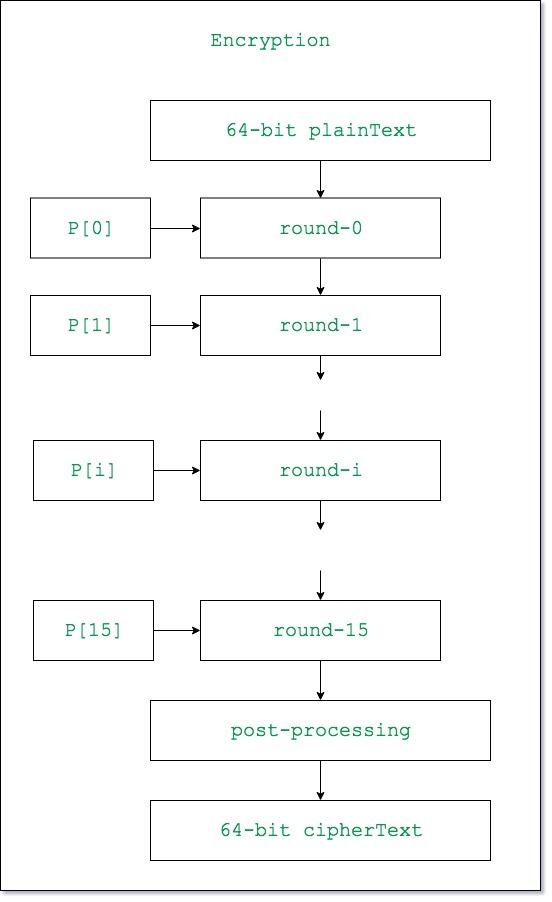
## Fig 1.7 AES Structure

## (<https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm>)

**4.4 BLOWFISH**

Blowfish is an encryption procedure planned by Bruce Schneier in 1993 as an option in contrast to DES Encryption Technique. It is fundamentally quicker than DES and furnishes a decent encryption rate with no viable cryptanalysis procedure found to date. It is one of the main, secure block cyphers not expose to any licenses and consequently unreservedly accessible for anybody to utilize.

1. Block Size: 64-bits
2. Key Size: 32-bits to 448-bits variable size
3. Number of sub keys: 18 [P-array]
4. Number of rounds: 16
5. Number of subsitution boxes: 4 [each having 512 passages of 32-bits each]



## Fig 1.8(Encryption process)

(<https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/> )

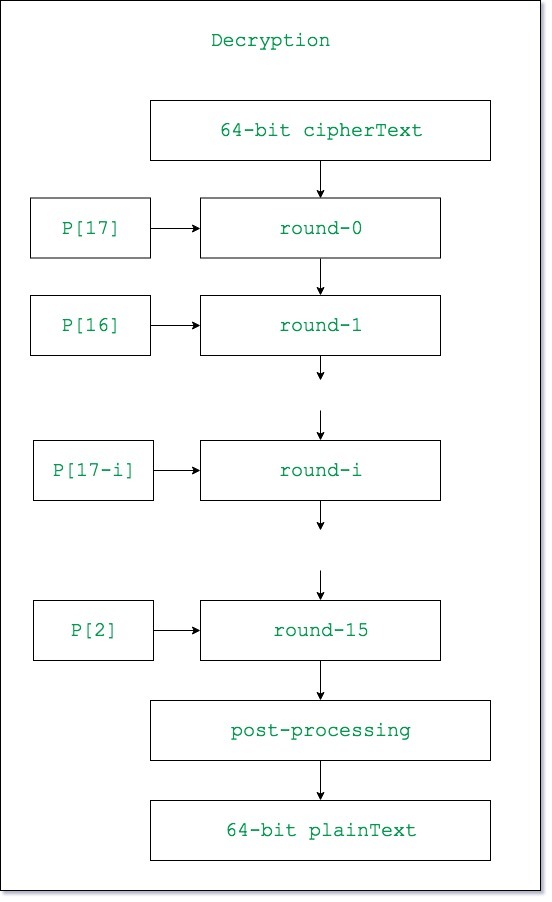


Fig 1.9(Decryption process

(<https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/>)

**5. RESULT AND DISCUSSION**

The result based on the implementation of string pattern:

DES Algorithm:

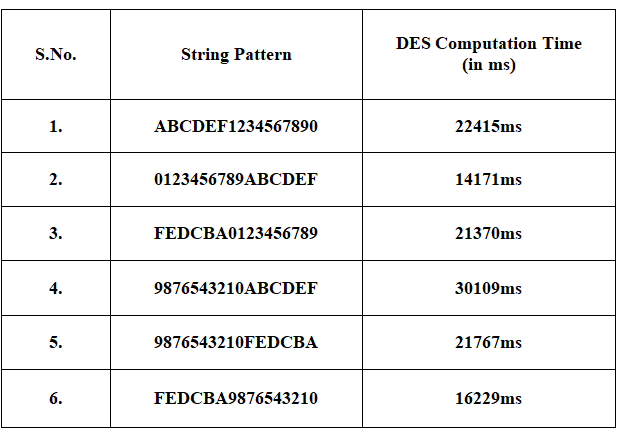


Table 1.1(String Pattern vs Time)

Time and Pattern Graph

Triple DES Algorithm:

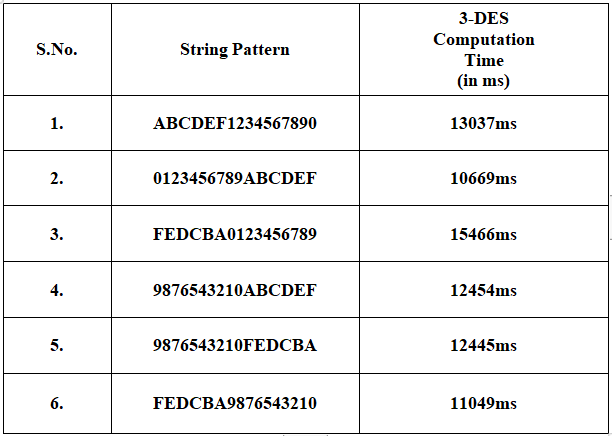


Table 1.2(String Pattern vs Time)

Time and Pattern Graph

AES Algorithm:

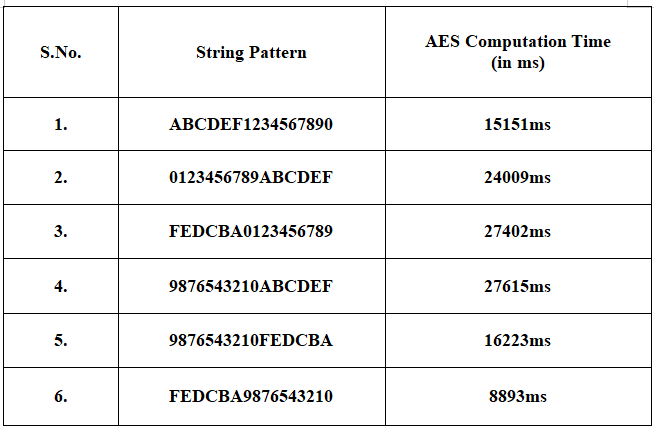


Table 1.3(String Pattern vs Time)

Time and Pattern Graph

Blowfish Algorithm:

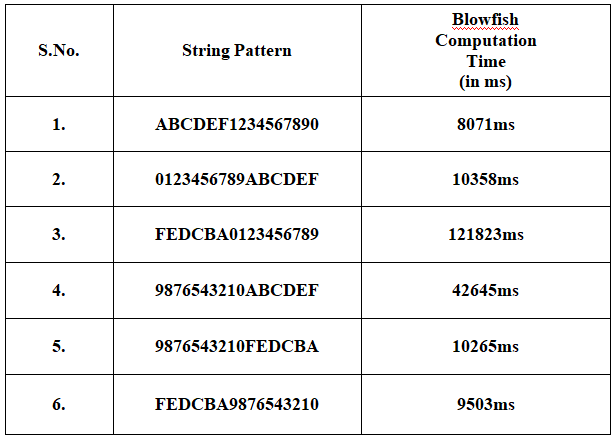


Table 1.4(String Pattern vs Time)

Time and Pattern Graph

Fig 2.0

(Encryption& Decryption time vs. String pattern for DES, 3DES, AES and Blowfish )

Fig 2.0 shows that the 3-DES algorithm records the fastest encryption& decryption time.

Based on the encryption& decryption time (for string pattern)we will select the 3-DES technique for further evaluation.

*Comparison of memory Used* :

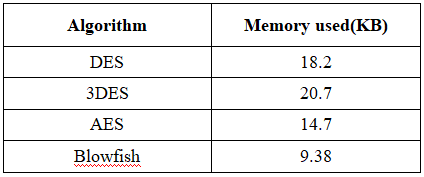


Table 1.4

In the table 1.4 presents that memory used for until operations for all cryptographic techniques that we studied. Blowfish consumed less memory storage than other types, while 3DES uses the highest memory.

1. **CONCLUSION**

Every one of cryptographic calculations has shortcoming focuses and quality focuses. We select the cryptographic calculation dependent on the requests of the application that will be utilized. From the examination results and the correlation, the blowfish calculation is the ideal decision if there should be an occurrence of time and memory as indicated by the measures of speculating assaults and the necessary highlights, since it records the most limited time among all calculations. Additionally, it devours the base memory stockpiling. On the off chance that secrecy and uprightness are central point, AES calculation can be chosen. On the off chance that the interest of the application is the system data transmission, the DES is the best choice. We can think about that blowfish and AES calculations are utilized to keep the application from speculating assaults and it tends to be applied on all the web conventions that depend on IPv4 and IPv6 and the assessments recoded in this paper indicating that all the calculations and the classes are worked well with various execution time and memory utilization.

1. **REFERENCES**

<https://www.sciencedirect.com/topics/computer-science/cryptographic-algorithm>

<https://en.wikipedia.org/wiki/Cryptography>

<https://www.geeksforgeeks.org/cryptography-and-its-types/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php>