Secure TCP-IP Network Algorithm

Dr. Taif S. Hasan
Computer Science Department
Al-Mamoon University College

ABSTRACT

In recent days network plays a key role in most modern applications. Especially through the services provided by Internet. Our paper presents simple rigid network security system. The system adopt the Transmission Control Protocol (TCP) as main protocol. TCP protocol is reliable connection protocol, but the main security method use are simple. And there is a need to improve its facilities. Blowfish is simple fast secure algorithm. By adopting the Blowfish method in specific position in the hierarchy of the TCP-IP layer a new secure model will be result. Also the system has the ability to be used with any recent application by follow simple steps.

***Keywords**: TCP-IP, Blowfish, Socket, Network, Security*

Introduction

The TCP/IP (transmission control convention/Internet convention) suite of protocols is the situated of conventions used to impart over the web. It is additionally broadly utilized on numerous authoritative systems because of its adaptability and wide show of usefulness gave. Microsoft who had initially built up their own particular arrangement of conventions now is all the more broadly utilizing TCP/IP, at first for transport and now to bolster different administrations. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption[1].

Papers Review

1. A New Security Architecture for TCP/IP Protocol Suite, International Journal of Advances Research in Computer Science,Volume1, No. 3, Sept-Oct 2010, M. Anand Kumar, Dr. S. Karthikeyan. In this paper a suggestion for a new security layer for TCP-IP. [2]
2. Security Issues in the TCP/IP Suite, Prabhaker. Department of Computer Science and Engineering, Wright State University, Dayton, Ohio 45435, This paper give a description for the weak point in the TCP-IP protocol. [3]
3. A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enjancement, Mohammad Al-Jarrah, and Abdel-Karim R. Tamimi. They introduce security policy , security control, and data security layer. [4]
4. An Enhanced Security for TCP/IP Protocol Suite, Internation journal of Computer and mobile computing, Dr. M. Anand Kumar, Dr. S, Karthikeyan, propose security architecture for TCP/IP protocol. [5]
5. Security analysis of TCP/IP Networks, Miroslav Sveda, Ondrej Rysavy et al Deal with security analysis for the TCP/IP protocol. [6]
6. Security Model for TCP/IP Protocol suite. M. ANAnd , Dr S. KrthikeyanKumar Also introduce new layer. [7]
7. In Blowfish algorithm, *e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16,* Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83 www.iosrjournals.org www. Ms NehaKhatri – Valmik1, Prof. V. K Kshirsagar2, Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India. [8]

The Proposed System

Our system mainly depends. The propose system depend basically on the use of the blowfish encryption technique through the TCP-IP layers. Each TCP/I layer perform specific function, In order to keep the layers without

any undesired modification and effects such as add extra difficulties, make conflict, change the data path, and others; the adopted model add extra layer responsible of security issues. The blowfish will be contained in the extra security layer. Figure 1 show the model structure.

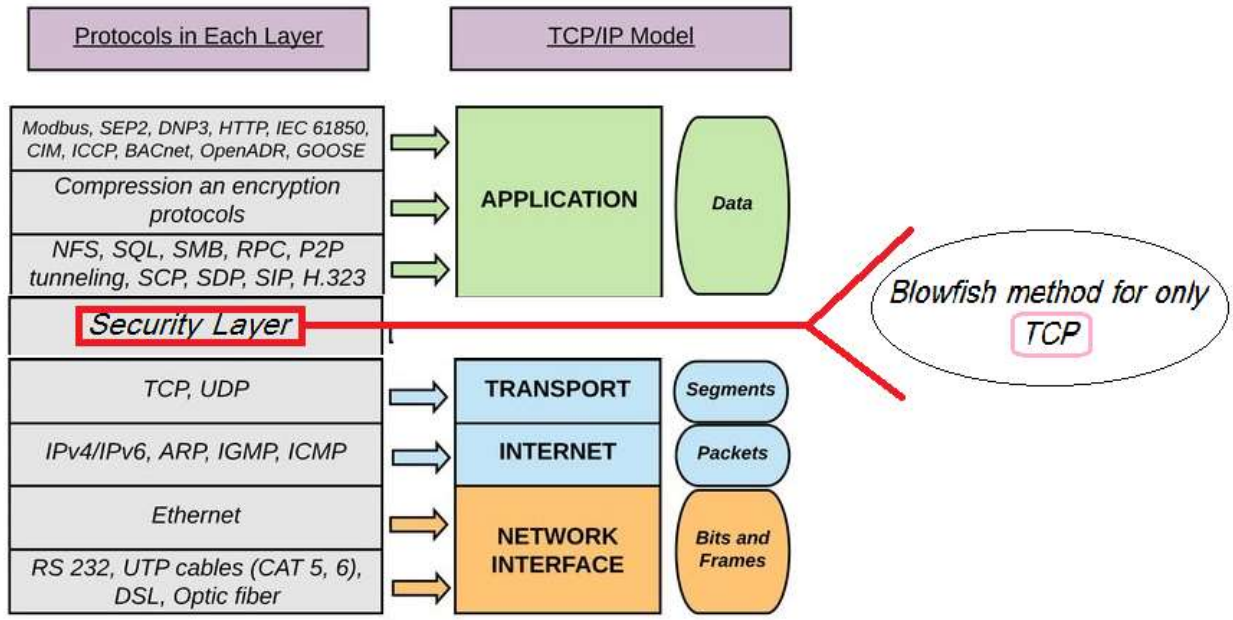


Figure (1) The Proposed Model

The Cryptography

In cryptography a side channel attack is an attack based on information gained from the physical implementation of a cryptosystem rather than brute force (or) theoretical weakness in the algorithms. For example timing information, power consumption, electromagnetic leaks or even sound can provide extra source of information which can exploit to break the system. Some side- channel attacks requires technical knowledge. As mentioned there are two types of cryptography in use today i.e., symmetric (or) secret key cryptography and asymmetric or public key cryptography. Symmetric is the oldest one. Secret key cryptography involves the use of only one key which is used for both encryption and decryption. [9]

Blowfish Encryption Method

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

- **Key sizes:** 32–448 bits
- **Block sizes:** 64 bits
- **Rounds:** 16
- **Structure:** Feistel cipher
- **Designers:** Bruce Schneier
- **First published:** 1993
- **Successors:** Twofish

As mention before the blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption as shown in Figure 2. [10]

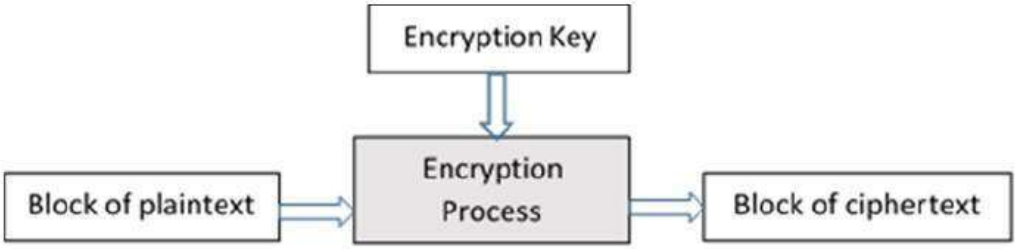
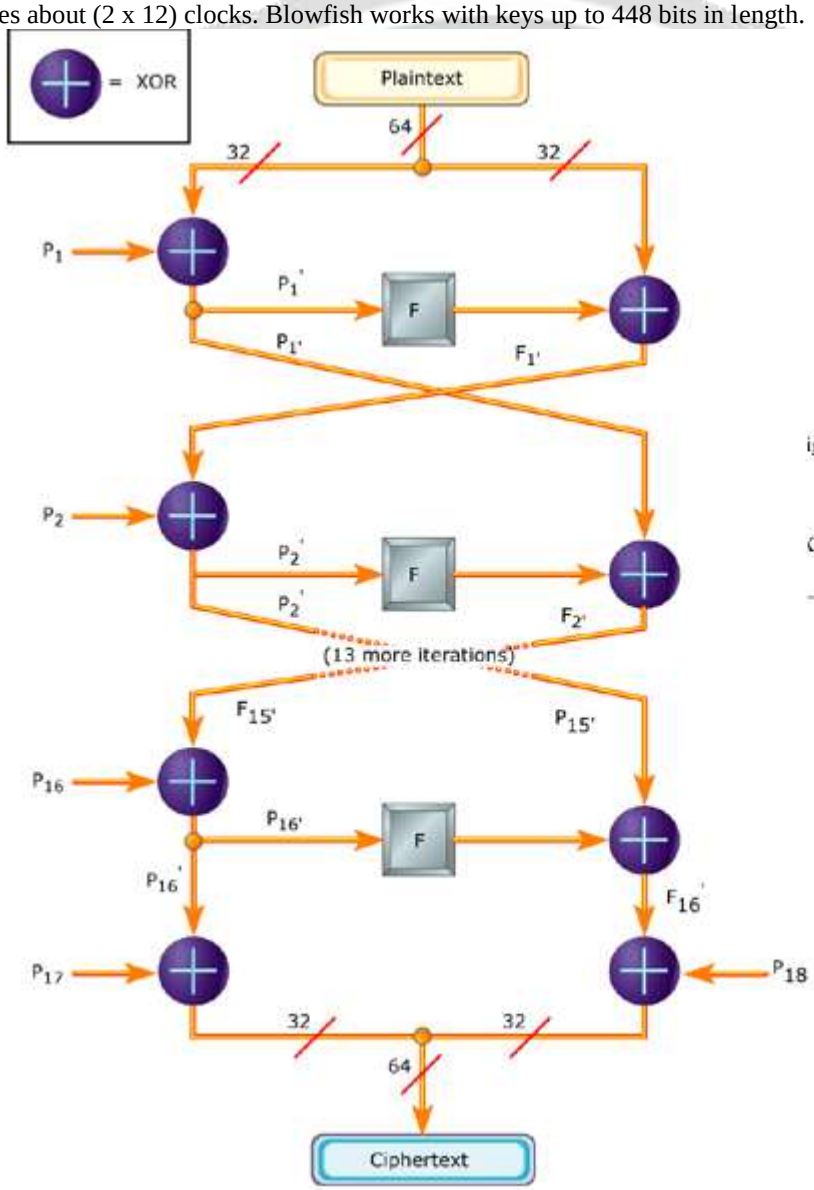


Figure (2) The Block Cipher

Blowfish Algorithm

Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. (Not-so-careful implementations, like Kocher, don't increase that time by much.) Longer messages increase computation time in a linear fashion; for example, a 128-bit message takes about (2 x 12) clocks. Blowfish works with keys up to 448 bits in length.



ign, and decided to modify

(OR Operators.

26 | Page

Figure (3): Blowfish algorithm

A graphical representation of the Blowfish algorithm appears in Figure 3. In this description, a 64-bit plaintext message is first divided into 32 bits. The “left” 32 bits are XORed with the first element of a P-array to create a value I'll call P', run through a transformation function called F, then XORed with the “right” 32 bits of the message to produce a new value I'll call F'. F' then replaces the “left” half of the message and P' replaces the “right” half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit cipher text. [11]

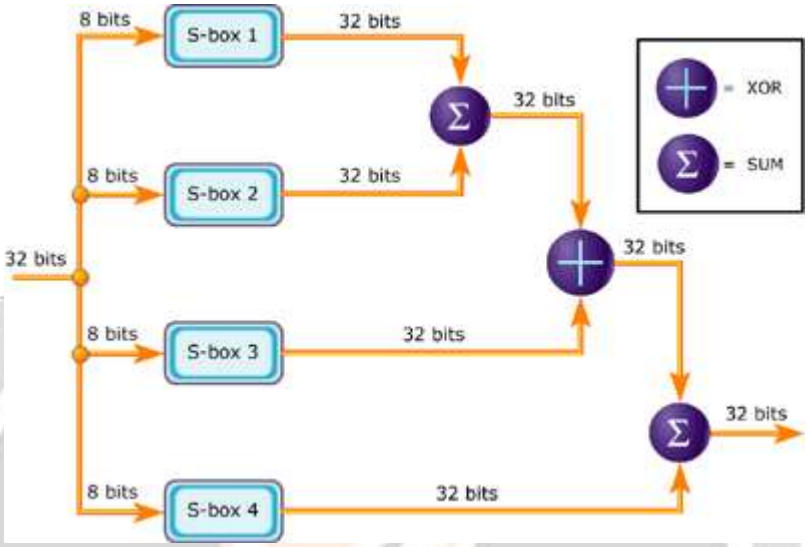


Figure (4): Graphic representation of F

A graphical representation of F appears in Figure 4. The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output.

Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text.

The P-array and S-array values used by Blowfish are pre computed based on the user's key. In effect, the user's key is transformed into the P-array and S-array; the key itself may be discarded after the transformation. The P-array and S-array need not be recomputed (as long as the key doesn't change), but must remain secret.

I'll refer you to the source code for computing the P and S arrays and only briefly summarize the procedure as follows:

- P is an array of eighteen 32-bit integers.
- S is a two-dimensional array of 32-bit integer of dimension 4×256.
- Both arrays are initialized with constants, which happen to be the hexadecimal digits of π (a pretty decent random number source).
- The key is divided up into 32-bit blocks and XORed with the initial elements of the P and S arrays. The results are written back into the array.
- A message of all zeroes is encrypted; the results of the encryption are written back to the P and S arrays. The P and S arrays are now ready for use.

TCP-IP Protocol

Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite. A protocol suit consists of a layered architecture where each layer depicts some functionality which can be carried out by a protocol. Each layer usually has more than one protocol options to carry out the responsibility that the layer adheres to. TCP/IP is normally considered to be a 4 layer system. The 4 layers are as follows: 1. Application layer, 2. Transport layer, 3. Network layer, 4. Data link layer as shown in Figure 5. [13]

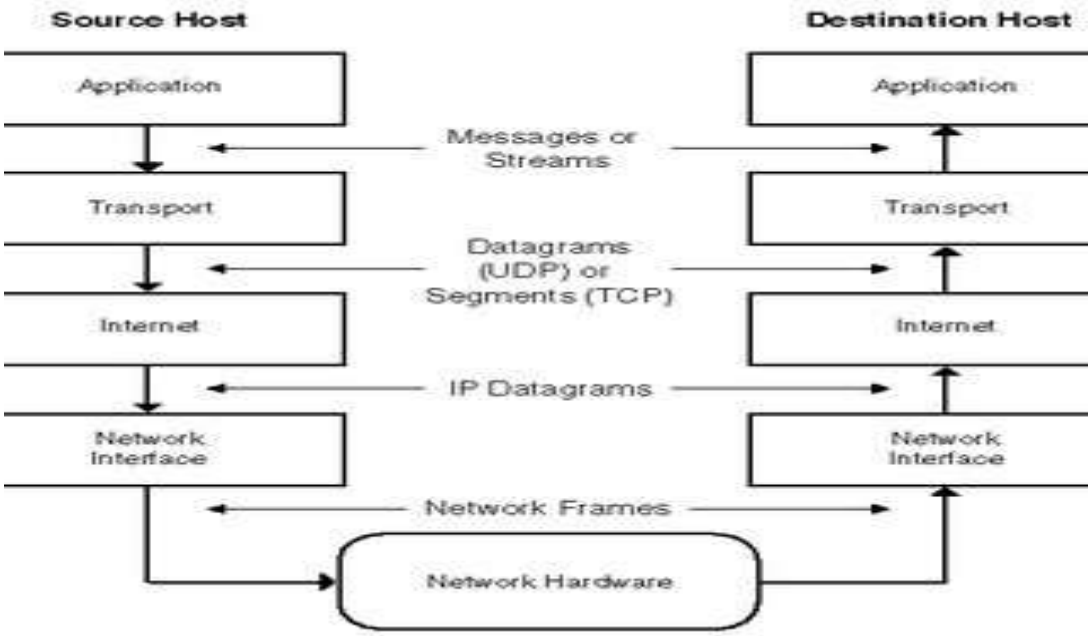


Figure (5): TCP/IP Layers

The Socket

The Internet Transfer Control (ITC) is a handy control for Internet programming, but there is another control that is even more robust and helps programmers to create more flexible applications. The Winsock control comes with Visual Basic 6.0 (VB6) and is used to create applications that access the low-level functions of the Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP/IP is a specification that defines a series of protocols used to standardize how computers exchange information with each other. TCP/IP provides communication across interconnected networks that use diverse hardware architectures and various operating systems. The protocols in TCP/IP are arranged in a series of layers known as a protocol stack. Each layer has its own functionality.

Winsock is a standard that is maintained by Microsoft. This standard is basically a set of routines that describe communications to and from the TCP/IP stack. These routines reside in a dynamic link library (DLL) that runs under Windows. [14]

The Ports

A port is a special memory location that exists when two computers are in communication via TCP/IP. Applications use a port number as an identifier to other computers. Both the sending and receiving computers use this port to exchange data. [15]

Result

Blowfish is the best suitable encryption method based on the result for the paper [16]. The result give indicator that the blowfish main properties are the speed, low memory need and the high security.

i. Figure 6 shows that the blowfish algorithm records the fastest encryption time, and RSA algorithm records the slowest encryption time. Based on the encryption time we will select the blowfish technique for further evaluation.

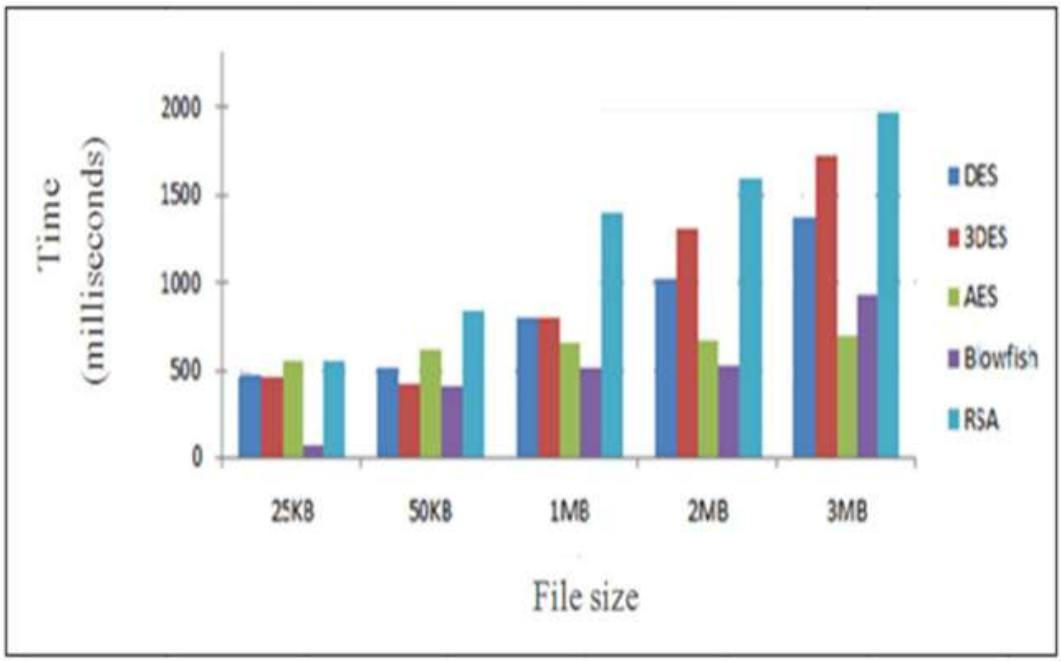


Figure 6: Encryption time vs. File size for DES, 3DES, AES, Blowfish and RSA

ii- Figure 7 shows that the decryption time for all algorithms is faster than the encryption time. Also, blowfish algorithm records the fastest decryption time and RSA algorithm records the slowest decryption time. Based on the decryption time feature we will select the blowfish technique to be considered at the next evaluation level.

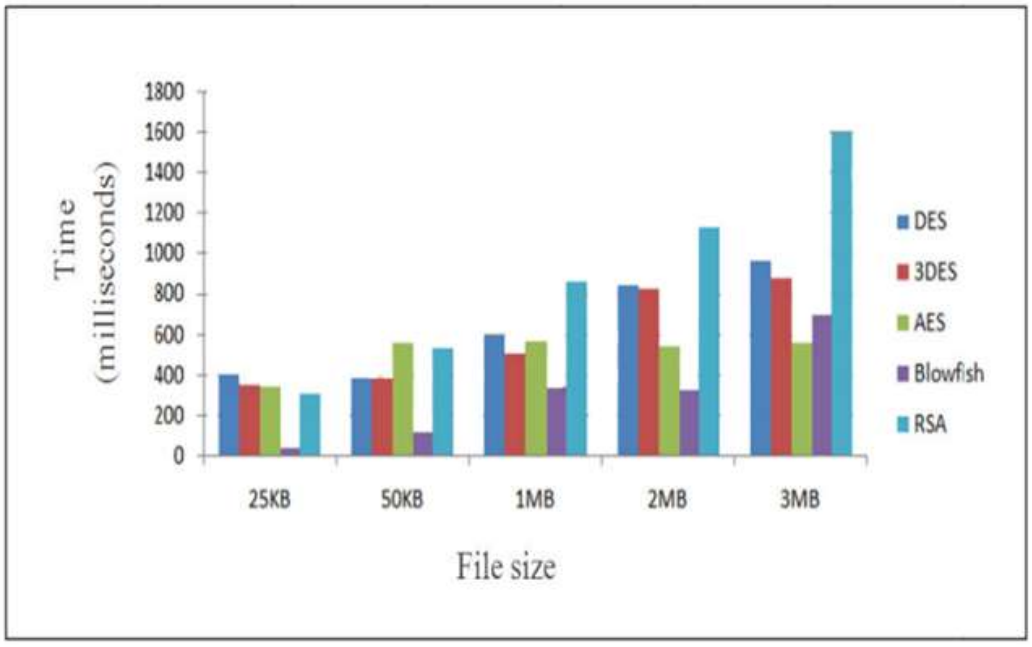


Figure 7: Decryption time vs. File size for DES, 3DES, AES, Blowfish and RSA

iii- Up next in the Table 1 presents that memory used for unit operations for all cryptographic techniques that we studied. Blowfish consumed less memory storage than other types, while RSA uses the highest memory.

Table 1: Comparison of memory used

Algorithm	Memory used (KB)

DES	18.2
3DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

iv- Figure 8 displays that AES manifests the highest avalanche effect, whereas RSA manifests the least avalanche effect. This has turned the attention back to AES for further analysis and improvements.

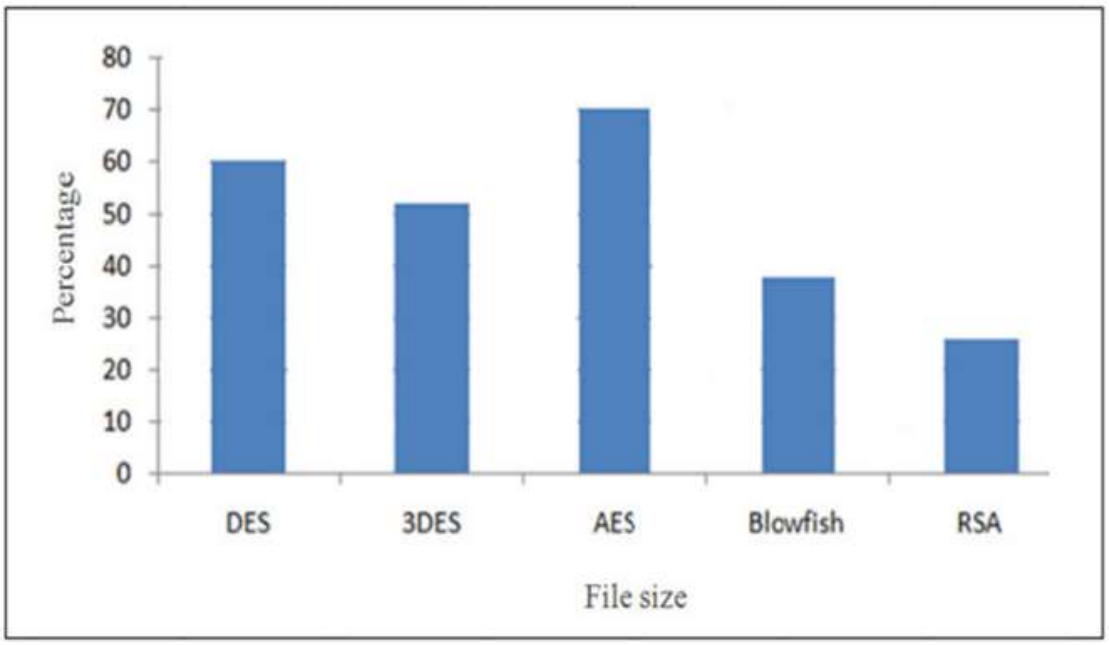


Figure 8: Decryption time vs. File size for DES, 3DES, AES, Blowfish and RSA

v- As the entropy test and final experiment. Table 2 shows that blowfish records the highest average entropy per byte of encryption. That should highlight the blowfish algorithm achievements for consideration of a new security aspect.

Table 2: Average entropy values

Algorithm	**Average entropy per byte of encryption**
DES	2.9477
3DES	2.9477
AES	3.84024
Blowfish	3.93891
RSA	3.0958

vi- Table 3 presents AES demands the highest number of bits to be encoded optimally, whereas DES demands the lowest number of bits to be encoded optimally.

Table 3: Optimal encoding length

Algorithm	Average number of bits demanded to optimally encode a byte of encrypted data
DES	27
3DES	40
AES	256
Blowfish	128
RSA	44

Conclusion

The objective of our paper is to design and build a simple and flexible design for securing TCP protocol. The TCP is not fast as the UDP protocol, so it must be careful when dealing with any extra processing. This lead us to choose secure and fast encryption method. Blowfish is one of the most secure and fast encryption methods. It is block ciphering method which is suitable for the TCP block data. The adopted security method serve many TCP services. Choosing the TCP protocol due to its role in many application it has wide range of important applications.

References

1. The Blowfish Algorithm Simplified, Avinash M Ghorpade1 , Harshavardhan Talwar2, Vol. 5, Issue 4, April 2016.
2. M. Anand Kumar, Dr. S. Karthikeyan, "A New Security Architecture for TCP/IP Protocol Suite", International Journal of Advances Research in Computer Science,Volume1, No. 3, Sept-Oct 2010.
3. Prabhaker Mateti, "Security Issues in the TCP/IP Suite", Department of Computer Science and Engineering, Wright State University, Dayton, Ohio.
4. Mohammad Al-Jarrah, and Abdel-Karim R. Tamimi, "A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement".
5. Dr. M. Anand Kumar, Dr. S, Karthikeyan, "An Enhanced Security for TCP/IP Protocol Suite", International journal of Computer and mobile computing, IGCSMC, Vol. 2, Issue 11, November 2013.
6. Miroslav Sveda, Ondrej Rysavy et al , "Security analysis of TCP/IP Networks".
7. M. ANAnd , Dr S. KrthikeyanKumar, "Security Model for TCP/IP Protocol suite".
8. Ms NehaKhatri – Valmik1, Prof. V. K Kshirsagar2, "In Blowfish algorithm, e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83 www.iosrjournals.org, Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India.
9. Practical Implementation of Blowfish Algorithm for Boosting Security Aspect in Networks, International Journal of Advanced Research in Computer Networking,Wireless and Mobile CommunicationsVolume: 2 Issue: 3 26-Jul-2014,ISSN_NO: 2320-7248.
10. Blowfish encryption algorithm for information security, January 2015.
11. Bill Gatliff, "Encrypting data with the Blowfish algorithm July 15, 2003, Technical article.
12. TCP/IP PROTOCOL LAYERING, January 2015, Available from: https://www.researchgate.net/publication/274639306_TCPIP_PROTOCOL_LAYERING [accessed Aug 30 2020].
13. Behrouz A. Forouzan, "Data Communications and Networking", 4th edition, McGraw Hill International Edition, 2007

14. Fred Halsall, "Computer Networking and the Internet", 5th edition, Person Education Limited,2005
15. Tanenbaum, A. S.; "Computer Network"; 3rd edit; Prentice Hall International Inc; 1996.
16. Mohammed Nazeh Abdul Wahid*, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", Limkokwing University of Creative and Technology, Post Graduate Centre, Cyberjaya, Malaysia.