A Study of New Trends in Blowfish Algorithm

Gurjeevan Singh*, Ashwani Kumar**, K. S. Sandha***

*(Department of ECE, Shaheed Bhagat Singh College of Engg. & Tech.
(Polywing), Ferozepur-152004)
**(Department of ECE, GTBKIET, Chappianwali ,Malout)
***(Department of ECE, Thapar University, Patiala)

Abstract

Wired and wireless networks are becoming popular day by day. Due to rapid growth of networks, information security becomes more important to protect commerce secrecy and privacy. Encryption algorithm plays a crucial role in information security but securing data also consumes a significant amount of resources such as CPU time and battery power. In this paper we try to present a fair comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption. Experiment results of comparison are carried out over different data types like text, image, audio and video. This paper briefly describes a new method to enhance the security of Blowfish algorithm; this can be possible by replacing the pre-defined XOR operation by new operation '#'. When we are adding additional key and replacing old XOR by new operation '#', Blowfish will provides better results against any type of intrusion.

Keywords: **AES, Algorithms, Blowfish, Cryptography, Network security**.

1. Introduction

Networks are admiring day by day in our life. The widespread for using wireless networks makes the need for protection of user data. Encryption algorithm plays an important role for information security. Encryption is the process of transforming plain text data into the cipher text (secure data) in order to reveal its meaning. Decryption is the reverse of the Encryption process in which we retrieve the original plain text from the cipher text. Fig. 1 explains the process of cryptography.

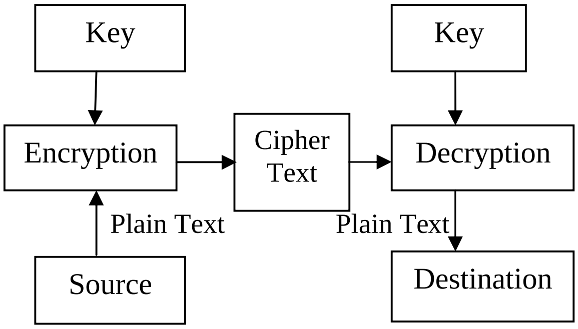


Fig. 1- Process of Cryptography

There are many Encryption algorithms which are developed and are used for information security. They are categorised into mainly two types depending upon the type of security keys. The two categories are symmetric and asymmetric encryptions. In symmetric or private encryption only one key is used to encrypt or decrypt the data. Strength of the symmetric encryption depends upon the size of the key. For the same algorithm, encryption using the longer key is tough to break than one using smaller key. In a symmetric or public encryption two keys are used, one is used to encrypt and other is used to decrypt the data [6]. Brief definitions of the most common encryption techniques are given as follows:

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [1], [6].

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [2], [6].

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [6].

Blowfish is block cipher 64-bit block that can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all users. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish [13]. This paper is organized as follows: Related work has been presented in section 2, performance analysis of different encryption algorithm in section 3, study of Blowfish algorithm in section 4, Study of proposed algorithm to modify Blowfish using 4-states 5 and finally section 6 describes Conclusions and future scope.

2. Related Work

In this section, we have surveyed a number of studies that make comparison in terms of performance analysis between the different encryption algorithms as well as a new proposed model of Blowfish. It was concluded in [8] that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation).

A study in [9] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

Elminaam et al. selected several symmetric encryption algorithms such as AES, DES, 3DES, RC6, Blowfish and RC2 having a performance evaluation in [4]. They concluded: there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding; Blowfish has better performance than other common encryption algorithms used, followed by RC6; In the case of changing data type such as image, RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption; Higher key size leads to clear change in the battery and time consumption.

In [5] the authors compare the various encryption algorithms and simulation results showed that AES has a better performance than other common encryption algorithms used. Since AES has not any known security threat so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. 3DES showed poor performance results compared to other algorithms since it requires more processing power. Since the battery power is one of the major limitations in MANET nodes, the AES encryption algorithm is the best choice.

It was concluded in [10] that adding additional key and replacing the old XOR by a new operation as proposed by this paper to give more robustness to Blowfish algorithm and make it stronger against any kind of intruding. The ciphering process is still simple and can be implemented by hardware in this new proposed improvement, as well as the time complexity of the new algorithm stays the same since only one operation is replaced by another operation, and the conversion operations is very simple and straightforward.

3. Performance Analysis of Different Encryption Algorithm

Throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [13] and the encryption time is considered as the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is also used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. In the study, the software encrypts a different file formats like text, image audio and video files with file size ranges from 4000 KB to 11 Mega Byte. The performance metrics like encryption time, decryption time and throughput have been collected for each file type [5].

3.1 Comparison of Throughput:

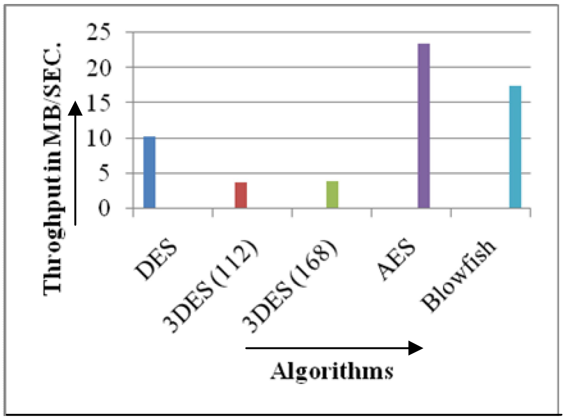
The Table 1 shows the throughput of various encryption algorithms for text, image, audio, and video files.

TABLE 1- Throughput in MB/SEC.

Throughput	Text	Image	Audio	Video
DES	10.616	9.326	10.01	11.16
3DES (112 bit key)	3.875	3.635	3.883	3.909
3DES (168 bit key)	3.885	3.802	3.872	3.953
AES	23.503	20.504	22.099	27.447
Blowfish	17.64	15.328	17.094	19.602

(Source: [5])

The following figure 2 shows the average throughput of encryption algorithms by considering all the file formats.



(Source: [5])

Fig.2- Average Throughput of Encryption Algorithms

From the results it is easy to observe that AES has an advantage over other algorithms in terms of encryption time, decryption time and throughput. Also it showed that Blowfish has a better performance than 3DES and DES. And it is clear that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [5].

4. Study of Blowfish Algorithm

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm [7]. Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at the most 448 bits into several sub key arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent Permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. The

Figure 3 shows the action of Blowfish as it has Blowfish has 16 rounds.

The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16:

xL = xL XOR Pi xR = F(xL) XOR xR

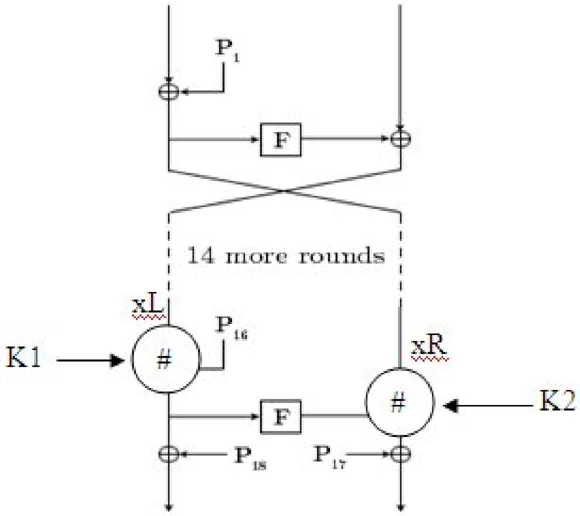
Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL and xR to get the cipher text [7, 11].

F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the cipher text block, then using the P-entries in reverse order.

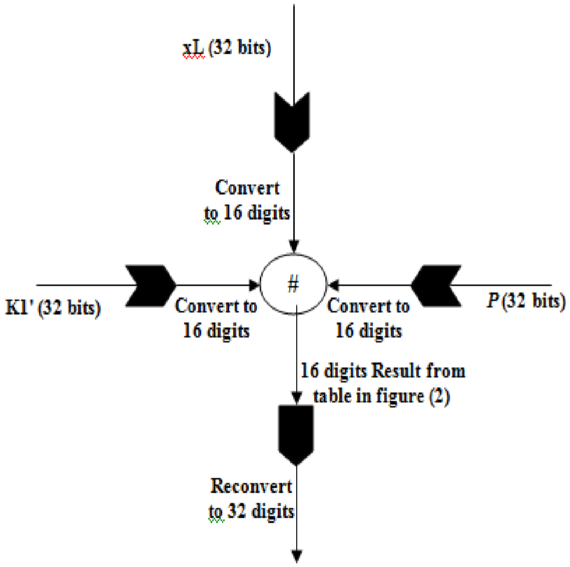


(Source: [10])

Fig. 3- Blowfish Each Round Action

5. Study of proposed algorithm to modify Blowfish using 4-states

This research proposed a new improvement to the Blowfish algorithm. The proposed improvement makes use of the new operation defined in the previous section, operation '#' applied during each round in the original Blowfish algorithm, where another key is needed to apply this operation at both sides, this key may come in binary form and convert to a 4-states key, or it may already come in a 4-states as that can be done with quantum channel. Consequently, two keys will be used in each round of the original Blowfish, the first key K1will be used with the xL and Pi to produce the next left part. The second key K2 will be used with F (xL) and xR to produce the right part. These three inputs to the '#' operation should be firstly converted from 32 bits to a 16 digits each may be one of four states (0, 1, 2, 3), i.e., each two bits converted to its equivalent decimal digits; see figure 4.



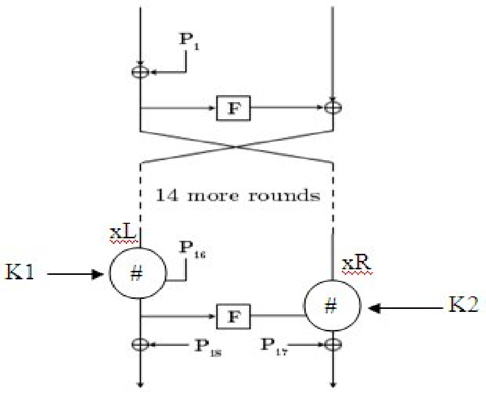
(Source: [10])

Fig.4- Inputs and Outputs of the # operation in DES Algorithm

For example, the binary number:

1001011101010010101001111010001001 will be converted to the number:

2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1



(Source: [10])

Fig. 5 New Structure of Each Round

Then the '#' operation will be applied to generate a new 16 digits that should be reconverted to 32 bits, see Figure 5. Full details of the proposed improved Blowfish are given in Algorithm [12].

6. Conclusions and Future Scope

The simulation results show that AES has a better performance than other common algorithms. AES is supposed to be better algorithm which was compared to original Blowfish Algorithm. But adding additional key and replacing the old XOR by new operation '#' as a purposed by this study to give more robustness to Blowfish Algorithm and make it stronger against any type of intrusion. This advance Blowfish Algorithm is more efficient in energy consumption and security to reduce the consumption of battery power device. In the new proposed model of Blowfish by further increasing the key length, Blowfish will provide the better results.

References

[1] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."*Dr. Dobb's Journal, March 2001, PP. 137-139.*

[2] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."*IBM Journal of Research and Development, May 1994, pp. 243 -250.*

[3] Diaa Salama Abdul. Elminaam, Hatem Abdul Kader and Mohie Mohamed Hadhoud, Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types, *International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010.*

[4] Diaa Salama Abdul Elminaam, Hatem Abdul Kader and Mohie Mohamed Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms, *International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.*

[5] M.Umaparvathi, Dr.Dharmishtan K Varughese, Evaluation of Symmetric Encryption Algorithms for MANETs, *IEEE, 2010.*

[6] W.Stallings, *"Cryptography and Network Security* 4th Ed," Prentice Hall, 2005, PP. 58-309.

[7] B. Schneier, "*Applied Cryptography*", John Wiley & Sons, New York, 1994.

[8] S. Hirani, *Energy Consumption of Encryption Schemes in Wireless Devices Thesis*, University of Pittsburgh, Apr. 9, 2003, Retrieved October 1, 2008.

[9] A. Nadeem and M. Y. Javed, A performance comparison of data encryption algorithms," Information and Communication Technologies, *ICICT 2005, pp.84-89, 2005.*

[10] Afaf M. Ali Al-Neaimi, Rehab F. Hassan, New Approach for Modifying Blowfish Algorithm Using 4-States keys, *The 5th International Conference on Information Technology, 2011.*

[11] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption", *Cambridge Security Workshop Proceedings (December 1993) Springer-Verlag, 1994, pp.191- 204.*

[12] Hala Bahjat AbdulWahab1 , Abdul Monem S. Rahma, 'Proposed New Quantum Cryptography

System Using Quantum Description techniques for Generated Curves", *The 2009 International conference on security and management, SAM2009, July 13-16 2009, Las Vegas, USA, SAM 2009.*

[13] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008. http://www.schneier.com/blowfish.html.