Interbit Exchange and Merge (IBEM) Pattern of Blowfish Algorithm

S. Sweetlin Susilabai, D.S. Mahendran, S. John Peter

Abstract: ***Nowadays security plays important role whenever there is communication between sender and receiver. To triumph over the issues of security intruders, various cryptographic algorithms are used. In this paper, authors have attempted to improve the security level of blowfish with proposed Inter bit exchange and merge (IBEM) pattern of data before applied which is fed into S-Boxes. Inter bit Exchange and Merge (IBEM) pattern of data allows the intruders cannot easily find key mechanism what the user actually send. The results of all the tests conducted which leads to a common conclusion that the security of the Inter bit Exchange and Merge process provides data in great secure manner when compared to original blowfish algorithm.***

Keywords: AES, DES, Blowfish, Cryptography.

I. INTRODUCTION

Cryptography [1] is most likely the most vital aspect of communications security and is becoming increasingly significant as a basic building block for computer security. It is the science that is broadly used for network security. Cryptography means to transfer vast data across insecure networks such as internet. Key aspects of cryptography square measure confidentiality, integrity, authentication, and non repudiation. An plain text is known as the original text, while the encoded message is called the cipher text. The process of converting from plain text to cipher text is called encryption; restoring the original text from the cipher text is decryption.

There are two types of cryptographic methods are available on the basis of key.

a) Symmetric key Cryptography: For enciphering message and deciphering the message it uses single common key. Symmetric key cryptography is also divided into two types on the source of their Operations:
   1. Stream Cipher: It encrypts a digital data stream one bit or one byte at a time.
   2. Block Cipher: It is one in which a block of plaintext is treated as a whole and used to construct a cipher text block of same length.

b) Asymmetric or Public Key Cryptography: In this type of cryptographic method uses two keys for enciphering message and deciphering the message called Public key and Private Keys.

II. RELATED WORK

Monika Agarwal, Pradeep Mishra [4] proposed a new approach to every time a new random number obtained and this as a result gives difference in the application of F function over each round. They have proposed and implemented a new approach to further improve the existing algorithm to achieve better results in terms of parameters such as Encryption time, Decryption time and Throughput. They used modified blowfish encryption algorithm, cipher text is produced for the same input it will intensely improved the security aspect of blowfish algorithm and provide less time consuming as compared to blowfish algorithm. They concluded that results clearly specify that the encryption time and decryption time for modified blowfish algorithm is almost half to that of blowfish algorithm.

Christina L , Joe Irudayaraj V S [6] altered S-boxes in the F-function. They modified the structure of F-function. They customized original Blowfish algorithm F-function with four S-boxes into the optimized Blowfish F-function with two S-boxes. They suggested that to optimized Blowfish algorithm reducing of two S-boxes will increase the speed and endow with the great security to data. They decreased that the execution time is to 0.2 milliseconds and the throughput is increased to 0.24bytes/milliseconds compare than original algorithms.

Vaibhav Poonia ,Dr. Narendra Singh Yadav [8] the authors calculated the performance of modified Blowfish algorithm in four different cases with different parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File. In all those cases they established that they have improved the Original Blowfish algorithm to some extents. The results of all cases and the tests conducted above and they concluded that the security of the modified algorithm with different cases makes the original Blowfish algorithm more compact and more secured than the earlier.

Saikumar Manku, K. Vasanth [7] introduced a proposed Blowfish algorithm reduce rounds of algorithm and proposed single blowfish round. In this proposed system each single round is introduced new modified. They designed the algorithm like two s-boxes linking with XOR as like some other two 2 s-boxes linked with XOR and then from the two XOR added then from there get key plain text.

Manuscript received January 25, 2019.

S. Sweetlin Susilabai, Research Scholar, Manonmaniam Sundaranar University, Tirunelveli. Tamilnadu, India

Dr.D.S. Mahendran, The Principal, Aditanar College of Arts & Science, Tiuchendur, Tamilnadu, India

Dr.S. John Peter, Associate Professor & Head, Department of Computer Science, St.Xaviers College, Tirunelveli, Tamilnadu, India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

They concluded that the modified algorithm makes great security thus no one attacks in between sender and receiver will hack the data.

B.Geethavani, E.V.Prasad and R.Roopa [5] proposed a new approach for hiding text in audio files such that original data can reach the receiver side in a safe manner without being modified anything. They sent well secured data, transfer in audio signals using discrete wavelet transform. They suggested new hybrid technique from the combination of cryptography and Steganography for tranferring the message in a highly secured manner. The original message is encrypted mistreatment Blowfish formula and also the resulted cipher message is surrounded into associate audio file mistreatment separate wave remodel. Finally they concluded that this method is well-organized method for hiding text in audio files such that data can reach the receiver side in a safe and secured manner without any modification

III. METHODOLOGY

A. Blowfish Algorithm

Blowfish[2] is a symmetric block cipher algorithm designed by Brute Schneier in December 1993. Blowfish is a alternate of DES or IDEA. One of the most admired feistel network ciphers is Blowfish. Blowfish algorithm has 64-bit block size and variable key length from 42 bits to 448 bits. .

The algorithm consists of a key-expansion part ,data-encryption part.

Blowfish develop the key of at most 448 bits into many sub key arrays the total is 1042 32 bit values or 4168 bytes. It is a 16- round feistel system, which provides very big key-dependent S-boxes and allows 16 iterations. Every round is prepared with a key and data dependent substitution and a key-dependent permutation. The 32-bit words and XOR operations are performed by additions. There is a P-array and four 32-bit S-boxes. The P-array contains 18 of 32-bit sub keys, while each S-box contains 256 entries. The input is a 64 bit data element.

The process of Sub key generation is illustrated as follows

i. First Initialize the P array and the four S boxes
ii. P Array and the four S boxes is denoted as hexadecimal digits of Pi.
iii. Perform a bitwise XOR operations of P-array and with the K array reusing words from the K array needed with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key)…
iv. Encrypt the 64 bit block.Use the above encryption process to encrypt the all-zeros with the current P and S arrays.
v. Take the place of p1 and p2 with output of encryption. Now new output is named as p1 and p2.
vi. Encrypt the output of step3 using current P box and S box and exchange p3 and p4 with resulting encrypted text. Now new output is named as p3 and p4.
vii. Repeat the above steps until we obtain all the elements of P array i.e P1, P2…. Feistel Structure as shown in fig 3.1.1

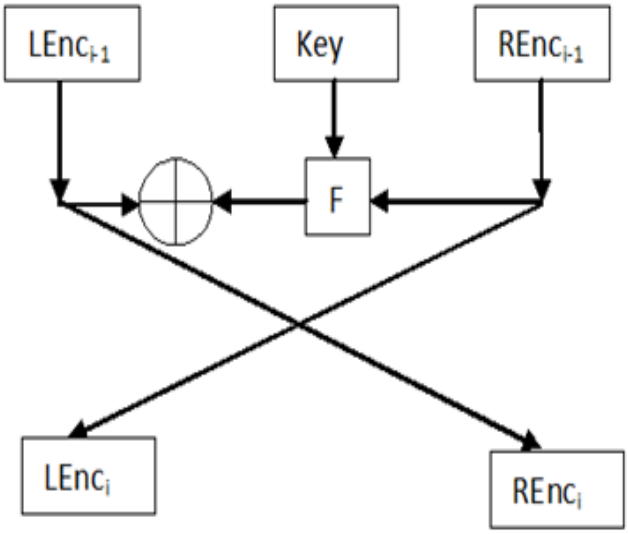


Fig. 3.1.1: Feistel structure

The encryption process for Blowfish of every round is carry out in the following steps:

1) Divide each block into 2 halves
2) Right half is swapped with left half
3) The right half is complete when XOR is finished on the left half and the result we acquire after applying 'f' to the right half and the key.
4) The rounds which are earlier can be attained even if the function 'f' is not spined upside down.

Blowfish encryption Algorithm :-

1. The original text(X) is splited into two 32-bit halves: $LEnc_0$, $REnct_0$.Let us take the variables $LEnc_i$ and $REnc_i$ to submit to the left and right half of the data after round I has finished.

2. For j = 1 to 16

$REncj = LEnc_{j-1} \oplus Pj$

$LEnc_j = F(REncj) \oplus REncj - 1$

exchange REnci and $LEnc_i$

3. Exchange $LEnc_j$ and REncj (Undo the last exchange)

4. $REncj = REncj \oplus P17$

5. $LEncj = LEnc_j \oplus P18$

6. combine $LEnc_j$ and REncj

The final resulting encrypted text has LEnc17 and REnc17.

The Blowfish algorithm and its functional as follows.

First split LEnc (32 Bits) into four 8-bit sectors: a1, b1, c1, and d1. Then apply the following formula.

F (LEnc) = {(Sbox1 [a1] + Sbox2 [b1]) Sbox3 [c1]} + Sbox4 [d1])}

Where + means addition modulo 2^32, and means exclusive OR and Sbox1, Sbox2, Sbox3, Sbox4 are four substitution boxes.

The following figure shows S-Box operations of Blowfish Algorithm

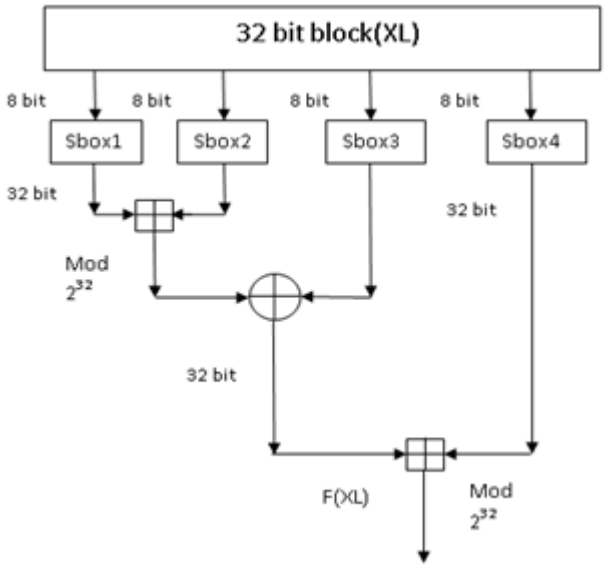


Fig. 3.1.2: S-Box operations of blowfish algorithm

B. Proposed Inter Bit Exchange and Merge (IBEM) :-

The original text can be split into 64 bits into two 32 bit halves XL and XR. This XL as well as XR are further divided into B1, B2, B3 and B4 sub patterns (8 bits).

Let us considered Bi and Bj are two sub bit patterns. The proposed Inter bit Exchange and Merge pattern IBEMij is constructed as follows:

1) Take the odd number of bits from Bi and even number of bits from Bj.

2) Exchange these bits in same order and merge them to form IBEMij.

3) These *IBEMij is fed into SBOX operations instead of original 8 bit.*

The proposed Inter bit Exchange and Merge (IBEM) pattern of data Blowfish algorithm and is applied as follows.

S1 ⟵ IBEMij (where i=1,j=3)
S2 ⟵ IBEMij (where i=2,j=4)
S3 ⟵ IBEMij (where i=3,j=2)
S4 ⟵ IBEMij (where i=4,j=1)

The following figure shows S-Box operations of Proposed Inter Bit Exchange and Merge pattern Blowfish encryption algorithm.

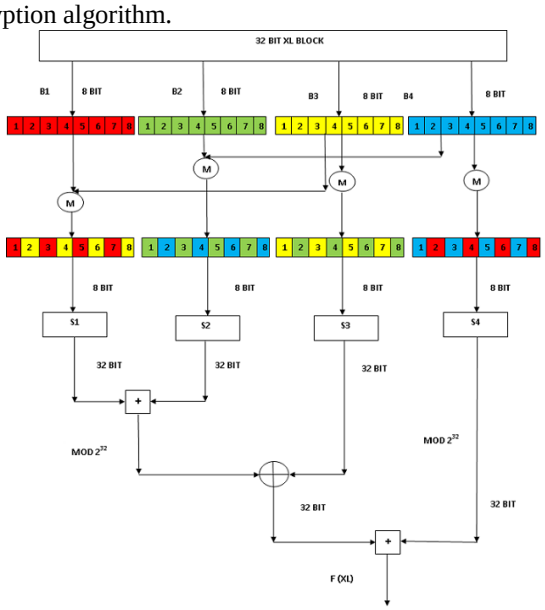


Fig.3.1.3: Inter Bit Exchange and Merge(IBEM)

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

A comparative parameters of AES, DES, original blowfish and IBEM are analyzed based on execution time throughput and encrypted file size. The performance criteria of results have been analyzed different input file size (kb).

These algorithms are implemented in java 1.8 and eclipse (4.7.0) integrated environment. Performance was measured on a Intel(R) Core(M) i7-855 0U CPU @ 1.80 GHz processor with 8GB RAM.

1. Execution Time
2. Through put
3. Encryption time

A. Performance comparison on the basis Execution Time

The comparison is performed using the text or message only. Encryption time is one of the performance parameter, which is calculated by using the amount of time required for converting original text into cipher text at the time of encryption. Decryption time is one of the performance parameter, which is calculated by using the amount of time required for converting cipher text into original text at the time of encryption. To improve the accuracy of the timing measurement, the program is executed in number of times. The encryption time and also decryption time is measured by using milliseconds. The summation of encryption time and decryption time is calculated as the execution time.

Execution time=Encryption time + Decryption Time.

The results of execution time for AES, DES, Blowfish and proposed IbEM algorithms with different input file sizes (kb) are shown in table 4.1

Table 4.1

Filesize(Kb)	AES	DES	Blowfish	IBEM
49.16	320	301	15	26
99.814	338	303	47	61
149.975	348	313	51	76

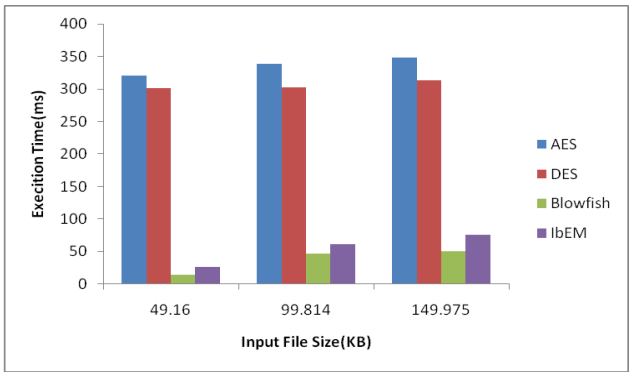


Fig 4.1: Performance comparison on the basis Execution Time

Comparison of total execution time for AES, DES, Blowfish and proposed IBEM by taking different input file sizes (kb) are shown figure 4.1 below

B. Performance comparison on the basis Throughput

The throughput of the execution scheme is evaluated as the total encrypted plaintext size in bytes divided by the total execution time. Throughput indicates the speed of encryption. The throughput of the execution scheme is calculated using the following formula.

Throughput =Total size of plaintext/ Total execution time. Where plaintext size is measuring in kilo bytes and total execution time is measuring in milliseconds taking different input file sizes.The results of throughput for AES, DES, Blowfish and proposed IbEM algorithms with different input file sizes (kb) are shown in table 4.2.

Table 4.2

Filesize(Kb)	AES	DES	Blowfish	IBEM
49.16	157	167	13426	7564
99.814	302	339	8699	6546
149.975	441	490	12045	7894

Comparison of throughput for AES, DES, Blowfish and proposed IBEM with different input file sizes (kb) are shown in Figure 4.2

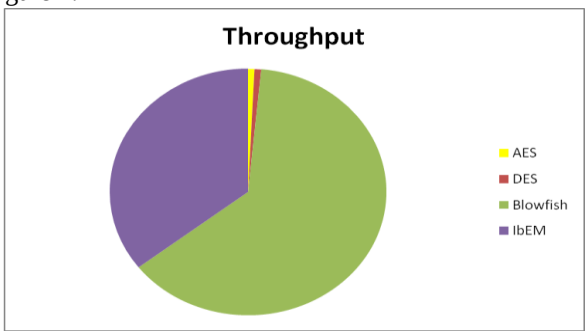


Fig 4.2: Performance comparison on the basis Throughput

The throughput of the execution scheme is calculated as the total encrypted plaintext size in bytes divided by the total execution time. Throughput indicates the speed of encryption. The above graph shows the result based on the throughput of the execution time with different input size. It shows that the throughput is less for IBEM when compared to original Blowfish algorithms.

C. Performance comparison the basis Encryption Time

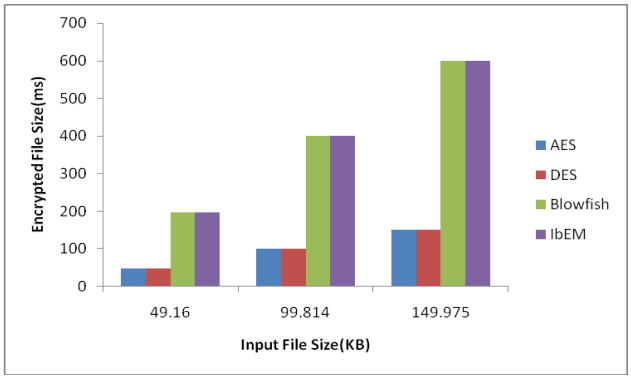
Encryption Time is one of a performance parameter which is calculated as the amount of time required for converting Original text message into cipher text at the time of encryption.

The results of encryption time for AES, DES, Blowfish and proposed IbEM algorithms with different input file sizes (kb) are shown in table 4.3.

Table 4.3

File size (Kb)	AES	DES	Blowfish	IBEM
49.16	49.172	49.172	196.672	196.672
99.814	99.828	99.828	399.281	399.281
149.975	149.984	149.984	599.921	599.922

Comparison of encryption time for AES, DES, Blowfish and proposed IBEM with different input file sizes (kb) are shown in Figure 4.3.



It is clear from the graph that the amount of encryption time taken by IBEM is almost equal as compared to that of original Blowfish algorithm for the same input.

V. CONCLUSION

The main objective of this paper is to evaluate the security of InterBit Exchange and Merge (IbEM) with proposed blowfish algorithm with changing of Inter bits between S-Box operations. We have attempted to improve the security level of blowfish with proposed Inter Bit exchange and merge (IBEM) pattern of data before applied which is fed into S-Boxes. The results of all the tests conducted which leads to a common conclusion that the security level of the Inter Bit Exchange and Merge process makes the original Blowfish algorithm more compact and more secure than the earlier. Here one more thing we want to conclude that the intruder could not able break up an is most secured than others cannot easily find key mechanism what the user actually send as suggested cannot easily find key mechanism as suggested is most secured than original blowfish. Even though the computation time of the proposed IBEM algorithm is little bit more than blowfish it is negligible one compared to the security we attained.

REFERENCES

1. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2nd edition, 2008.
2. William stalling,” Cryptography and network security”, 3rd ed.
3. Manikandan G, Rajendran P, Chakarapani K, Krishnan G and Sundarganesh G "A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Applied Information Technology, Vol. 35, No.2, pp.149-154, 2012.
4. Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology, Vol. 1, Issue 6, pp. 79-83, 2012.
5. B.Geethavani, E.V.Prasad and R.Roopa , “A New Approach for Secure Data Transfer in Audio Signals Using DWT”, 2013, IEEE.
6. Christina L , Joe Irudayaraj V S, “Optimized Blowfish Encryption Technique”, International Journal of Innovative Research in Computer and Communication Engineering,Vol. 2, Issue 7, July 2014.
7. Saikumar Manku and K. Vasanth “Blowfish encryption algorithm for information security”, ARPN journal of engineering, vol 10, June 2015
8. Vaibhav Poonia ,Dr. Narendra Singh Yadav, “Analysis of modified Blowfish Algorithm in different cases with various parameters”, International Conference on Advanced Computing and Communication Systems (ICACCS -2015), Jan. 05 – 07, 2015.