Journal of Theoretical and Applied Information Technology
31st January 2012. Vol. 35 No.2

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

A MODIFIED CRYPTO SCHEME FOR ENHANCING DATA SECURITY

[1]MANIKANDAN.G, [2]RAJENDIRAN.P, [3]CHAKARAPANI.K,[4]KRISHNAN.G,[5]SUNDARGANESH.G

[1,2]Assistant Professor, School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India.
[3]SeniorAssistantProfessor, School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India.
[4,5]Student, School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India.

E-mail: [1]manikandan@it.sastra.edu, [2]rajendranap@it.sastra.edu, [3]kcp@core.sastra.edu, [4]gkrishnan@ict.sastra.edu, [5]sundarganesh2012@gmail.com

ABSTRACT

On considering the current scenario, Most of the existing systems which offer security to a network or web or to a data are vulnerable to attacks and they are breached at some point of time by effective cryptanalysis, irrespective of its complex algorithmic design. In general, today's crypto world is restricted to a practice of following any one single encryption scheme and that too for a single iteration on a single file basis. This is evident in the 99% of the encryption-decryption cases. So, A need for "practically strong and infeasible to get attacked" technique becomes vital. In this paper, we propose a Software tool which involves Cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. We used modified Blowfish algorithm for Encryption and Decryption of data. Though we use only one algorithm, we differentiate the cryptographic scheme by varying the key for varying file slices. Our results clearly justifies that our tool serves as a better solution both in terms of performance as well as security.

Keywords: *Cryptography, File Slicing, Modified Blowfish Algorithm, Security*

1. INTRODUCTION

Cryptography is a well known and widely used technique which deals with protecting the information by encoding or transformation of data into an unreadable format [1]. The original text is converted into a scramble equivalent text called cipher text and this process is called as "Encryption" and the reverse is called "Decryption".

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

- *Symmetric key Cryptography*: The cryptographic scheme which uses a single common key for enciphering and deciphering the message.
- *Asymmetric or Public Key Cryptography*: This type of cryptographic scheme uses two keys for encryption and decryption called Public key and Private Keys.

We can also classify symmetric key cryptography into two types on the basis of their operations as

- *Stream Ciphers*: It is a symmetric key cipher where stream of plaintext are mixed with a random cipher bit stream (key stream), typically by any logical operation. In this case of stream cipher one byte is usually encrypted at a particular time.
- *Block Ciphers:* It is also known as symmetric key cipher which operates over a fixed-length group of bits. It usually takes particular bit block of plaintext as input, and produces a corresponding n-bit output block of cipher text.

For our research work, we adopted modified - blowfish algorithm one of our research works which falls under symmetric block cipher category [2].

2. EXISTING SYSTEM

Blowfish, a symmetric block cipher uses a Feistel network, 16 rounds of iterative encryption and decryption functional design. The block size of blowfish algorithm is 64 bits, and the key size may be of any length but having a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

limit up to 448 bits. The power of the Blowfish algorithm relies on its sub-key generation and its encryption.

Blowfish cipher uses 18 each of 32-bit sun arrays commonly known as P-boxes and four Substitution boxes each of 32 bit size and having 256 entries each. It uses a Feistel cipher which is a general method of transforming a function into another function by using the concept of permutation. The working of blowfish cipher can be illustrated as follows,

It splits the 64 bit block into two equal blocks having 32 bit size each. Lest block is XORed with first sub array P1 and thus obtained result is fed in to a function called F-function. Inside the F-function substitution operations are carried out which in turn converts 32 bit blocks in to another 32 bit blocks. Thus resulted 32bit entries are XORed with the Right half and the result obtained is swapped as the left half for the next round. So, After the successful completion of each round Right half becomes the new left half or vice versa and Fiestal structure is followed up to 16 rounds. The resultant left and right halves are not swapped but XORed with the seventeenth and eighteenth P-arrays. The Fiestal Structure of blowfish algorithm is shown in the Fig-2

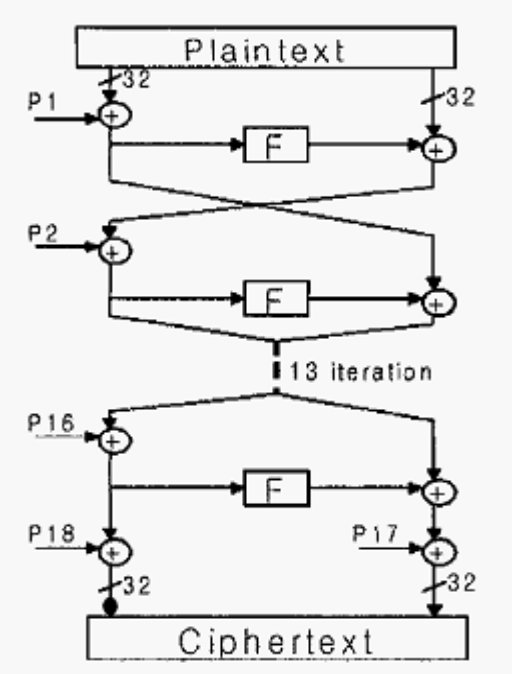

Fig 1: Fiestal structure of Blowfish Cipher

3. PROPOSED SYSTEM

This Software tool involves Cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. In this approach a file which has secret data is sliced into desired number of pieces upon user's specification and then the cryptographic encryption phase is carried out. In order to achieve more security we can adopt more than one cryptographic scheme which definitely ensures nil suspicion and more security. In this paper, we differentiate the cryptographic scheme by providing different key for each encryption of sliced files; provided the key should be given correctly at the time of decryption to avoid erroneous results. We are using modified Blowfish algorithm for Encryption and Decryption of data which serves as a better solution both in terms of performance and as well as security. This enhancement in security and performance is sustainably justified in our previous work [2].

In the file joining phase, En-Ciphered files thus obtained from the different En-Ciphering techniques are merged and hence transmitted to reception side as a single file which makes the file infeasible to breach and suspicion less to get to know that varying crypto schemes are adopted. And hence the data security is maximized. At the receiver's end, We once again splits the files and decrypts it using the same algorithm and then joins all split files together to retrieve the original message.

When coming to cryptographic perspective, in order to enhance the performance of the Blowfish Algorithm it is proposed to modify the F-Function by adopting the concept of multithreading.

The Block diagram of the proposed approach is shown in Fig.2 on next page.

Journal of Theoretical and Applied Information Technology
31st January 2012. Vol. 35 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

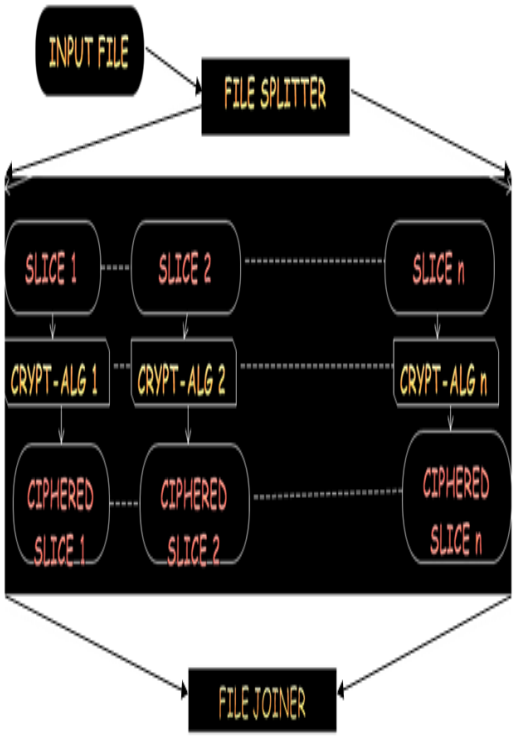

Fig 2: Pictorial Representation of File Splitter-Joiner

3.1 Modified F-Function:

Function F plays an important role in the algorithm, and we decided to modify function F. Original function F is defined as follows. [3]

$F(X) = ((S_1 + S_2 \bmod 2^{32}) \text{ XOR } S_3) + S_4 \bmod 2^{32}$

Instead, we modified the F-Function by replacing 2 addition operations as XOR Operations . Thus the modified F-Function is written as,

$F(X) = ((S1 \text{ XOR } S2 \bmod 2^{32}) + (S3 \text{ XOR } S4 \bmod 2^{32}))$

This modification leads to the simultaneous execution of two XOR operations. In the case of original F-function which executes in sequential order and it requires 32 Addition operations and 16 XOR operations. But in the case of our modified F-function it requires the same 48 gate operations (32-XOR,16-addition) but time taken to execute these 48 operations will be reduced because of multithreading [2]. We executed 32 XOR operations in parallel order using threads and hence time taken to complete 16 gate operations will be equal to the time taken to complete 32 XOR operations since we are running it in parallel environment [4]

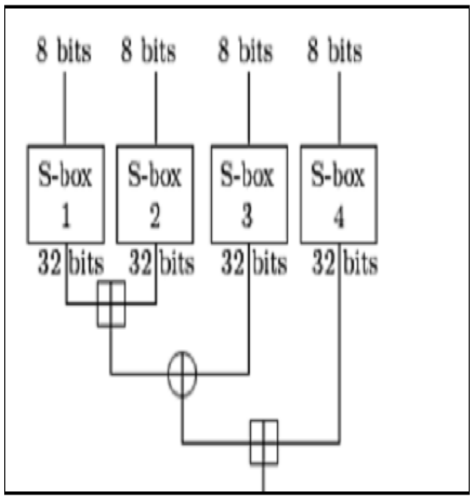

Fig 3: Existing F-Function

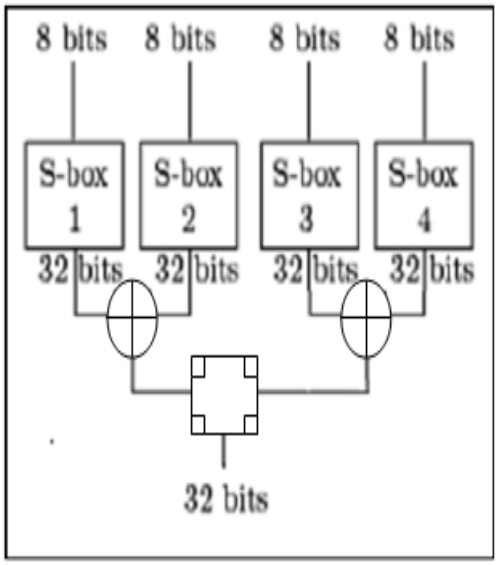

Fig 4: Modified F-Function

4. SIMULATION & RESULTS

For the purpose of simulating the File splitting and file merging and for modified blowfish algorithm we used Java which is well known for its platform independency and better GUI features. We developed, tested and executed using JDK 1.6 in core 2 duo processor. We adopted JCreator1.6 for IDE purposes.

Journal of Theoretical and Applied Information Technology
31st January 2012. Vol. 35 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 5: File Splitter GUI

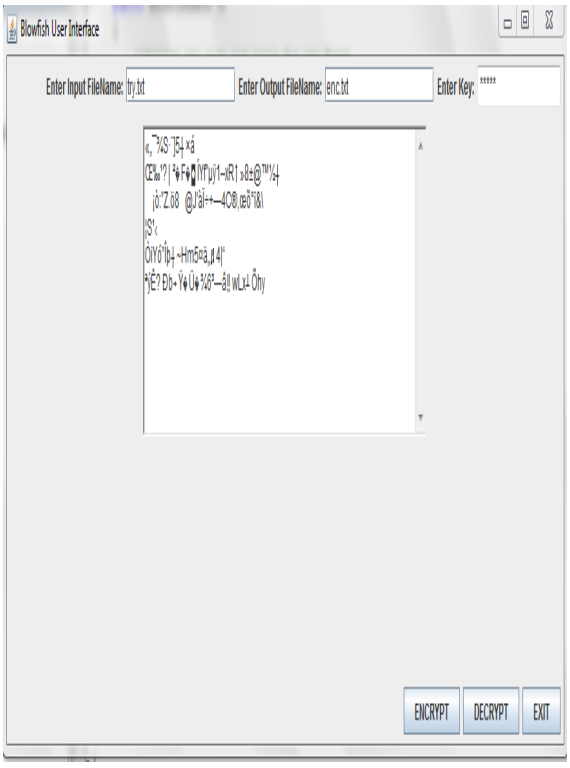

Fig 7: Blowfish Encryption

Fig 6: File Joiner GUI:

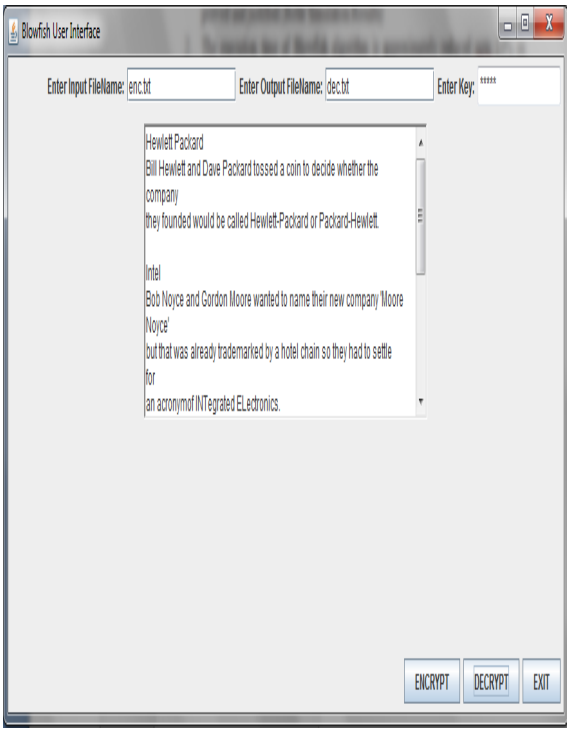

Fig 8: Blowfish Decryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: A Table of Comparison of Execution time consumed:

Time Vs Algorithm	Start Time (ms)	End Time (ms)	Elapsed Time (ms)
Original Blowfish Algorithm	1289281669804	1289281670225	499
Modified blowfish algorithm	1289282873275	1289282873706	431

Thus it is experimentally proved that the execution time of modified blowfish algorithm is 13.5% lesser than the original algorithm.

5. SIGNIFICANT FEATURES

This proposal has several merits to be appreciated.

First, on considering the File splitting and merging modules,

1. Its simpler design & easy in implementing it.
2. The Design and working is fashioned in such a way that, it is infeasible to breach.
3. It also leaves no Suspicion about Splitting & Merging of files.
4. Thus our ultimate aim of providing a tool kit which offers "strong and infeasible to get attacked" is achieved.
5. This software tool is modular, so any encryption algorithm can fit well in the place of our modified Blowfish algorithm.
6.

Next, On considering the Encryption & Decryption Phase,

1. The execution time of Blowfish algorithm is approximately reduced up to 13.5% on comparing with the original Blowfish Algorithm.
2. Although, we used 2-XOR gates and 1-ADDER but the original F-function uses 2-ADDERs and 1-XOR gate and there is no abrupt change in the execution time or clock cycles required for execution. This is because all fundamental logical operations like AND,OR,XOR takes more or less equal time when running under any programming languages since those languages are logically driven.
3. It's quite hard for the eavesdroppers to realize that the F-function is modified and hence probability of attack is less on comparing with the original Blowfish algorithm.
4. Since our proposed system bring modifications only to the order of execution and no changes is made to the actual functionalities (i.e., we didn't added or removed new operations rather we changed only the order of execution of existing Xor and Adders) so performing cryptanalysis is not necessary.

6. CONCLUSION

This paper will satisfy our foremost aim of providing a system which is "infeasible to get breached". It also provides a high end data security when transmitting over any insecure medium. Intruders will not have any idea about our modification both in terms of algorithm as well as in our design, so breaching this system is highly impossible. We are sure that this software tool is unique of its kind and it can also be tuned in terms of higher performance and security in near future by adding or replacing cryptographic part because of its modularity in design. That is, it has a good performance without compromising the security and the modified F-function also enhances the performance by reducing the clock cycles upto 33% and reduces the execution time upto 14% [2].

REFERENCES:

[1]. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, 1995.

[2]. Manikandan Ganesan, Krishnan Ganesan, "A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm", *International journal of Advanced Research in Computer Science, 2011*.

[3]. Kishnamurthy G.N, Dr.V.Ramaswamy and Mrs.Leela.G.H ,"Performance Enhancement of Blowfish algorithm by modifying its function" Proceedings of International Conference on Computers, Information, System Sciences and Engineering 2006, University of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Bridgeport, Bridgeport, CT, USA. pp. 240-244.

[4]. William Stallings, Cryptography and Network Security, 3rd Ed, Wiley, 1995.

[5]. 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.*

[6]. Dr.V.Ramaswamy, Kishnamurthy.G.N, Mrs. Leela.G.H, Ashalatha M.E, "Performance enhancement of CAST –128 Algorithm by modifying its function" *Proceedings of International Conference on Computers, Information, System Sciences and Engineering 2007*, University of Bridgeport, Bridgeport, CT, USA.

[7]. L. Knudsen, "Block Ciphers: A Survey", State of the Art in Applied Cryptography: *Course on Computer Security and Industrial Cryptography (Lecture Notes in Computer Science no. 1528), Springer-Verla*g, pp. 18-48, 1998.

[8]. Encryption Technology White paper, http://security.resist.ca/crypt.htm .

[9]. Bruce Schneier, http://www.schneier.com/paper-blowfish-fse.html