ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm

Vaidhyanathan V
School of Computing, SASTRA University
Tamil nadu, India.
vvn@it.sastra.edu

Manikandan G*
School of Computing, SASTRA University
Tamil nadu, India.
manikandan@it.sastra.edu

Krishnan G
School of Computing, SASTRA University-613402
Tamil nadu, India
gkrishnan@ict.sastra.edu

Abstract : In this world, whatever information that we send can easily be cracked by any third party by intruding it. This obviously results us in a condition to rely upon the science of preserving secrecy and security to our message. This can be very much achieved via a strong encryption algorithm. Blowfish block cipher is one of its kind which still remains as one of the strong encryption algorithm that is not breaked completely till date. It also has a comfortable design which suits for any enhancement or modification in its structure. This is one such work which enhances the performance and provides even a bit more security to the already existing Blowfish Algorithm and it is proved and justified experimentally.

Keywords: Block cipher, Blowfish, F-Function, Security, Performance.

I. INTRODUCTION

Cryptography is a well known and widely used technique that manipulate information in order to crypt their existence. More specifically, cryptography protects information by transforming it into an unreadable format [1]. The original text is transformed into a scramble equivalent text called cipher text and this process is called as "Encryption". This is achieved via an Encryption Algorithm. Only those who possess a secret key can decrypt the cipher text into plaintext. Simply it scrambles a message so it cannot be understood.

Cryptography deals with protecting information by encoding or transformation of data [1].There are two types of cryptographic schemes available on the basis of key.

A. *Symmetric key Cryptography*: This is the cryptographic scheme which uses a common key for enciphering and deciphering the message.
B. *Assymetric or Public Key Cryptography*: This type of cryptographic scheme uses two keys for encryption and decryption called Public key and Private Keys.

We adopted Symmetric key cryptographic scheme and hence only one key is needed for communication. So, the chosen cryptographic scheme involves,

A. *Plaintext*: The original message that has to be communicated to receiver.
B. *Encryption*: Enciphering of data by using a key via a desired encryption algorithm at sender side.
C. *Transmission*: Transfer of cipher message to receiver through a public communication channel.
D. *Decryption*: Deciphering of the ciphertext thus received via the same algorithm (reverse Encryption) by using the key.

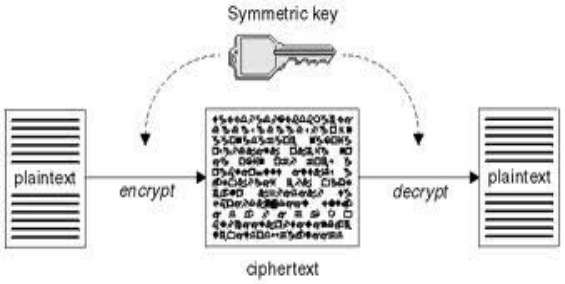

Figure 1: Symmetric Key Cryptography

`

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

A. *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 (say exclusive-or (xor) operation). In a stream cipher the plaintext digits are encrypted one at a time
B. *Block Ciphers*: It is also a symmetric key cipher operating on fixed-length groups of bits, called blocks. A block cipher encryption algorithm takes a n-bit block of plaintext as input, and produces a corresponding n-bit output block of ciphertext.
C. We have chosen block cipher for our cryptographic operation since it is the main tool for implementing private key encryption in practice.[1]

II. LITERATURE REVIEW

A. Blowfish Algorithm:

Blowfish, a symmetric block cipher that uses a Feistel network, iterating simple encryption and decryption functions of 16 times each. The block size is 64 bits, and the key can be any length up to 448 bits. The strength of the Blowfish algorithm relies on its sub-key generation and its encryption. Blowfish is a block cipher which uses a variable-length key. It is well fitted for applications in which the key size does not change often. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. [2]

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 an another function by using the concept of permutation.[3] 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 an 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

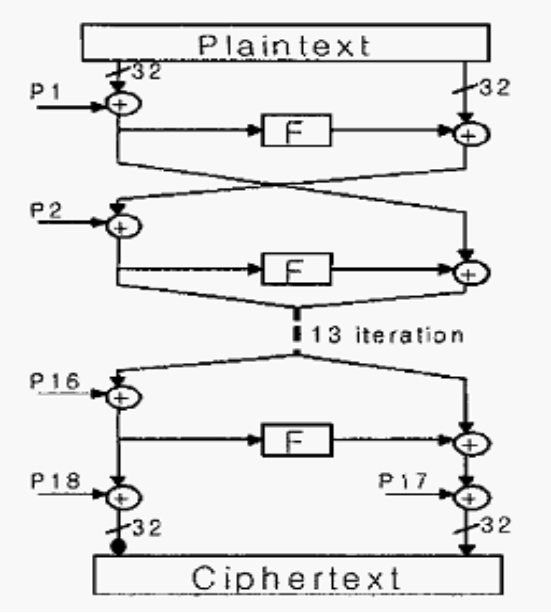

Figure 2: Fiestal structure of Blowfish Cipher

The transformation operations that actually happen inside an F-function are XOR Operation, ADD Operation and few table look up operations. These operations are carried out between four S-Boxes and as a result of all manipulations finally 32 bit entries are transformed into another 32 bit entry. F-Function of a Blowfish algorithm can be depicted pictorially in Fig-3.

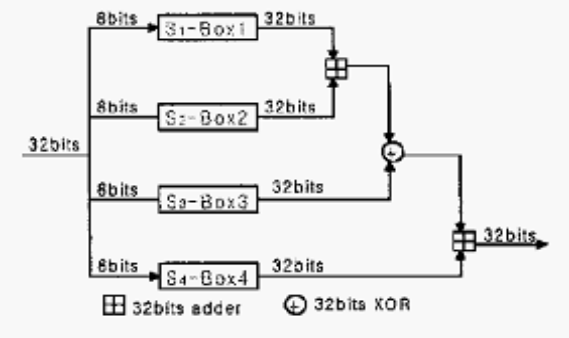

Figure 3: Structure of F-function

III. PROPOSED SYSTEM

We proposed a system which actually brings some modification to the already existing Blowfish Algorithm in terms of its design. Since F-Function Plays a dominant role in Blowfish encryption it is decided to modify the F-function without changing its basic functionalities. The original F-function works algorithmically as,

A. In step1,32 Bit Addition of S-box 1 and S-box 2.
B. In step 2,32 Bit XOR of result of step 1 and S-box 3 .
C. In step 3,The result of step 2 is then XOR with S-4.[4]

But we modify the order of execution of F-Function such that,

A. In step 1,32 Bit XOR of S-box 1 and S-box 2.
B. In step 2,32 Bit XOR of result of S-Box 3 and S-box 4 .
C. In step 3,32 Bit Addition of the results of step 1 and 2.

Our Proposed system can be diagrammatically represented as,

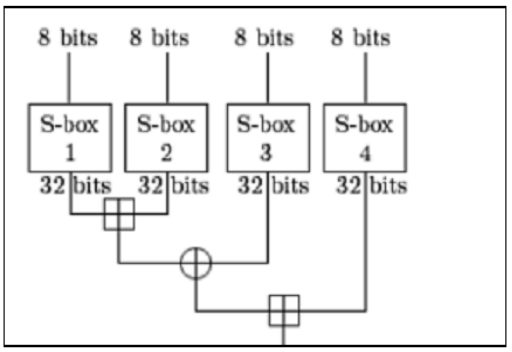

Figure 4: Existing F- Function

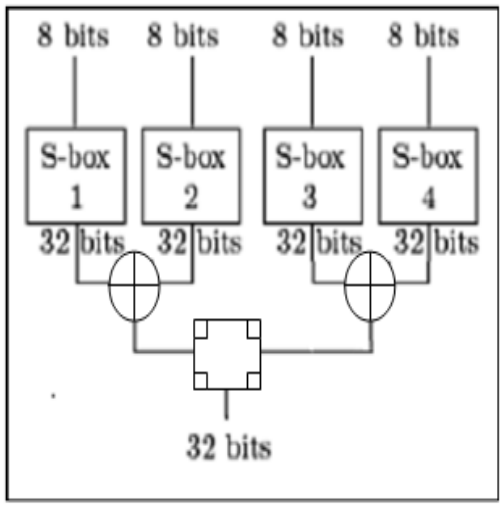

Figure 5: Modified F-Function

The Blowfish algorithm is enhanced both in terms of performance as well as security and they are as follows,

A. The Performance is enhanced because of the execution of steps 1 and 2 in the modified execution of F-function concurrently by performing multithreading and it is proved and justified.(Refer Simulation Results)
B. The execution time of Blowfish algorithm is approximately reduced up to 13.5% on comparing with the original Blowfish Algorithm.
C. 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.
D. 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.
E. 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.

IV. SIMULATION AND RESULTS

We simulated our modified blowfish system in Java since it is better suitable for its platform independent features, user friendly GUI Features and so on than any other programming languages.

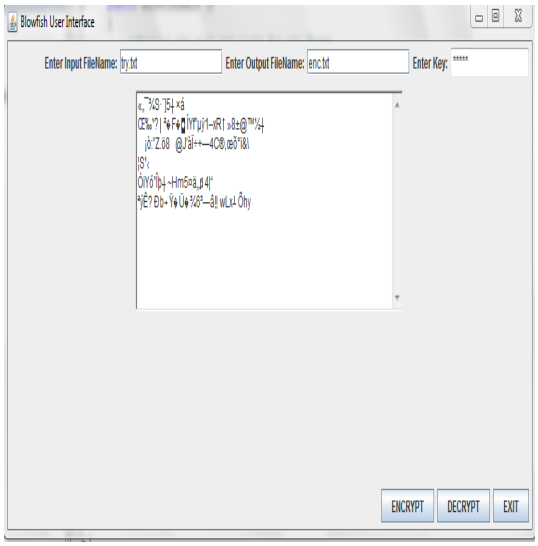

Figure 6:Blowfish Encryption

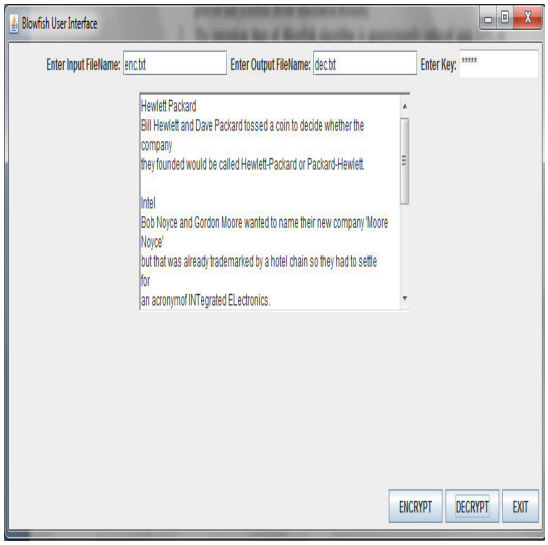

Figure 7:Blowfish Decryption

Table 1: Comparison of Execution Time

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.

V. FUTURE ENHANCEMENTS

The execution time of blowfish algorithm can be further reduced and hence the performance is improved more by adopting the concepts of parallelism which results in the execution of f-Function in parallel environment. Our current future works are concentrated on reducing the execution time f the algorithms if the operations of f-function are executed in a parallel.[5]

VI. CONCLUSION

In this paper we have presented a novel method enhancing security and performance of Blowfish algorithm by using the concept of Multithreading. We have proven that this approach is both an effective Cryptographic method with respect to time as well as a theoretically unbreakable one since the function is modified and hence hard to guess it .Our experimental results proves and justifies that with the commercially available computers the time taken for encryption and decryption process is negligible and we conclude that it has a good performance without compromising the security.

VII. REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practices, 2nd ed., Prentice Hall, 1999.

[2] 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.

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

[4] 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 Bridgeport, Bridgeport, CT, USA. pp. 240-244

[5] 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.

[6] 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-Verlag, pp. 18-48, 1998.

[7] Wikipedia, "Blowfish (cipher). " http://en.wikipedia.org/wiki/Blowfish_cipher”.

[8] B. Schneier **,http://www.schneier.com/paper-blowfish-fse.html**

[9] University of Alberta, http:// www.eualberta.ca I-elliott /ee552 / studentAppNot/1998ff blowfish-encryption.

[10] M. Matsui, “The First Experimental Cryptanalysis of the Data Encryption Standard,” Advances in Cryptology-CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 1-11.

[11] S. Vaudenay, “On the Weak Keys in Blowfish,” Fast Software Encryption, Third International Workshop Proceedings, Springer- Verlag, 1996, pp. 27-32.