ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 4, October 2014

Modified F – Function for Feistel Network in Blowfish Algorithm

S. G. Saravana Kumar, Dr.A.Shanmugam

Associate Professor, Department of E.E.E., Park College of Engg. and Technology, Coimbatore.
Dean & Professor, Department of E.C.E. & E.I.E., SNS College of Technology, Coimbatore.

Abstract: ***A secure computing environment would not be complete without consideration of encryption technology. Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection. Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data. It is obtained by following certain steps of predefined operations called algorithms. The introduction of a key adds another level of security. The process of encryption should be as complicated as possible so that anyone who intercepts the data should not be easily decrypting it. The 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 is 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, we propose a new modified feistel network for blowfish algorithm to make a strong cipher text.***

Keywords: **Encryption, blowfish algorithm, cipher text.**

I. INTRODUCTION

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearranges the data bits in digital signals. In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to difficult on the communications without access to the key. The stronger the cipher, the harder it is for unauthorized people to break it. In this paper we are proposing a modified feistel network for the blowfish algorithm by introducing the concept of GA. The process makes the encryption so complicated so that they cannot be decrypted in the usual way. In this paper we are proposing a modified feistel network for the blowfish algorithm by introducing the concept of GA. The process makes the encryption so complicated so that they cannot be decrypted in the usual way. When we are adding additional key and replacing old XOR by new operation '#', Blowfish will provides better results against any type of intrusion [1]. The simulation results showed that Blowfish has better performance than other commonly used encryption algorithms. Since Blowfish has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm [2].

II. GENETIC ALGORITHMS

Crossover and mutation are two basic operators of GA. Performance of GA depends on them very much. The type and implementation of operators depends on the encoding and also on the problem. There are many ways how to perform crossover and mutation.

a. Crossover

The genetic algorithms typically use the following types of operators:

- Selection: Operator for selecting individuals for reproduction according to their fitness;
- Crossover: Operator of merging the genetic information of two individuals. In many respects the effectiveness of crossover is depended on coding.
- Mutation: In real evolution, the genetic material can by changed randomly by erroneous reproduction or other deformations of genes, e.g. by gamma radiation.

Usually, there are two means of modifying genetic material: a recombination operation that could be understood as some kind of crossover and mutation. The available crossover operators are:

- Single-point Crossover or simple crossover;
- Two-point Crossover;
- Uniform Crossover or discrete crossover;
- Flat Crossover.

b. Mutation

- **Flip Bit** -A mutation operator that simply inverts the value of the chosen gene (0 goes to 1 and 1 goes to 0). This mutation operator can only be used for binary genes.
- **Boundary** - A mutation operator that replaces the value of the chosen gene with either the upper or lower bound for that

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 4, October 2014

gene (chosen randomly). This mutation operator can only be used for integer and float genes.

- **Nonuniform** - A mutation operator that increases the probability that the amount of the mutation will be close to 0 as the generation number increases. This mutation operator keeps the population from stagnating in the early stages of the evolution then allows the genetic algorithm to fine tune the solution in the later stages of evolution. This mutation operator can only be used for integer and float genes.
- **Uniform** - A mutation operator that replaces the value of the chosen gene to a uniform random value selected between the user-specified upper and lower bounds for that gene. This mutation operator can only be used for integer and float genes.
- **Gaussian** - A mutation operator that adds a unit Gaussian distributed random value to the chosen gene. The new gene value is clipped if it falls outside of the user-specified lower or upper bounds for that gene. This mutation operator can only be used for integer and float genes.

III. F - FUNCTION IN FEISTEL NETWORK

A Feistel network is a general method of transforming any function (usually called an F function) into a permutation. It was invented by Horst Feistel and has been used in many block cipher designs. The working of a Feistal Network is given below:

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying *f* to the right half and the Key.
- Note that previous rounds can be derived even if the function *f* is not invertible.

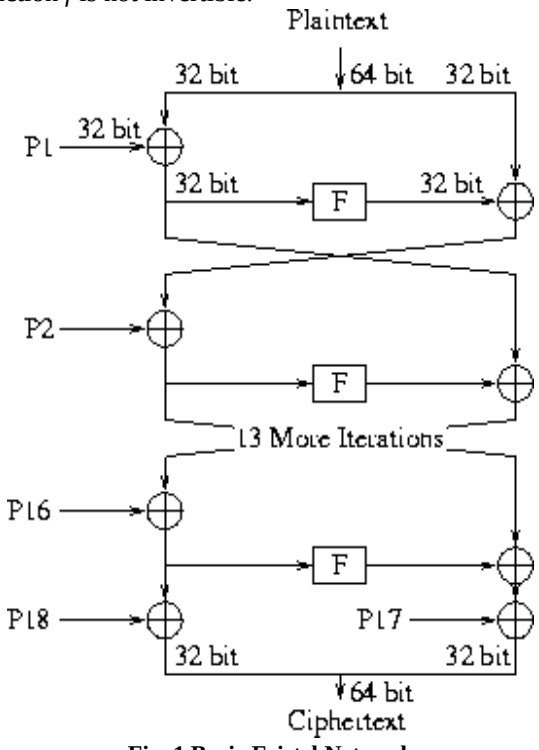

Fig. 1 Basic Feistel Network

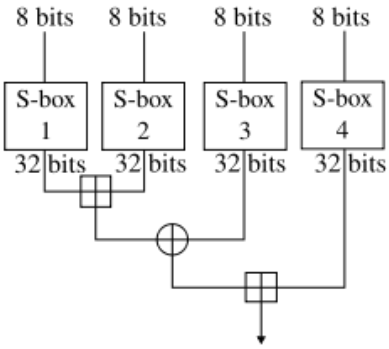

Fig. 2 Basic F – Function in Feistel Network

Fig. 1 & Fig. 2 show the basic feistel network and the operation of F – function in the feistel network. This method is quite well known to everyone and the hackers can possibly identify it. We propose a Modified Feistel Network and a modified F – Function for the feistel network by implementing the genetic algorithm and mutation concept so as to increase the complexity of the algorithm and the quality of the cipher text.

IV. MODIFIED FEISTEL NETWORK AND G – FUNCTION.

We are proposing a modified feistel network and G – function for the blowfish algorithm to improve its complexity and security level of the cipher text obtained from the algorithm. The modified network finds very efficient since the genetic algorithm and mutation concept is involved. Fig. 3 show the modified feistel network and the Fig. 4 show the G – Function.

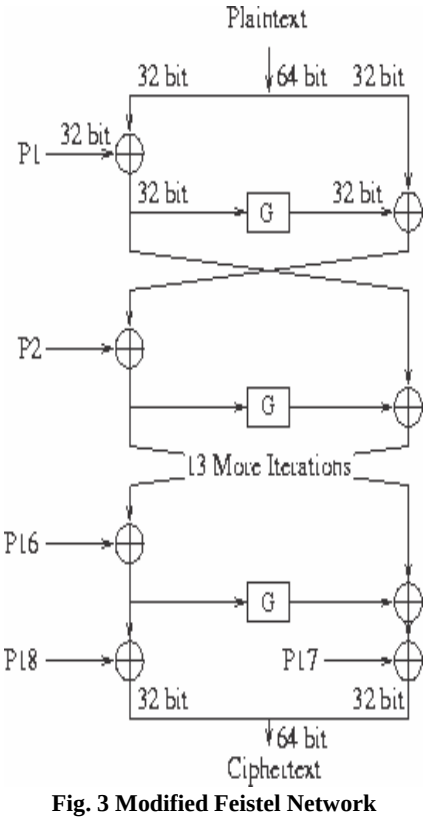

Fig. 3 Modified Feistel Network

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 4, October 2014

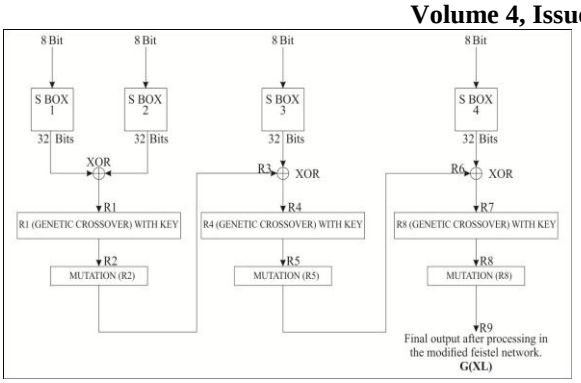

Fig. 4 Modified G – function

V. PROPOSED CHANGES IN THE ALGORITHM

1. Introducing a new method of key generation for the algorithm.
2. Since using multiple secret keys and introducing a new function for the encryption increases the complexity of the algorithm [3].
3. The method of transmitting the data was changed. The data travels in two different paths with different values. This makes the interceptor to confuse and also if the interceptor gets both the transmitted data it is very complicated for them to decrypt since the original key was not known to the sender itself.

ACKNOWLEDGMENT

We would like to thank all our colleagues, friends and family for the full support provided to us for doing this research. We also thank our Management and Principal for supporting us.

REFERENCES

[1] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications, Vol. 1, Issue 2, pp.321-326.

[2] Simar Preet Singh, and Raman Maini "Comparison Of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127.

[3] Alaa H. AL-Hamami, Mohammad A. AL-Hamami, Soukaena H. Hashem "A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique" World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, No. 3, 88-91, 201).

[4] Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E "Blow-CAST-Fish: A New 64-bit Block Cipher" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[5] CARLISLE M. ADAMS, "Constructing Symmetric Ciphers Using the CAST Design Procedure" Designs, Codes and Cryptography, 12, 283–316 (1997), Kluwer Academic Publishers, Boston.

[6] Bruce Schneier, "Designing Encryption Algorithms for Real People".

[7] Serge Vaudenay, "On the weak keys of blowfish", Third International Workshop Cambridge, UK, February 21–23 1996 Proceedings.

[8] Bruce Schneier and John Kelsey, "Unbalanced Feistel Networks and Block-Cipher Design", Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis.

[9] Bruce Schneier, "Why cryptography is harder than it looks" Counterpane Systems.

[10] Bingjie Huang, and Tianjie Cao, "A Password-based Encryption Scheme with Symmetric Key Cryptography" , 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010), DOI: 10.7763/IPCSIT.2012.V53.No.2.48.

[11] Alaa H. AL-Hamami, Mohammad A. AL-Hamami, Soukaena H. Hashem, " A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique" World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, No. 3, 88-91, 2011.

[12] Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 1, November 2011.

AUTHORS BIOGRAPHY

S.G.Saravana Kumar received the B.E., degree in Electrical & Electronics Engineering from K.S.Rangasamy College of Technology under Periyar University and M.E., Degree from Bannari Amman Institute of Technology under Anna University Chennai. He is doing his Research in the area of VLSI Design & Testing under Anna University Chennai. Presently he is working as Associate Professor, Department of Electrical and Electronics Engineering, Park College of Engineering and Technology, Coimbatore. His areas of interest include FPGA Implementation of Signal Processing algorithms, Encryption algorithms, and Electrical Machines.

Dr.A.Shanmugam received the B.E., Degree in PSG College of Technology in 1972, Coimbatore and ME Degree from College of Engineering, Guindy, Chennai in 1978 and Doctor of Philosophy in Electrical Engineering from Bharathiyar University, Coimbatore in 1994. He was working as a Lecturer in Annamalai University untill 1978. He was the Professor and Head of Electronics and Communication Engineering Department at PSG College of Technology, Coimbatore during 1999 to2004. Authored a book titled "Computer Communication Networks" which was published by ISTE, New Delhi, 2000. He was working as Professor & Dean of Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam until 2013. Presently he is working as Professor and Dean of E.C.E. and E.I.E, SNS College of Technology, Coimbatore. He is on the editorial board of International Journal Artificial Intelligence in Engineering

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 4, October 2014

& Technology (ICAIET), University of Malaysia, International Journal on "Systemics, Cybernetics and Informatics (IJSCI)" Pentagram Research Centre, Hyderabad, India. He is member of the IEEE, the IEEE computer society.