IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. II (Nov – Dec. 2015), PP 24-30
www.iosrjournals.org

Simulated Analysis and Enhancement of Blowfish Algorithm

[1]Rohan Kumar, [2]Rahul Thakkar, [3]Manoj Kumar
[1,2,3]School of Computer Application Lovely Professional University

Abstract: *This paper represents or analyzes the security of system based on Blowfish. Blowfish mainly focuses on the encrypt and decrypt techniques and algorithms apply for cryptanalysis. It describe the algorithms for encryption as well as decryption algorithms and also give the sufficient description of key generation, key expansion, function and working principle of Blowfish cipher with proper explanations. Taking the current era, Most of the famous systems which offer security for a network or web or to a data are vulnerability to attacks and they are broken at some point of time by effective cryptanalysis methods, irrespective of its complex algorithmic design. In the general, today's cryptography world is bounded to an interpretive of following any one or multi encryption scheme and that too for a single iteration on a single file only. This is evident in the maximum of the encryption-decryption cases. It also describes the comparisons between older blowfish and enhances blowfish. It also shows enhance Blowfish algorithm for encryption and decryption of data. It is also give the proper simulated analysis of encryption and decryption time for different file formats using a windows application. It describe feature of application and its process and efficiency as well as calculation of time and throughput.*

Keywords*: Cryptography, Function F1, Function F2, Enhance Blowfish Algorithm, Security, Encryption, Decryption, AES, Feistal Cipher, Windows Application.*

I. Introduction Of Cryptology

Cryptology the technique or methodology and science of protection or secret writing or reading and sending of messages in encrypted form [1]. It works based on two main areas: cryptography and cryptanalysis.

Cryptography is basically related with converting data into some unreadable form to make them secure and safe to attacks. Where the term cryptanalysis is related with breaking or decryption of code and messages which are in coded form. Cryptanalysis is used to break cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown [2].

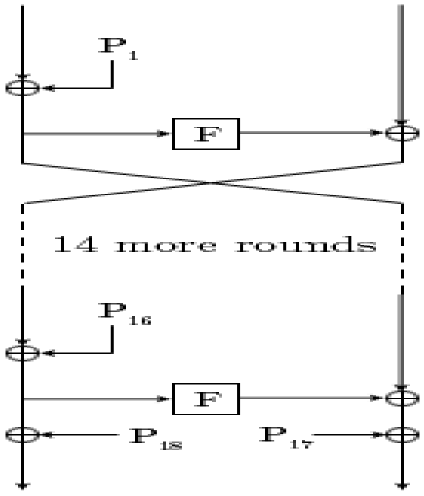
II. Introduction To Cryptography

An encryption calculation assumes a critical part in securing the information in putting away or exchanging it[1][9]. The file encryption techniques calculations are ordered into Symmetric (mystery) and Asymmetric (open) keys encryption [3]. In Symmetric key encryption or mystery key encryption, one and only key is utilized for both encryption and decoding of information. Information encryption standard (DES), Triple DES, Advanced Encryption Standard (AES) and Blowfish Encryption Algorithm [1]. In open key encryptation utilizes two keys, one for encryption and other for unscrambling RSA[4].

III. Existing Blowfish Encryption Algorithm

Blowfish was composed in 1993 by Bruce Scheier as an issue, option to current encryption algorithms [1]. Blowfish is a balanced piece encryption calculation planned in thought with [5]:-

- **fast**: It encodes information on huge 32-bit chip at a rate of 26 clock cycles for each byte. [5]
- **compact**: It can run in under 5k of memory that is least memory correlation to other cipher[6].
- **simple**: It utilizes expansion, XOR, lookup table with 32-bit operands [7].
- **secure**: The key length of variable, it can be in the scope of 32bit to 448 bits: default length is 128 bits key [3] [1].
- it is suitable for applications where the key does not change frequently, in the same way as correspondence connection or a programmed record encryptor.
- unpatented and emine
- Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date [9].
- Schneir designed Blowfish as a general - purpose algo, intended as an alternative to the DES and free of the problems and constraints associated with other algorithms [8].
- Blowfish is a Feistel block cipher with a 64 bits block size and a variable key size up to 448 bits long [5] [10].
- It is consists of total 16 round process or functioning as well as DES or Feistel[11].



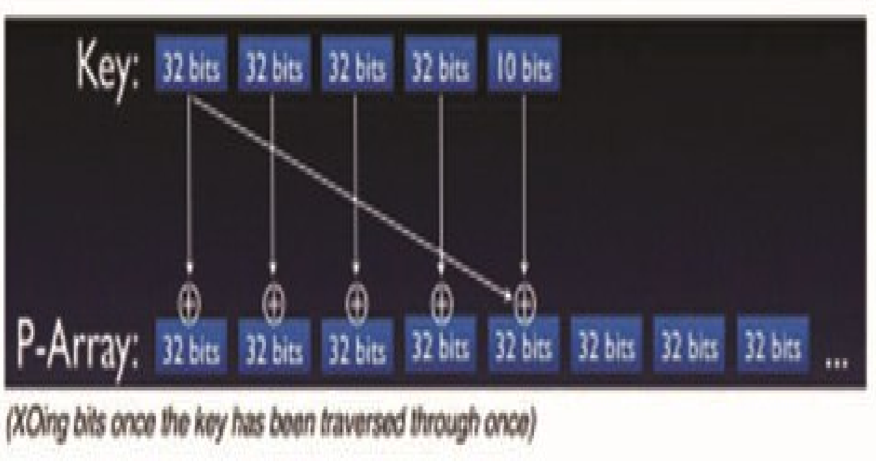
IV. Description Of Blowfish Algorithm

Blowfish symmetric square figure calculation encodes piece information of 64-bits in one time. It will take after the feistel system and this calculation is separated into two sections [8].

1. **Key-development**: Blowfish is a Feistel system square figure with a 64 bits piece size and a vary key size up to 448 bits long[8].the 448 bits limit is here to beyond any doubt that each bit of each sub-key relies on upon each piece bit of the key.
2. **Data-Encryption** :It have a capacity to emphasize sixteen rounds of system. Each round comprises of a key-subordinate change, and a key information subordinate alteration. All operations are XOR and increases on 2^5 bits plain-text [5]. The main processes are four ordered exhibit information maintenance tables for every round [8].

V. Key Expenssion

1. The initial 2^5bits of the key are XOR with PA1.it is the initial 2^5-bit enclose the P-array [6].
2. The second 2^5 bits of the key are XOR with PA2, as well as key are XOR until each of the 448, or less, keys bits have been XOR [7].
3. By cycle the keys-bit by coming back to the start of the key, unless the whole P-exhibit has been XOR with key-value [8]. The key, until the whole PA-show has been XOR.



VI. Blowfish Encryption And F1-Function

Blowfish algorithm is a Feistel structure network containing of sixteen rounds [5]. The input is a 2^6-bits data elements, X

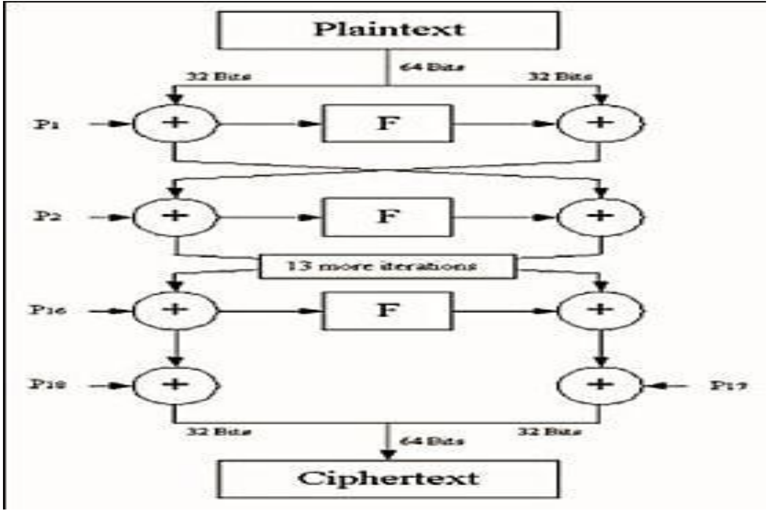
Divide X into two 32-bit halves: X_L, X_R

For i = 1 to 16:

$X_L = X_L$ XOR P_i

$X_R = (X_L)$ XOR X_R

Exchange X_L and X_R
Exchange X_L and X_R (and Undo the last-one swapping.) [11].



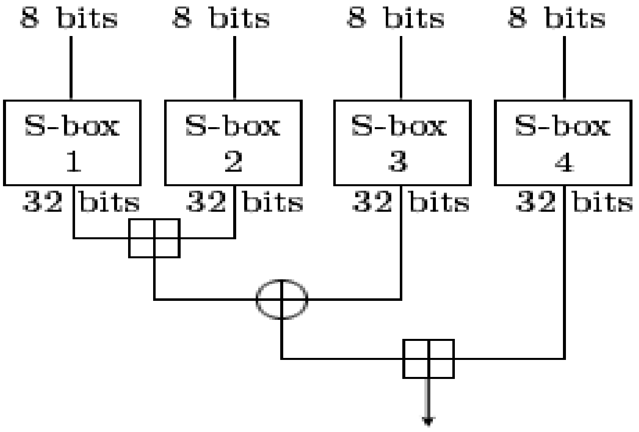
VII. Proposed Blowfish Algorithm

In the new introduced algorithm a file which has data is splits into desired number of parts according user's need and then after the crypto-graphical encryption phase is used. In order to get high reliability paper defines more than one crypto scheme which really gives surety of more safety and reliability. It describe the method that make difference between the cryptographic scheme by providing various keys for each encryption of split files; key should be given correctly at the time of decryption for batter results. Using enhanced Blowfish algorithm for Encrypt and Decrypt of data which gives as a better results both in terms of performance and as well as safety. In enhancement of the algorithm we use another function F2 for more complexity to crystalize.

In order to crypto-graphical aspects, in order to enhance the functionality of the Blowfish algorithm it is introduced to modify the F1-Function as F2-Function by taking the concepts of multithread.

VIII. Existing Function F1

The F1 function is: F1(X_L) = ((S1,a + S2,b mod 2^{32}) XOR S3,c) + S4,d mod 2^{32}) [8].
Where a, b, c, d are four 8 bit quartered derived from X_L. Decryption process is the same as encryption process, except the P-arrays are used in opposite. It produced 32 bits.Ḩ is additional XOR 2^{32}[8] [6].



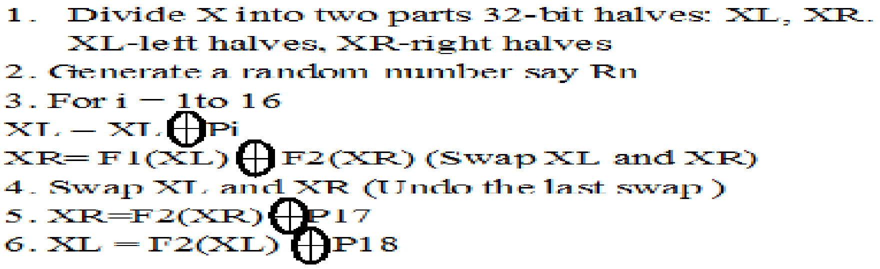
F1= ((S1[a] + S2[b] mod 2^{32}) ^ S3[c]) + S[d] mod 2^{32}).

IX. Enhance Function F2

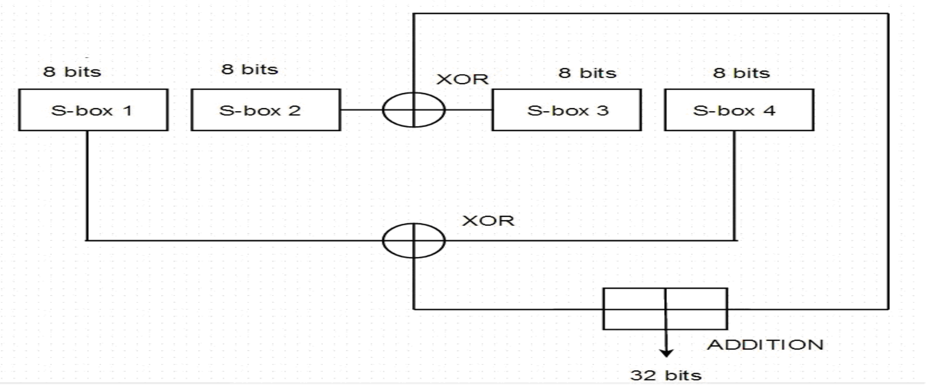
- Enhance F2-Function: Function F1 plays pivot role in the algorithm or design, and decided to modify Function F1[12].
- Original function F1 is defined as follows [8][6].
  F1= ((S1[a] + S2[b] mod 2^{32}) ^ S3[c]) + S[d] mod 2^{32}).
- Instead, modify the F1-Function by replacing two addition operators by two XOR Operators.
- Thus the modified F2-function is written as,

F2= ((S1 [a] ^ S2 [d] mod 2^{32}) + (S3 [b]) ^ S[c] mod 2^{32})).

- This improvement increases the simultaneous process of two XOR operators [12]. In the original F1-function it process in sorted order and it needs 2^5 Addition operations and 2^4 XOR operations [8]. But in the modified F2-function it needs the same 48 gate operations 2^5-XORs, 2^4-additions but time taken to processed these operations will be decrease because of multithreading process [12].
- Execution of 32 XOR operations in parallel order using threads and hence time taken to complete 16 gate operations will be equivalent to the time taken to complete 32 XOR operations since running it in parallel environment [12].
- The remaining steps remain the same as that of Blowfish algorithm. The Enhance blowfish encryption algorithm runs on the input plain text:-



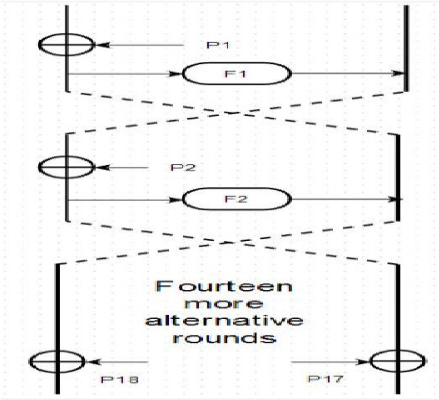
```
1. Divide X into two parts 32-bit halves: XL, XR.
   XL-left halves, XR-right halves
2. Generate a random number say Rn
3. For i = 1to 16
$XL = XL \oplus Pi$
$XR= F1(XL) \oplus F2(XR)$ (Swap XL and XR)
4. Swap XL and XR (Undo the last swap )
5. $XR=F2(XR) \oplus P17$
6. $XL = F2(XL) \oplus P18$
```



F = ((S1 [a] XOR S2 [d] mod 2^{32}) + (S3 [b]) XOR S[c] mod 2^{32})).

X. Enhance Feistal Structure

In advance and enhance feistal structure of Blowfish algorithm, there is used of two function F1 and F2. Here F1 is the old function or the original one. Here first half of plain text is xor with p1or permutation box, and then after F1 is come in action. After swapping of XL and XR xor with function key F2. This process in goes 16 rounds alternative move with F1 and F2. This movement makes plain text encryption more complex structure.



XI. Significant Of Enhance Blowfish

1. The process time of algorithm is approximately decreased compare with the original algorithm.
2. Here 2-XOR gates and 1-ADDITION are used but the original F1-function uses 2-ADDITIONs and 1-XOR gate and there is no abrupt change in the execution time or clock cycles required for successful

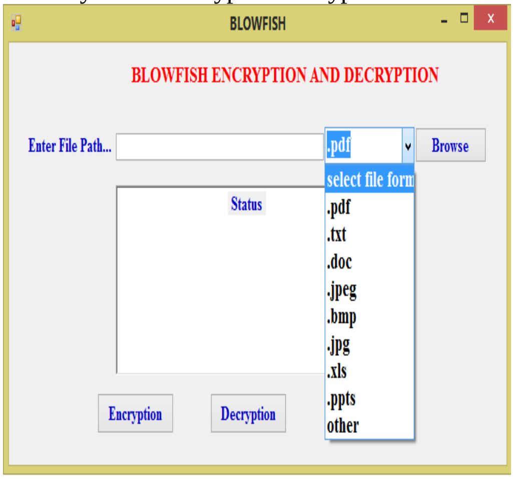
execution. This is because all fundamental logical operations like AND, OR, XOR takes more or less equal time when running or execution under any programming languages since those languages are logically driven.

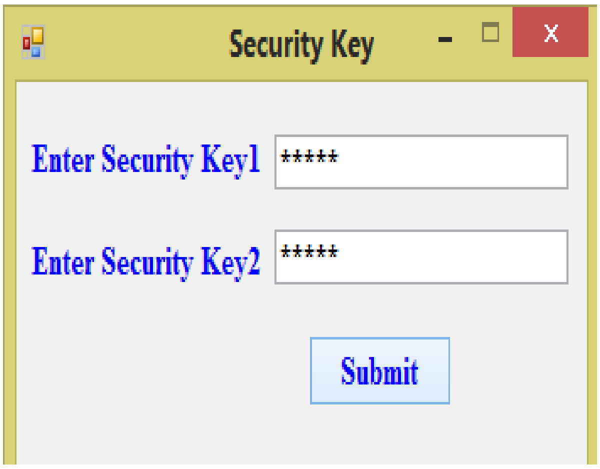
3. It's complicated for the attacker to realize that the F1-function is modified and hence chances of attack are less on comparing with the original algorithm [10].
4. Since introduced system bring changes only to the order of process and no changes is made to the actual functionalities did not added or removed new operations just changed only the order of process of previous XOR and Addition so doing cryptanalysis is not necessary [12].
5. Algorithm become for complex thus security improved.
6. Two symmetric F functions are used which are quite difficult to cryptanalyze.

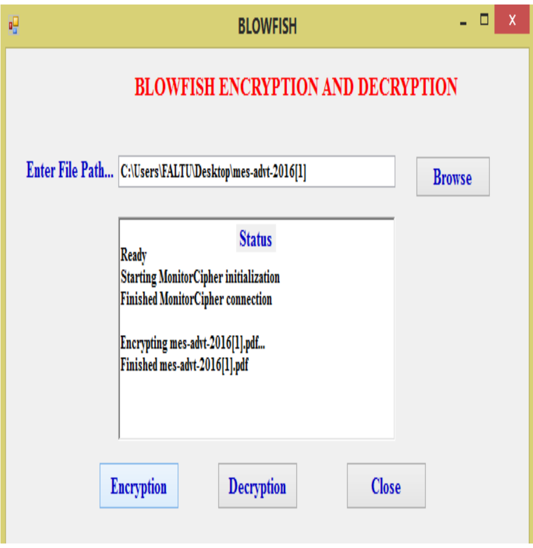
XII. Simulated Analysis Of Blowfish Algorithm Using Windows Application

The all enhancement and significant of Blowfish algorithm are done using the windows application. This application is basically developed in the C# language. The application is tested on the personal computer with configuration Windows 8.1, 4GB RAM 64 bit system, 2.40 GHz processor. Significant of application is following:-

1. We can select any type of file format to encrypt or decrypt.
2. This application is well define for encrypt as well as decrypt any type of file or any size.
3. It also able to do multiple encryptions i.e. if user wants to encrypt the already encrypted file, user can do it very frequently.
4. We can decrypt a file as much times as we want.
5. Users select a file and then after user click on encryption or decryption button a new window is open to save the file location.
6. Then after an input dialog of insert key is open. It consists of two key textbox for re-conformation of key. In both condition encryption and decryption user need to give same key.
7. After successful insertion of key it will encrypt or decrypt a file within some second.







BLOWFISH

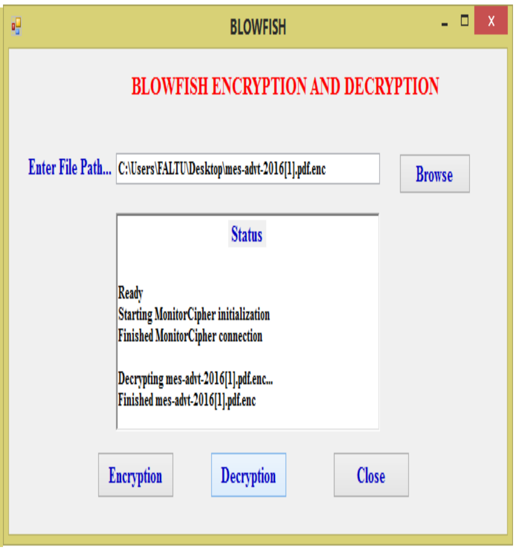
BLOWFISH ENCRYPTION AND DECRYPTION

Enter File Path... C:\Users\FALTU\Desktop\mes-advt-2016[1]

Status
Ready
Starting MonitorCipher initialization
Finished MonitorCipher connection

Encrypting mes-advt-2016[1].pdf...
Finished mes-advt-2016[1].pdf

Fig. Encryption window



BLOWFISH

BLOWFISH ENCRYPTION AND DECRYPTION

Enter File Path... C:\Users\FALTU\Desktop\mes-advt-2016[1].pdf.enc

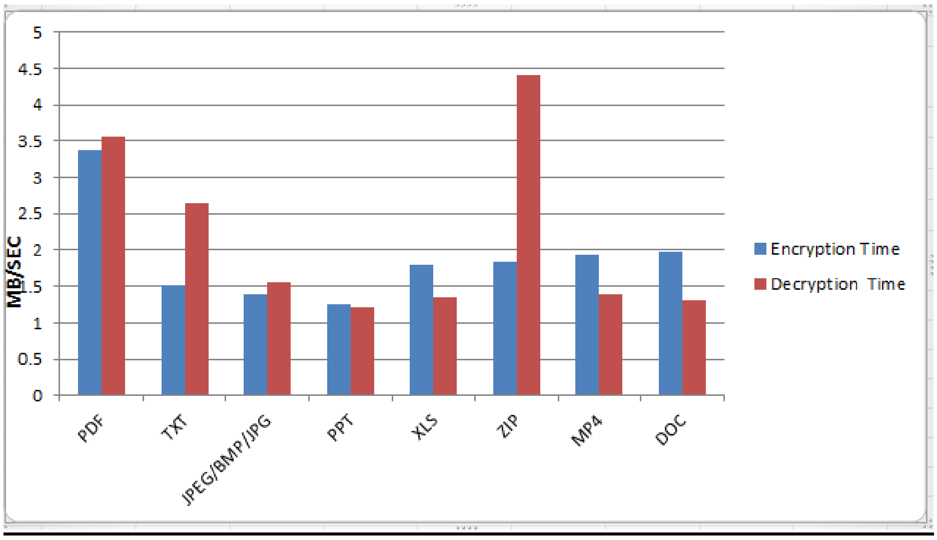
Status
Ready
Starting MonitorCipher initialization
Finished MonitorCipher connection

Decrypting mes-advt-2016[1].pdf.enc...
Finished mes-advt-2016[1].pdf.enc

Fig. decryption window

XIII. Performance Analysis Of Different File Format Using Blowfish Algorithm

Throughput of encryption and decryption is calculated as the total plain text and cypher text in KB and time i rocess takes time to produced cipher-text from plain-text and decryp from cipher-text. It sl decryption time. This application can take different file formats like pdf, text, image, docs, xls, ppts, zip, video files in any range. The performance chat and table is design to show the encryption time, decryption time of each file format individually.



The performance table is design to show the encryption time, decryption time of each file format individually.

Encryption and Decryption rate in MB/SEC			
File Type	Size	Encryption Time	Decryption Time
PDF	861KB	3.37	3.55
TXT	40KB	1.52	2.65
JPEG/BMP/JPG	144KB	1.40	1.55
PPT	877KB	1.26	1.22
XLS	71KB	1.80	1.35
ZIP	7KB	1.84	4.41
MP4	23591KB	1.93	1.40
DOC	50KB	1.98	1.31

XIV. Conclusions

Cryptology the technique or methodology and science of protection or secret writing or reading and sending of messages in encrypted form. Blowfish is the symmetric block cipher, where simply one and only key is utilized for encryption and unscrambling. Blowfish was composed in 1993 by Bruce Scheier as an issue, option to existing encryption calculations. the key length is variable ,it can be in the scope of 32bit to 448 bits: default 128 bits key length. It is Unregistered and eminence free. Blowfish is one of the quickest piece figures all in all utilization, aside from when evolving keys. It also provides a batter data safety when transmitted over any unsecure way. Attackers will not have any guesses about modification both in terms of algorithm. That is, it has a good performance without compromising the security and the modified F2-function also improved the performance by decreasing the rounds up to some percentages and decrease the processing time. Use of two functions F1 and F2 make algorithm structure more complex for the attacker. Using of application user can easily secure all types of file within some second. The complete simulated analysis is described and tries to make algorithm more secure.

Reference

[1]. M. Anand Kumar and Dr. S. Karthikeyan Published Online March 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.02.04.

[2]. Cryptography And Network Security-William Stallings.

[3]. Gurjeevan Singh, Ashwani Kumar, K. S. Sandha /International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[4]. M. Anand Kumar and Dr.S.Karthikeyan I. J. Computer Network and Information Security, 2012, 2, 22-

[5]. Jasdeep Singh Bhalla, Preeti Nagrath International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153

[6]. P. KarthigaiKumar, K.Baskaran,” An ASIC implementation of low power and high throughput blowfish crypto algorithm”, Microelectronics Journal 41 (2010), pp.347–355.

[7]. Pratap et al., International Journal of Advanced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201

[8]. Kevin Allison, Keith Feldman Ethan Mick Schneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher(Blowfish)." Blowfish Paper. 1993. Web. 18 Mar. 2012.

[9]. Milind Mathur, Ayush Kesarwani Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[10]. Deepak Kumar Dakate, Pawan Dubey International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012

[11]. Afaf M. Ali Al-Neaimi, Rehab F. Hassan IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.3, March 2011.

[12]. Chakarapani.k Journal of Theoretical and Applied Information Technology 31st January 2012. Vol. 35 No.2