



**L** OVELY  
**P** ROFESSIONAL  
**U** NIVERSITY

---

**Blowfish Algorithm**

A Paper Writing Report submitted

By

**Mandeep Kaur**

To

**School of Computer Applications**

In partial fulfillment of the Requirement for the

Award of the Degree

Of

**Master of Computer Application**

Under the guidance

Of

**Ms Rajni Bhalla**

April 2015

## **CERTIFICATE**

This is to certify that **Mandeep Kaur** has completed MCA report titled **Blowfish Algorithms** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree.

The report is fit for the submission and the partial fulfilment of the conditions for the award of MCA.

## **DECLARATION**

I hereby declare that the pre-dissertation entitled **Blowfish Algorithms** submitted for the MCA Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree.

**Date**  
**29/04/2015**

**Name –Mandeep Kaur**  
**Reg no.-11403850**

# BLOWFISH ALGORITHM

**Abstract**— This paper represent or analyze the security of system based on Blowfish. Blowfish mainly focuses on the encryption and decryption techniques and algorithms based on 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. On considering the current scenario, Most of the famous 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 the general, today's cryptography world is bounded 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. It also describes the comparisons between older blowfish and enhances blowfish. We used enhance Blowfish algorithm for Encryption and Decryption of data.

Keywords: Cryptography, Function F, Enhance Blowfish Algorithm, Security, Encryption, Decryption, AES, Feistel Cipher.

## 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].

## INTRODUCTION TO CRYPTOGRAPHY

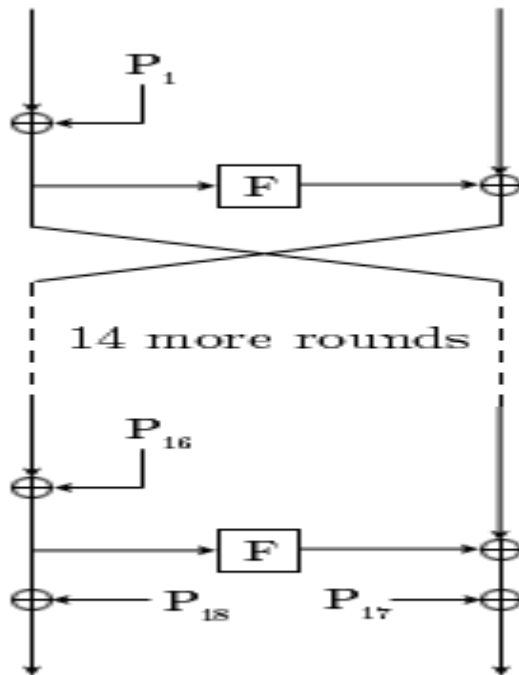
An encryption calculation assumes a critical part in securing the information in putting away or exchanging it[1][9]. The encryption calculations are ordered into Symmetric (mystery) and Asymmetric (open) keys encryption [3]. In Symmetric key encryption or mystery key encryption, one and only key is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

## EXISTING BLOWFISH ENCRYPTION ALGORITHM

Blowfish was composed in 1993 by Bruce Scheier as an issue, option to existing encryption algorithms[1]. Blowfish is a symmetric 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].
- Schneier 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 consists of total 16 round process or functioning as well as DES or Feistel[11].



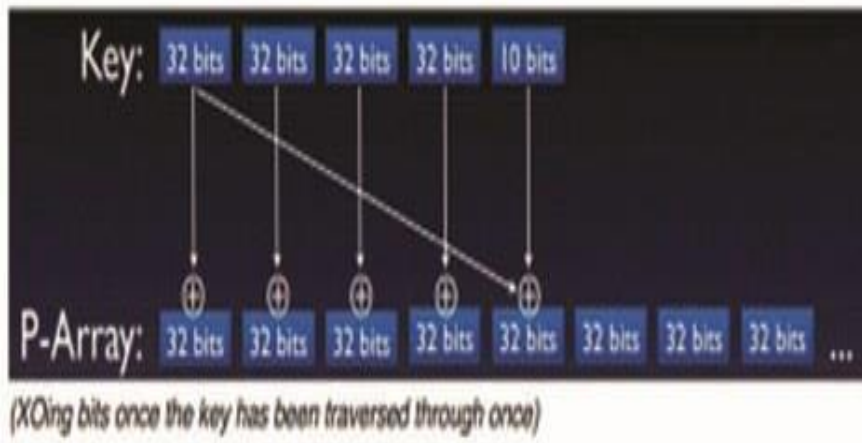
## DESCRIPTION OF BLOWFISH ALGORITHM

Blowfish symmetric square figure calculation encodes piece information of 64-bits at a 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 bit piece size and a variable key size up to 448 bits long[8].the 448 bits limit is here to beyond any doubt that each bit of each subkey relies on upon each bit of the key.
2. **Data-encryption :**It is having a capacity to emphasize 16 times/rounds of system. Each round comprises of a key-subordinate change, and a key- and information subordinate substitution. All operations are XORs and increases on 32-bit plain text[5]. The main operations are four ordered exhibit information lookup tables for every round[8].

**KEY EXPENSION**

- The initial 32 bits of the key are XORed with PA1.it is the initial 32-bit enclose the P-array [6] .
- The second 32 bits of the key are XORed with PA2, as well as key are XOR until each of the 448, or less, key bits have been XORed[7].
- Cycle through the key bits by coming back to the start of the key,until the whole P-exhibit has been XORed with key[8].the key, until the whole PA-show has been XORed.



**BLOWFISH ENCRYPTION AND F-FUNCTION**

Blowfish is a Feistel network consisting of 16 rounds[5]. The input is a 64-bit data element, X

Divide x into two 32-bit halves:  $X_L, X_R$

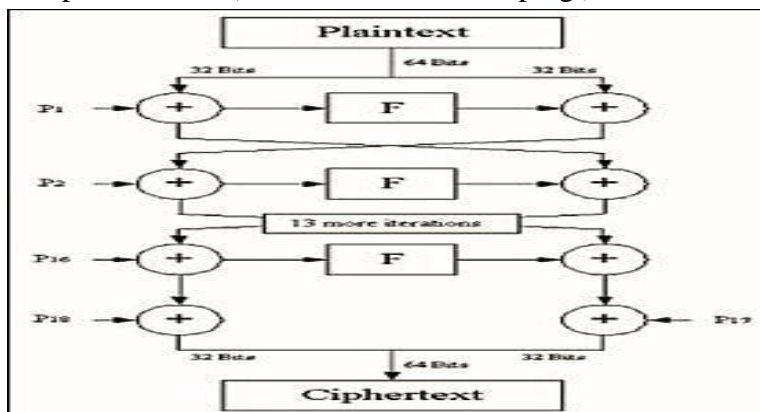
For  $i = 1$  to 16:

$$X_L = X_L \text{ XOR } P_i$$

$$X_R = (X_L) \text{ XOR } X_R$$

Swap  $X_L$  and  $X_R$

Swap  $X_L$  and  $X_R$  (and Undo the last swaping.) [11].



**PROPOSED BLOWFISH ALGORITHM**

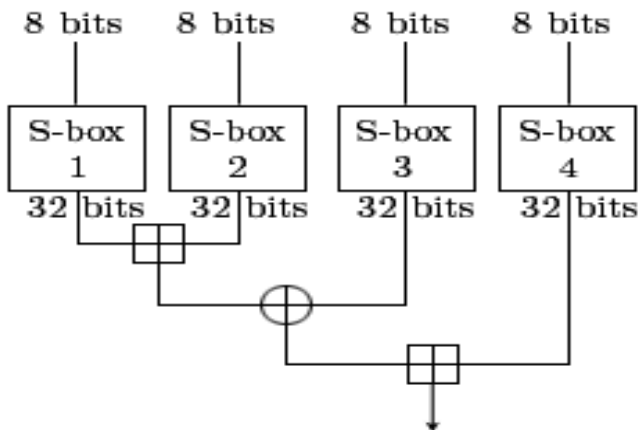
In the new approach a file which has secret data is sliced into desired number of pieces upon user's specification and then the cryptographic encryption phase is carried out. In order to get more security paper can define more than one crypto scheme which definitely ensures null suspicion and more security. It describe the method that 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 batter results. Using enhanced 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.

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.

**EXISTING FUNCTION F**

The F function is:  $F(X_L) = ((S1,a + S2,b \text{ mod } 2^{32}) \text{ XOR } S3,c) + S4,d \text{ mod } 2^{32}$

where a, b, c, d are four 8 bit quartered derived from  $X_L$ . Decryption is the same as encryption, except the P-arrays are used in reverse.it produced 32 bits.H is additional XOR  $2^{32}$ [8] [6].



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

**ENHANCE FUNCTION F**

- Enhance F-Function: Function F plays an important role in the algo or design, and we decided to modify Function F[12].
- Original function F is defined as follows[8][6].  
 $F = ( (S1[a] + S2[b] \text{ mod } 2^{32}) \text{ XOR } S3[c] ) + S[d] \text{ mod } 2^{32} )$ .
- Instead, modified the F-Function by replacing 2 addition operations as XOR Operations.
- Thus the modified F-Function is written as,  
 $F = ((S1 [a] + S2 [b] \text{ mod } 2^{32}) \text{ XOR } (S3[c] + S[d] \text{ mod } 2^{32} ))$ .
- This modification leads to the simultaneous execution of two XORed operations[12]. In the case of original F-function which executes in sorted order and it requires 32 Addition operations and 16 XORed operations[8]. But in the case of our modified F-function it requires the same 48 gate operations 32-XORs, 16-additions but time taken to execute these 48 operations will be reduced because of multithreading[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 = 1 to 16:

$XL = XL \oplus P_i$

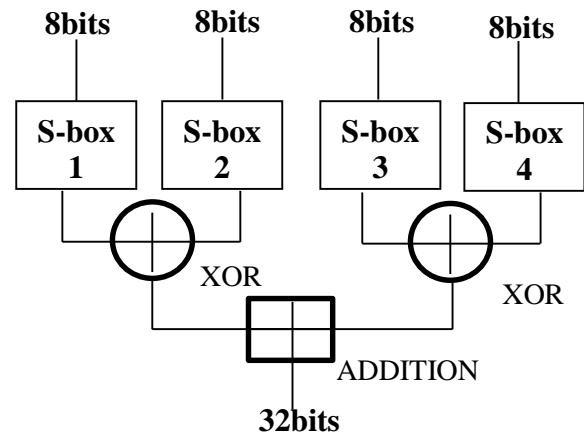
$XR = F(XL) \oplus XR$  (Swap XL and XR)

4. Swap XL and XR (Undo the last swap )

5.  $XR = XR \oplus P_{17}$

6.  $XL = F(XR) \oplus P_{18}$

7. Concatenate XL and XR



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

### SIGNIFICANT OF ENHANCE BLOWFISH

1. The execution time of Blowfish algorithm is approximately reduced on comparing with the original Blowfish Algorithm.
2. Although, we used 2-XOR gates and 1-ADDITION but the original F-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/execution under any programming languages since those languages are logically driven.
3. It's quite hard for the attacker to realize that the F-function is modified and hence probability of attack is less on comparing with the original Blowfish algorithm [10].
4. Since our proposed system bring modifications only to the order of execution and no changes is made to the actual functionalities didn't added or removed new operations just changed only the order of execution of existing XOR and Addition so performing cryptanalysis is not necessary[12].

### CONCLUSION

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 Schneier as an 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 high end data security when



transmitting over any insecure medium. Intruders will not have any idea about modification both in terms of algorithm. 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 up to some percentages and reduces the execution time.

## **REFERENCE**

1. M. Anand Kumar and Dr.S.Karthikeyan Published Online March 2012 in MECS (<http://www.mecspress.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 [www.ijera.com](http://www.ijera.com)
4. M. Anand Kumar and Dr.S.Karthikeyan I. J. Computer Network and Information Security, 2012, 2, 22-28
5. JasdeepSinghBhalla,PreetiNagrath 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. KevinAllison,KeithFeldmanEthan MickSchneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher(Blowfish)." Blowfish Paper. 1993. Web. 18 Mar. 2012.
9. MilindMathur,AyushKesarwaniProceedings 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. HassanIJCSNS International Journal of Computer Science and Network Security, VOL.11 No.3, March 2011.
12. Chakarapani.k Journal of Theoretical and Applied Information Technology 31<sup>st</sup> January 2012. Vol. 35 No.2