International Journal For Technological Research In Engineering
Volume 3, Issue 9, May-2016 *ISSN (Online): 2347 - 4718*

BLOWFISH ALGORITHM: A DETAILED STUDY

Veena Parihar[1], Mr. Aishwary Kulshrestha[2]
[1]Rajasthan College of Engineering for Women, Jaipur, Rajasthan, INDIA
[2]Department of Computer Science Engineering, Rajasthan Technical University, Kota, Rajasthan, INDIA

Abstract: As there is enormous increase or rise in the data exchange by the electronic system, the requirements of information security has become a compulsion. The most important concern in the communication system which is between sender and receiver is the security of the information which is to be transmitted. To get rid of the intruders various cryptographic algorithms are used for example: AES, DES, Triple DES, Blowfish, etc. This paper is about encryption and decryption of messages using the secret-key block cipher which is known as 64-bits Blowfish which is being designed to increase the overall message security and also to improve the performance.
Index Terms: Blowfish, AES, Private Key, Public Key, Feistel network

I. INTRODUCTION

In the field of the information security, the cryptography algorithms plays a very important role. These cryptographic algorithms are categorized into the following two categories, Symmetric and Asymmetric key cryptography [1]. In the case of symmetric key encryption [2], we use only the single key to encrypt as well as to decrypt the data. In such types of the encryption techniques key will plays a crucial role in the process of encryption and decryption of the data. The use of weak key in the algorithm will let out data to be decrypted very easily. The strength of the Symmetric key encryption will depends upon the strength of the key, weaker the key, weaker the algorithm and vice versa. In the similar way the symmetric algorithms can be classified into two main categories: block ciphers and stream ciphers. The working of block ciphers algorithms is that it operates on data in forms of groups or blocks. .Examples of Symmetric Key Encryption is the Data Encryption Standard (DES), the Advanced Encryption Standard (AES) and Blowfish. While in the case of the asymmetric key encryption, we have two types of keys which are used in the process, namely, private keys and public keys. In this, the public key is used in the process of encryption while the private key is used for the decryption process. Example of such a asymmetric encryption is Digital Signatures. Public key is known to all the public while the private key is known only to the user. In this paper we will focus on the Blowfish algorithm, and it is among the most public domain encryption algorithms [3]. It was designed in the year 1993 by Bruce Schneider and thereafter it is considered as the quick substitute of the existing encryption algorithms. Blowfish is the symmetric key block cipher and it make use of the 64 bit block size and the key which is variable in length. The encryption key which we use in the Blowfish can take length key 32 bits to 448 bits. The Blowfish algorithm has variants of 14 rounds or less [4]. Blowfish is among the fastest block ciphers which have developed till date. Blowfish algorithm is free from patents and copyrights. Till date no successful attack on this algorithm is known but it suffers from weak keys problem.

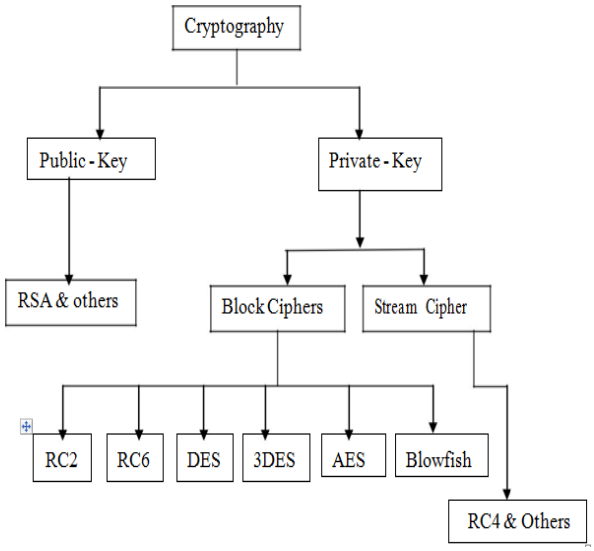

Figure 1:- Overview of the field of Cryptography

Algorithm	Key Size	Block Size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 Bits	10, 12 or 14
Blowfish	32-448 bit .	64 bits	16

Figure 2:- Comparison of DES, 3DES, AES and Blowfish algorithm.

II. DESCRIPTION OF ALGORITHM

Blowfish is the symmetric block cipher algorithm and it encrypts the block data of 64-bits at a time. It follows the Feistel network and the working process of this algorithm is divided into two parts.

A. Key-expansion

In this part we will broken down the key of at most 448 bits into several sub key arrays such that total will count to 4168 bytes.

B. Data-Encryption

In the data encryption process we will iterate 16 times of network. And in each round, there consists of the key-dependent permutation, and the key- and data- dependent substitution. The operations in the algorithms are XORs or additions on 32-bit words. What more we have to do in this process is to create four indexed array data lookup tables for each round.

Key Generation:

• Blowfish uses large number of sub keys. These keys are generating earlier to any of the data encryption or the decryption.

• The p-array consists of 18, 32-bit sub keys: P1,P2,……..,P18

• Four 32-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,……. S1,255

S2,0, S2,1,…….. S2,255

S3,0, S3,1,…….. S3,255

S4,0, S4,1,……... S4,255

Steps to Generate Sub Keys:

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. And also this string also consists of the hexadecimal digits of pi (less the initial 3).

2) XOR P1 with the first 32 bits of the key, XOR P2 with second which is 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycles the process through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; For example, if A is a 64-bit key, then AA, \ AAA, etc., are equivalent keys.)

III. BLOCK DIAGRAM OF DATA ENCRYPTION

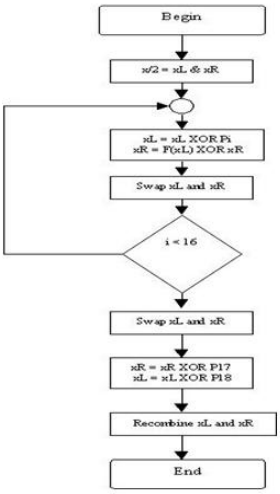

Figure 3:- Block Diagram of Data Encryption.

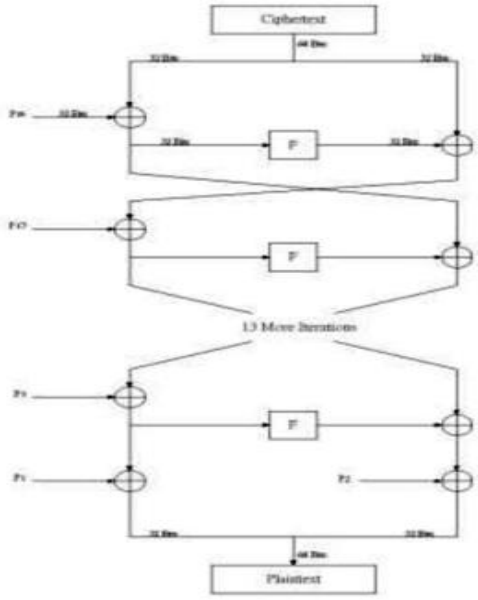

Figure 4:- BLOCK DIAGRAM OF DATA DECRYPTION

IV. FUNCTION F

Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, x. Divide x into two 32-bit halves:

xL, xR

For i = 1to 16: xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.) xR = xR XOR P17

xL = xL XOR P18 Recombine xL and xR

V. BLOCK DIAGRAM OF DATA DECRYPTION

Decryption is exactly the same as encryption, except that P1, P2 ..... P18 are used in the reverse order. F = ((S1[a] + S2[b] mod 232) XOR S3[c]) + S[d] mod 232

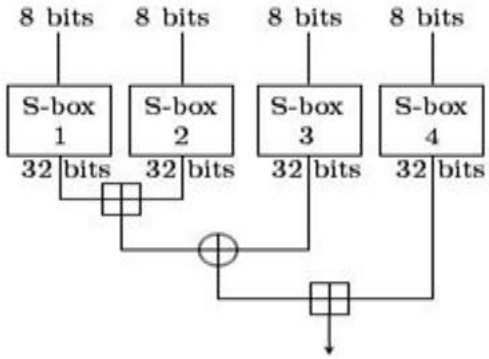

Figure 5:- FUNCTION F

VI. WORK IN FIELD OF BLOWFISH ALGORITHM

According to paper "Blowfish Algorithm Josef Steinberger , and Karel Ježek ". Ms Neha Khatri – Valmik, Prof. V. K Kshirsagar Dept. of Comp. Science & Engg. Govt. College of Engg. Aurangabad, India. Apr. 2014

In this paper the author has discussed Blowfish algorithm,

that it is a variable-length key block cipher. And in this he have described in details the working of the blowfish algorithm and applications where the blowfish algorithm is used. For this paper we get the idea regarding the process which is adapted in the encryption and decryption using the blowfish algorithm. The information which we get from this paper are as follows, the key size which is used for encryption and in the decryption process and rounds which are performed in the data encryption and final output which we get from that.

Another paper is IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB, Pia SinghProf. Karamjeet Singh"
This paper is about the encryption and the decryption of the images using a secret-key block cipher called 64-bits Blowfish designed in order to increase the security and also to the improve performance. In this paper they have taken up an image. Firstly they obtained the matrix and pixels of the chosen image & then they followed the process of encrypting the image matrix [7] using blowfish algorithm. According to this paper, they have shown the original image, an encrypted image and the decrypted image in the final outcome. The text is also hidden in the image using a specific key and image which is hidden with a data is encrypted and decrypted by the 32 bit iteration loop. This paper provides idea about the encrypting and decrypting of images.
Another paper is "A Survey on Cryptography Algorithms" Maulik P. Chaudhari and Sanjay R. Patel.
This paper discusses in details the requirement of the cryptographic algorithm in the field of the information security. In this paper the author has discussed in details plaintext attack[7] against a reduced-round variant of blowfish that is made easier by the use of weak key.
Blowfish is more secure and fast processing algorithm. But in this paper the author also identified some problem in the existing Blowfish algorithm i.e. the blowfish weak keys produces "bad" S-boxes.
Another paper is "Superiority of Blowfish Algorithm, Pratap Chnadra Mandal"
This paper provides a proper comparison between the four most common and used symmetric key algorithms: DES, the 3DES, the AES and also the Blowfish. And the comparison is also made on the basis of these parameters: rounds block size, key size, and the encryption / decryption time, also the CPU process time in the form of throughput and power consumption [8]. These results show that blowfish is better than other algorithm.

VII. CONCLUSION

In last we can say that, Blowfish has not any known security weak points so far it can be considered as an excellent type of standard encryption algorithm. And it also takes much less time in the processing than any other encryption techniques. Also all types of the image sizes and also the format that can be encrypted (.jpg, .bmp). By using this algorithm, lower correlation & higher entropy can also be achieved.
.

REFERENCES

[1] Himani Agrawal and Monisha Sharma "Implementation and analysis various symmetric cryptosystems " in indian Journal of Science and Technology in Vol. 3 No.12 (Dec 2010) ISSN: 0974- 6846.pp.1173-1176.
[2] Jawahar Thakur, Nagesh Kumar,"DES,AES andBlowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011), pp.6-12
[3] Shanta, yoti Vashishtha on " Evaluating the performance of Symmetric Key Algorithms: AES(Advanced Encryption Standarand DES (Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ,pp.43-49
[4] Monika Agrawal,Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques"International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882.
[5] Ms NehaKhatri – Valmik and Prof. V. K Kshirsagar ,"Blowfish Algorithm",IOSR Journal of Computer Engineering (IOSR-JCE),e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83,Apr. 2014
[6] Pia SinghProf. Karamjeet Singh, "IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013,ISSN 2229-5518
[7] Maulik P. Chaudhari and Sanjay R. Patel,A Survey on Cryptography Algorithms,International Journal of Advance Research in Computer Science and Management Studies,Volume 2, Issue 3, March 2014,ISSN: 2321-7782
[8] Pratap Chnadra Mandal,Superiority of Blowfish Algorithm,International Journal of Advanced Research in Computer Science and Software Engineering

