iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: V Month of publication: May 2017

DOI:

www.ijraset.com
IC Value: 45.98

Volume 5 Issue V, May 2017
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A new Approach of Blow fish Algorithm in the Network System

Lepakshigoud.T[1], Dr. Nagaraj B Patil[2], Annapurna.T[3], Dr .K.S.R Sridhar[4]
[1]Visvesvaraya Technological University, Belagavi, Karnataka, India,
[2]Government Engineering of College, Raichur, Karnataka, India,
[3,4] Ballari Institute of Technology and Management, Ballari, Karnataka, India

Abstract:-This paper is about encryption and decryption of the text, image, audio, video using a single key with 64 bits block cipher which is an improved the security from source to destination in the network system this algorithm will be used as a key size from 32 bits to 448 bits. This performance and security level is the main used for the transfer data to other in the network. In the algorithm to evaluate the encryption or decryption speed of the data increased in the network. The method to use for the data transfer from source to destination, it provides high quality encryption and decryption, and also high security because length of key is more so this algorithm good for the network system.

Key words: Algorithms, Blowfish, Cryptography, Network system.

I. INTRODUCTION

Network system is admiring day by day in our life. The widespread for using wired and wireless networks makes the need for protection of user information. Encryption and Decryption algorithm plays an important role for information security. Encryption is the process of transforming plain text data into the cipher text (secure data) in order to reveal its meaning. Decryption is the reverse of the Encryption process in which we retrieve the original plain text from the cipher text. There are many Encryption algorithms which are developed and are used for information security. They are categorized into mainly two types depending upon the type of security keys. The two types are symmetric and asymmetric encryptions system. In symmetric /private encryption only one key is used to encrypt or decrypt the data. Strength of the symmetric encryption depends upon the size of the key. For the same algorithm, encryption using the longer key is tough to break than one using smaller key. In a symmetric / public encryption two keys are used, one is used to encrypt and other is used to decrypt the data [3].

It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [1], [3].DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size).Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [2], [3]. 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [3].Blowfish is block cipher 64-bit block that can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is license-free, and is available free for all users. Blowfish has variants of 14 rounds or less.[7].

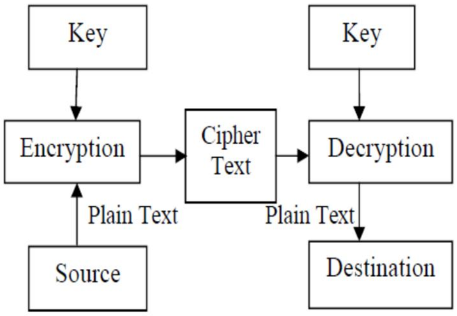


Fig. 1 explains the process of cryptography.

II. BLOWFISH ALGORITHM

The Blowfish algorithm is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish *Algorithm* is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher [4]. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

A. Feistel Networks

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:

1) Split each block into halves
2) Right half becomes new left half
3) 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.
4) Note that previous rounds can be derived even if the function *f* is not invertible.

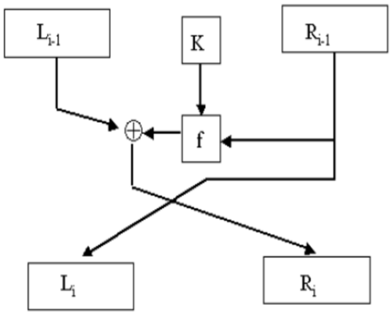


Fig 2**:** Feistel Networks

B. The Blowfish Algorithm

1) Manipulates data in large blocks
2) Has a 64-bit block size.
3) Has a scalable key, from 32 bits to at least 256 bits.
4) Uses simple operations that are efficient on microprocessors

E.g. exclusive-or, addition, table lookup, modular- multiplication, it does not use variable-length shifts or bitwise permutations, or conditional jumps. Employs pre computable sub keys, on large-memory systems, these sub keys can be pre computed for faster operation. Not pre computing the sub keys will result in slower operation, but it should still be possible to encrypt data without any pre computations.

Consists of a variable number of iterations.

For applications with a small key size, the trade-off between the complexity of a brute-force attack and a differential attack make a large number of iterations superfluous [8,9]. Hence, it should be possible to reduce the number of iterations with no loss of security (beyond that of the reduced key size).

1) Uses sub keys that are a one-way hash of the key.
2) This allows the use of long passphrases for the key without compromising security.
3) Has no linear structures that reduce the complexity of exhaustive search.
4) Uses a design that is simple to understand. This facilitates analysis and increase the confidence in the algorithm. In practice, this means that the algorithm will be a Feistel iterated block cipher.

C. Description of The Algorithm

Blowfish is a variable-length key, 64-bit block cipher.
The algorithm consists of two
parts: a key-expansion part and a data- encryption part.
Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes.
Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words.
The only additional operations are four indexed array data lookups per round.
Sub keys: Blowfish uses a large number of sub keys.
These keys must be pre computed before any data encryption or decryption.
The P-array consists of 18 32-bit sub keys:

P1, P2,..., P18.
_ There are four 32-bit S-boxes with 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.

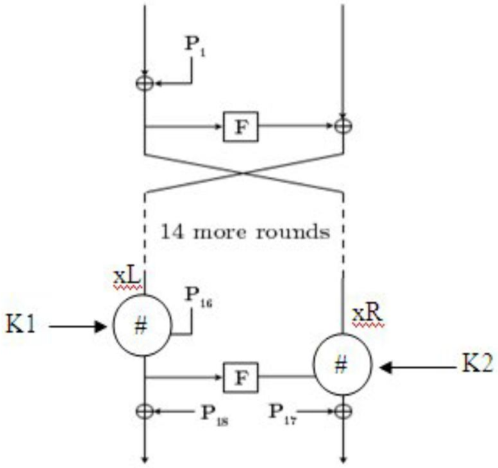


Fig 3: Blow fish each round action

1) Encryption

Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
Finally, recombine xL and xR to get the ciphertext.
5 of 7, Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

III. IMPROVED FOUR STATE OPERATIONS

To increase the security and key space, that makes the encryption algorithms more robustness to the intruders, a new manipulation bits process has been added in by using different truth table for manipulation bits process work on 4- states (0,1,2,3) , while the traditional binary process (XOR) work on (0, 1) bits only. The symbol # has been used to refer to the operator that execute this process use truth tables that shown in fig.4.The new operation needs 3 inputs, the first one specify the table number that should be used to calculate the result among the 4 tables, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result. Here, example for # operation, this operation need 3 inputs, first one specify the table number that should be used to calculate the result among the four truth tables as shown in Table 1, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result this result is in 16 digits. Input in 32 bit binary format 1001011101010010101001111010001001 which is converted into the number 2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1

Input 1: 0 1 3 0 1 2 2 3 1
Input 2: 3 2 2 1 0 1 2 1 1
Input 3: 1 0 0 2 1 3 2 1 2
Result: 3 0 2 3 1 2 2 2 2

#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Fig 4: The truth tables for the # operation

IV. PROPOSED ALGORITHM OF A BLOWFISH

This research proposed a new improvement to the Blowfish algorithm. The proposed improvement makes use of the new operation defined in the previous section, operation (#) applied during each round in the original Blowfish algorithm, and where another key is needed to apply this operation, this key may come in binary form and convert to a 4-states key. Here, originally Blowfish algorithm linear cryptanalysis and differential cryptanalysis attacks are heavily depends on the S-box design. Consequently, multiple keys will be used in each round of the original Blowfish, the first key Ki will be used with the ***f*** function. The second key will be the first input to the # operation, the second input will be the output of the ***f*** function, and the third input to the # operation will be the value Li, Algorithm shows the three 32-bits input to the # operation ,and the 32-bits output, with places needed to convert these 32- bits to 16-digits. These three inputs to the # operation should be firstly converted from 32 bits to a 16 digits each may be one of four states (0,1,2, 3), i.e., each two bits converted to its equivalent decimal digits. Algorithm of modified data encryption standard with 4 state operations

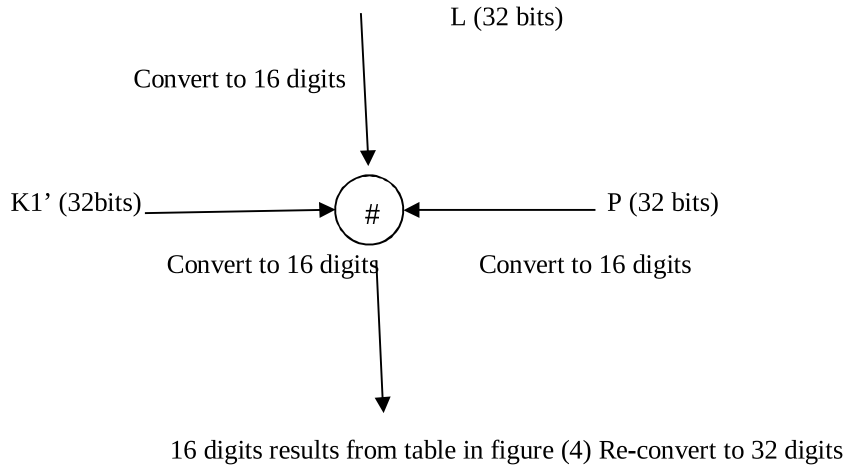


Fig 5: Design of Modified Blowfish algorithm

For example, the binary number will be converted to the digit number.

10 01 01 11 01 01 00 10 10 10 01 11 10 10 00 10 01 → 2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1

Algorithm of modified blowfish algorithm with 4 state operations:

Input: Plaintext $m_1 \ldots m_{64}$, 64 bits
Key: k_1, $k_2 \ldots\ldots\ldots k_{448}$ bits,
X÷x into ‘2’ 32 bits halves,
xL, xR, then, for i=1 to 16,
xL= xL XOR Pi
xR = F(xL) XOR xR, Swap xL and xR
After 16th round, swap xL & xR, again to undo the last swap,
Then, xR=xR XOR P17 and xL= xL XOR P_{18}

Finally, recombine xL & xR to get the cipher text

E g: Show the how the encryption and decryption operations results will be according to apply the (#) operation.

xL	=	01 10 00 10 11 10 01 11 10 10 10 01 01 11 00 10
Pi	=	10 10 01 11 01 01 11 01 10 10 11 11 01 10 00 10
K_1	=	11 10 11 01 01 10 10 00 11 01 11 00 11 01 01 10

4-State, 6-digits numbers

Pi’	=	1 2 0 2 3 2 1 3 2 2 2 1 1 3 0 2
xL’	=	2 2 1 3 1 1 3 1 2 2 3 3 1 2 0 2
K_1’	=	3 2 3 1 1 2 2 0 3 1 3 0 3 1 1 2

Then the (#) operations applied according to tables in figure the results of encryption will be New xL=2 2 0 1 2 1 0 1 1 0 0 1 1 1 0 2 If we reverse the whole operations, we will get the initial which is the result of the decryptions operations that equal to the original data.

K1'	=	3 2 3 1 1 2 2 0 3 1 3 0 3 1 1 2
Pi'	=	1 2 0 2 3 2 1 3 2 2 2 1 1 3 0 2
New xL	=	2 2 0 1 2 1 0 1 1 0 0 1 1 1 0 2
xL	=	2 2 1 3 1 1 2 3 2 3 0 3 2 0 2 1

V. CONCLUSION

This information resources are increased cryptography will continue to increase in a security mechanism in the network system. The network for banking, shopping, and business, benefits and services delivery distributed processing and government applications will use improved for access control and data security in the network system. The blowfish algorithm is now considered to be secure for applications through network by adding more key, modified functions implementation and replacing the XOR operations as a new operation as proposed by this to give more robustness to blowfish algorithm its stronger security, more efficiency of the cryptography and fast process from source to destination in the network system.

REFERENCES

[1] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."Dr. Dobb's Journal, March 2001, PP. 137-139.

[2] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."IBM Journal of Research and Development, May 1994,pp. 243 -250.

[3] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP. 58-309.

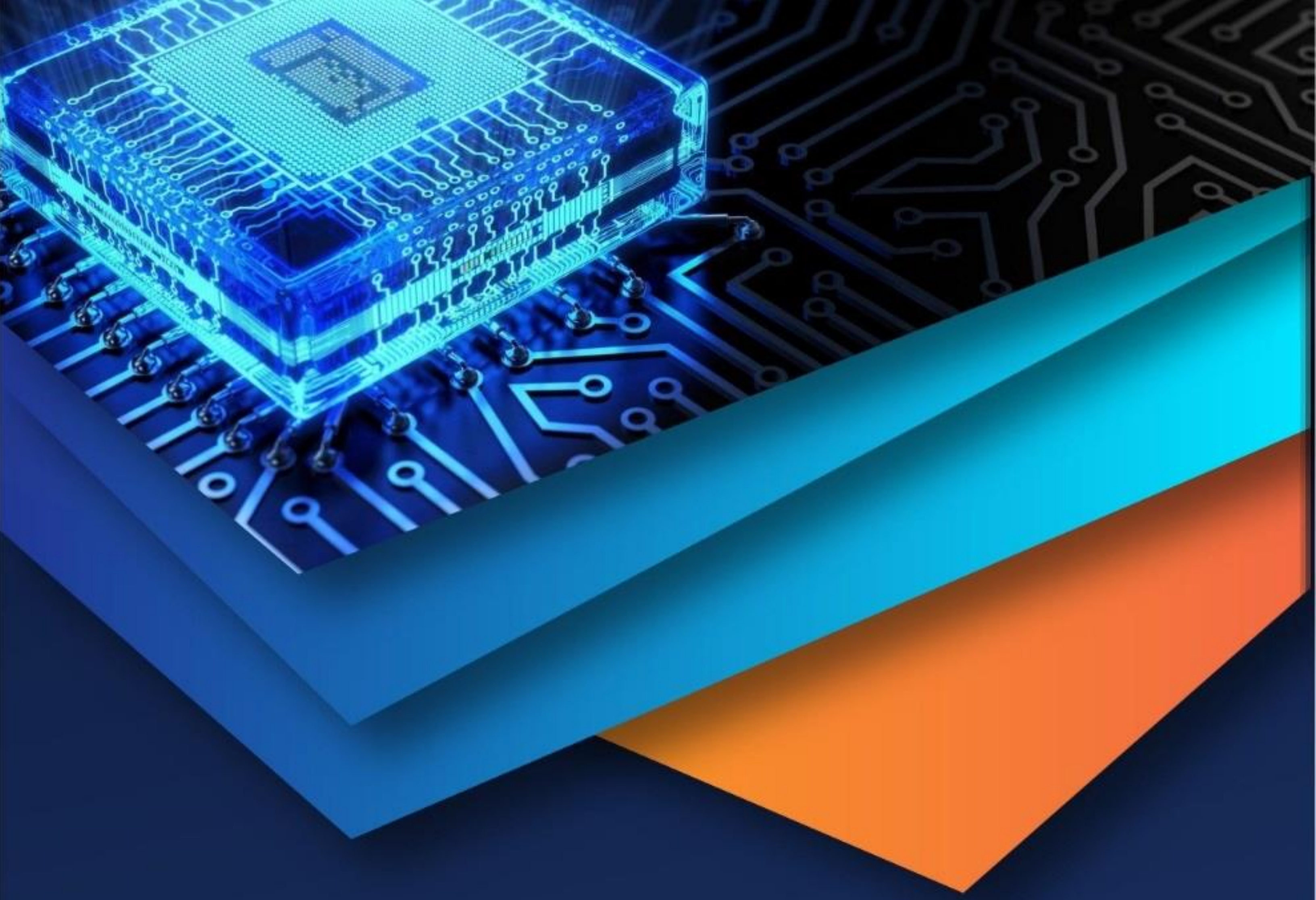
[4] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[5] Lepakshi goud.T,“ Dynamic routing with Security using a Blowfish Algorithm in the multiple Organizing system”, IJAEST, vol No.4,issue No 1, 2011,1-9.

[6] B. Schneier, Applied Cryptography, John Wiley and Sons , New York,1994

[7] Irfan.Landge1, Burhanuddin Contractor2, Aamna Patel3 and Rozina Choudhary4 ‘’Image encryption and decryption using blowfish algorithm’’ World Journal of Science and Technology 2012, 2(3):151-156ISSN: 2231 – 2587.

[8] Shah Kruti R., Bhavika Gambhava ‘’ New Approach of Data Encryption Standard Algorithm’’ International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY