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
www.iosrjournals.org

Blowfish Algorithm

Ms NehaKhatri – Valmik[1], Prof. V. K Kshirsagar[2]
Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India.
Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India.

***Abstract**: Blowfish is a popular security algorithm that was developed by Bruce Schneier in the advent of the year 1994. The algorithm works on the same line as DES and it consumes block coding with blocks of a size of 64 bit. Blowfish became quite popular after its advent, just because Bruce Schneier[1] himself is one of the most famous cryptology expert and above this the algorithm is non patented, open source freely and freely available for use and modifications.*
Blowfish is a 64-bit block cipher with a variable-length key. It defines 2 distinct boxes: S boxes, a P box and four S boxes [3]. Taking into consideration the P box P is a one-dimensional field with 18 32-bit values. The boxes contain variable values; those can be implemented in the code or generated during each initialization. The S boxes S1, S2, S3, and S4 each contain 256 32-bit values.
***Index Terms:** blowfish, encryption, security, algorithm, cryptography*

I. INTRODUCTION

Encryption algorithms are divided in two categories, symmetric key encryptions and public key encryptions. Symmetric algorithms [3], such as Blowfish, use the exactly the same key for encryption and decryption. This can be conveyed like a password that needs to be kept secret from everyone other than sender and receiver of the message. Public key encryption algorithms [5] use two keys, one for encryptionand another for decryption. The key used for encryption, the "public key" need not be keptsecret. The sender of the message uses that public key to encrypt their message, and the recipientuses their secret decryption key, or "private key", to read it. In a sense, the public key "locks" themessage, and the private key "unlocks" it: once encrypted with the public Key, nobody exceptthe holder of the private key can decrypt the message. RSA is a popular public key encryptionalgorithm.

1.1 The Blowfish Algorithm

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key toboth
Encrypt and decrypt messages. Blowfish is also a block cipher [5], meaning that it dividesa message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.

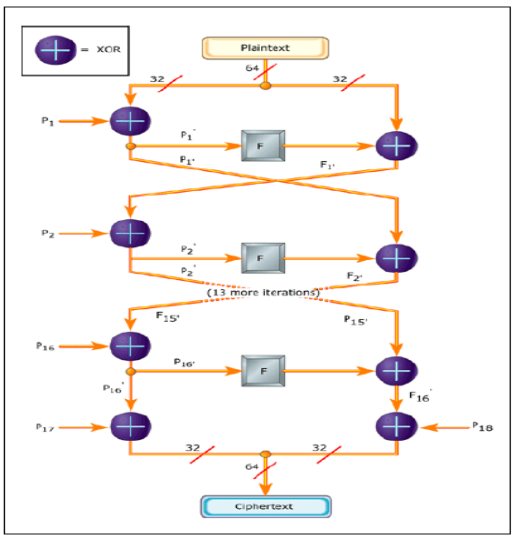

Figure 1: *Blowfish algorithm*

Blowfish consists of two parts: key-expansion and data encryption. During the key expansion stage, the inputted key is converted into several sub key arrays total 4168 bytes. There is the P array, which is eighteen 32-bit boxes, and the S-boxes, which are four 32-bit arrays with 256 entires each. After the string initialization,

the first 32 bits of the key are XORed with P1 (the first 32-bit box in the P-array). The second 32 bits of the key are XORed with P2, and so on, until all 448, or fewer, key bits have been XORedCycle through the key bits by returning to the beginning of the key, until the entire P-array has been XORed with the key.Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to geta 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits ofoutput (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to geta new 64 bit block. Replace the next values in the P-array with the block. Repeat for all thevalues in the P-array and all the S boxes in order.

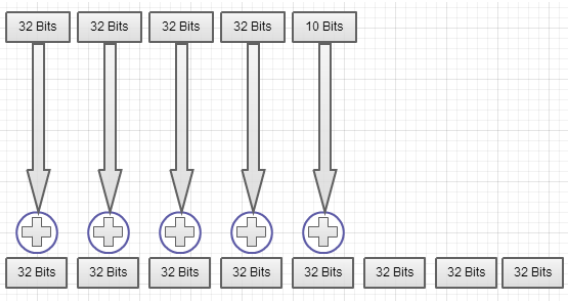

Figure 2.*XORing bits once the key has been traversed through once*

Encrypt the all zero string using the Blowfish algorithm [1], using the modified P-array above, to geta 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits ofoutput (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to geta new 64 bit block. Replace the next values in the P-array with the block. Repeat for all thevalues in the P-array and all the S boxes in order.

II. Literature Survey

2.1 Types of Cryptography

Encryption algorithms are classified in two broad categories- Symmetric key Cryptography and Asymmetric Key Cryptography.

2.1.1 Symmetric Key Cryptography

In symmetric Cryptography the key that is used for encryption is similar to the key used in decryption. So the key distribution has to be made prior to the transmission of information. The key plays a very important role this cryptography since the security directly depends on the nature of the key length etc. There are various symmetric key algorithms such as DES &AES.

2.1.2 Asymmetric Key Cryptography

In Asymmetric Cryptography, two different keys are used for encryption and decryption they are public and private. The public key is available to anyone on the network; those who want to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can decrypt the cipher text through his/her own private key. Private Key is kept secret from the others. Symmetric Encryption Algorithm is faster as compared to Asymmetric key algorithms. The memory requirement of Symmetric algorithm is less than asymmetric.

2.1.3 DATA ENCRYPTION STANDARD (DES)

DES (Data Encryption Standard) is the first encryption standard recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM in 1974 and adopted as a national standard in 1997.

DES is a 64-bit block cipher under 56-bit key. The algorithm processes with a permutation of sixteen rounds block cipher and a final permutation. DES application is very popular in the commercial, military, and other domains. DES standard is public & the design criteria used are classified.

2.1.4 ADVANCED ENCRYPTION STANDARD (AES)

AES was invented by scientists named Joan and Vincent Rijmen in the year 2000. AES makes use of the Rijndael block cipher, Rijndael key and block length can be of 128, 192 or 256-bits, If both the key-length and block length are 128-bit. Rijndael performs 9 processing rounds. If the block/key is 192-bit, it will perform 11 processing rounds & for 256-bits, Rijndael performs 13 processing rounds.

Each processing round involves the following four steps:

1. Substitute bytes – It uses an S-box to perform a byte by byte substitution of the block,
2. Shift rows – It is simple permutation,
3. Mix column – It is a substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix and
4. Add round key – It is the key for the processing round is XORed with the data.

III. Proposed System

This system basically uses the Blowfish encryptionalgorithm [1] to encrypt the data file. This algorithm is a 64-bit block cipher with a variable length key. This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement. It is a 64 bit block cipher and itis fast algorithm to encrypt the data. It requires 32 bitmicroprocessor at a rate of one byte for every 26 clock cycles.

It is variable length key block cipher up to 448 bits. Blowfish contains 16 rounds.

Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round Feistalnetwork [3].

Plain text and key are the inputs of this algorithm. 64 bit Plain text is taken and divides into two 32bits data and at each round the given key is expanded & stored in 18 p-array and gives 32bit key as input and XOR ed with previous round data.

Functionality is to divide a 32-bit input into four bytes anduses those as indices into an S-array. The lookup results arethen added and XOR ed together to produce the output. At16th round there is no function .The output of this algorithmshould be 64bit cipher text.

3.1 ALGORITHM STEPS:

It is having a function to iterate 16 times of network. Each round consists of key-dependentpermutation 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 lookup tables for each round.

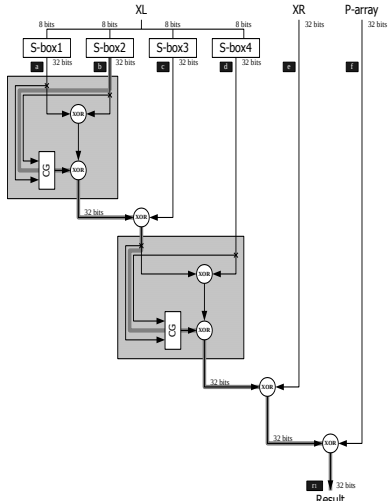

Fig 3. DFG of the loop

Algorithm

Divide x into two 32-bit halves: xL, xR
For i = 1to 32:
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

For decryption, the same process is applied, except that thesub-keys Pi must be supplied in reverse order. The natureof the Feiestelnetwork [1] ensures that every half is swappedfor the next round (except, here, for the last two sub-keysP17 and P18).

IV. CONCLUSION

The proposed algorithm of the Blowfish can achieve efficient data encryption up to 4 bits per clock. In this design, we avoid I/O limited constraint by modifying the I/O from 64 bits to 16 bits. The proposed architecture should satisfy the need of high-speed data encryption and can be applied to various devices respectively.

In this paper we discussed Blowfish algorithm, it is a variable-length key block cipher. It is suitable for applications where the key do not change often, like a communications link. It is faster than DES.
Blowfish is a 16 pass block encryption algorithm that is never broken.
BLOWFISH is used frequently because:

- It has been repeatedly tested&found to be secure.
- It is fast due to its taking advantage of built-in instructions on the current microprocessors for basic bit shuffling operations.
- It was placed in the public domains.

Acknowledgment

First and foremost, I would like to thank my guide, Prof. VivekKhirsagar, for his guidance and support. I will forever remain grateful for the constant support and guidance extended by guide, in making this paper. Through our many discussions, he helped me to form and solidify ideas. The invaluable discussions I had with him, the penetrating questions he has put to me and the constant motivation, has all led to the development of this project.

REFERENCE

[1] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc. 1996
[2] The homepage of description of a new variable-length key, 64-bit block cipher http://www.counterpane.com/bfsverlag.html
[3] Patterson and Hennessy, "Computer Organization & Design: The Hardware/ Software Interface", Morgan Kaufmann, Inc. 1994
[4] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994, Proceedings, Springer-Verlag,1994, pp.191-204.
[5] S. Vaudenay, "On the Weak Keys in Blowsh," Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, 1996, pp. 27-32.
[6] P. Karthigai Kumar and K. Baskaran. 2010. An ASIC implementation of low power and high throughput blowfish crypto algorithm. Microelectron. J. 41, 6 (June 2010), 347-355.
[7] TingyuanNie; Chuanwang Song; XulongZhi; , "Performance Evaluation of DES and Blowfish Algorithms," Biomedical Engineering and Computer Science (ICBECS), 2010 International Conference on , vol., no., pp.1-4, 23- 25 April 2010.
[8] TingyuanNie; Teng Zhang; , "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Conference , vol., no., pp.1-4, 23-26 Jan. 2009

About Author

Ms NehaKhatriValmik perceived her BE IT degree in Information Technology from Peoples Education Society's College of Engineering under Dr.BabasahebAmbedkar University, Aurangabad, India, in 2008. She is currently pursuing post graduate degree at Govt College of Engineering, Aurangabad. Her interests lie in various subjects like Digital Electronics, Computer Networks, Digital Image Processing. Ms NehaKhatriValmik as a teaching experience of more than 4 years and she is currently working as Assistant Professor at Jawaharlal Nehru Engineering College under the Department of Computer Science & Engineering, Aurangabad.