

SECURE MULTICASTING USING BLOWFISH ALGORITHM

Mrs. Veena Jose
M.Phil Scholar,

School of Information Technology and Science,
Dr. G.R.D College of Science,
Coimbatore, Tamilnadu, India

Ms. C. Divya
Assistant Professor,

School of Information Technology and Science,
Dr. G.R.D College of Science,
Coimbatore, Tamilnadu, India

Abstract— The communication mechanism of one to many is termed as multicasting. This technology is helpful in situations where group communication is to be performed. In today's world, security is the main concern where communication is performed through a network. In this context, Blowfish algorithm works fine. It is a symmetric algorithm, means the sender and receivers should use the same key for encrypting the data as well as decrypting. The data to be transmitted is converted into cipher text and this is sent to all the receivers. The cipher text is generated with the help of a key and the same key will be used by all the receivers to decrypt the encrypted text. Class D addresses are used for multicasting.

Keywords— Multicasting, Symmetric, Security, Blow Fish, Plain Text, Cipher Text.

I. INTRODUCTION

1.1 Multicasting

Multicasting means sending data from one to many. This type of communication is good in situation where a group of members having common needs to be communicated. The group members may be in different places, so communication is to be done through networks. The network has the threat of attackers always. So the data to be communicated through the network can not be transmitted in the plain text format as it will be easy for the attackers to identify the secret information. So the original data is to be represented in some other format. How the data is converted into the other format is to be made secret and this should be known only to the authorized people.

1.2 Cryptography

The data transmitted through the network is to be secured from unauthorized users. For protecting the data, it is converted from its plaintext format to another format. The conversion of data from the plain text format into another form is known as encryption. The converted text is known as cipher text. At the receiver side, this ciphertext is to be converted back to the plain text format. The whole process is termed as cryptography.

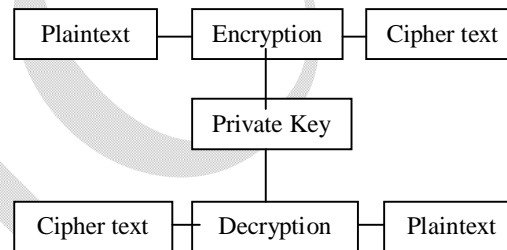
1.3 Symmetric and Asymmetric Key Cryptography

The *cryptography* is done with the help of a key. There are two types of cryptography – Symmetric-key cryptography and Asymmetric-key cryptography.

Symmetric key cryptography is also known as private key cryptography. In this encryption mechanism, the sender and receiver share the same key for encryption and decryption. The key that is shared is known as private key.

The *private key* is to be made confidential, because if this key is accessed by any unauthorized party, they can easily access the encrypted text.

Sender

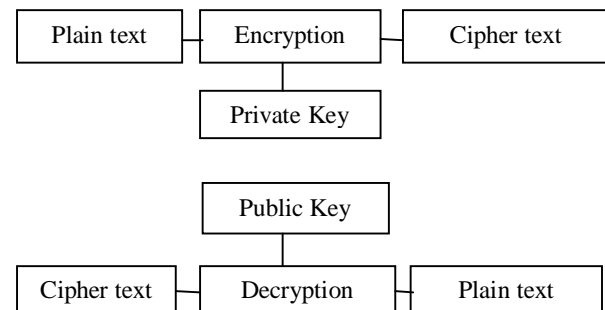


Receiver

Fig 1: Symmetric Cryptography

Asymmetric-key cryptography is also known as public key cryptography. In this method, sender will be encrypting the data with a private key and receiver will be decrypting the data with a public key. The private key is private to the sender and the public key is known to the public.

Sender



Receiver

Fig 2: Public Key Cryptography

II. LITERATURE SURVEY

Compares three encryption algorithms namely DES, AES and Blowfish. These algorithms are analysed by considering certain performance metrics such as execution time, memory required for implementation and throughput. Based on the experiments, it has been concluded that the Blowfish is the best performing algorithm among the algorithms chosen for implementation [1].

Compares the encryption algorithms DES (Data Encryption Standard), 3DES (Triple DES), BLOWFISH and AES (Rijndael). Based on the performance analysis of these algorithms under different hardware and software platform, it has been concluded that the Blowfish is the best performing algorithm among the algorithms under the security against unauthorized attack and the speed is taken into consideration [2].

Focuses on multicasting which has been widely utilized for delivering messages from one sender to multiple recipients. Nowadays in some applications like video-conferencing systems, the messages delivered via multicasting should be available to authorized recipients only. Therefore, secure multicasting becomes an important design issue in a distributed environment. To achieve secure multicasting, the goal is aimed at finding a way to distribute the new key securely and efficiently [3].

Based on [4], data sent from a source to multiple users are to be secured from unauthorized users. Before sending data, the data from the source is to be encrypted with the help of a key and the authorized destinations will be using the key to decrypt the data. The Encryption and decryption is performed with the help of algorithms - AES (Advanced Encryption Standard) and RC4 (Rivest Cipher 4). Encryption Time, Memory usages output byte and battery power are the major issues of concern.

Based on [5], the comparison of different symmetric encryption algorithms are as follows: RC2: Block Cipher with 64-bits block and a variable key size that range from 8 to 128 bits. It is vulnerable to related key attack. DES: Symmetric algorithm which uses one 64-bit key. 3DES: This symmetric algorithm uses 64-bit block size with 192 bits of key size. Encryption level is 3 times that of DES [6][7].

It is slower than other block cipher methods. AES algorithm is a replacement of DES which can be used in non-military information security application by US government agencies. It can encrypt data blocks of 128 bits using symmetric keys 128, 192 or 256. It has variable key length of 128, 192 or 256 bits with default value -256. RC6: Block cipher derived from RC5. This algorithm is designed to meet the necessities of the AES. RC6 has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits.

Blowfish: Symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable –

length key from 32 bits to 448 bits. Blowfish is unpatented and license-free and is available free for all uses. This algorithm gives better Performance and no attack is known to be successful against it.

III. METHODOLOGY

The data to be transmitted is kept in a file and this file is encrypted using Blowfish algorithm. This encrypted file is communicated among the group members, so that they can decrypt the file using the same key which is known to them. The unauthorized people, if they try to access the file, they won't be able to receive the original data without the key.

3.1 Multicasting

Here, the multicasting is implemented with the help of class D addresses in classful addressing mechanism. The network communication based on IPv4 reserves class D addresses for implementing multicasting. This is a 32 bit address and a group will be uniquely identified with this address. The socket programming with class D address helps to implement multicasting operation. When one member of this group sends some information, the other group members who listen to this socket will be able to receive the information. The file encrypted using the Blowfish algorithm is transmitted to multiple receivers. The sender generates the key and this is shared with the receivers. Receivers should also use the same key for decrypting the file [8][9].

3.2 Blowfish algorithm

In order to maintain secrecy of this information, the symmetric key cryptographic mechanism – Blowfish algorithm is used.

Working of Blowfish Algorithm

Blowfish works in a block of 64 bits with a variable key size upto 448 bits. Blowfish has 2 parts: - Key expansion and data encryption. The given key is converted into several sub key arrays, a total of 4168 bytes. The P arrays which are eighteen 32-bit boxes and S boxes which are four, 32-bit arrays with 256 entries each. All the boxes are initialized with a fixed string [10].

After string initialization, first 32 bit of key are XORed with P1, second 32 bit of the key are XORed with P2 and so on until all the key bits are XORed.

Encrypt the all zero string, using the modified P-array above to get a 64-bit block. Replace P1 and P2 with first and second 32 bit block of the output respectively [13][14].

To get a new 64 bit block, use the 64 bit output as input back to the Blowfish cipher. The next values in the P array are

replaced with the block. The process is to be repeated for all values in the P – array and S- boxes in the order[11][12].

Divide the 64 bit block x into two, 32 bit halves- xL and xR .

For i from 1 to 16:

Perform $xL = xL \text{ XOR } P_i$

$xR = F(xL) \text{ XOR } xR$

swap xL and xR

Next i

Swap xL and xR (The last swap is to be avoided)

$xR = xR \text{ XOR } P_{17}$

$xL = xL \text{ XOR } P_{18}$

Recombine xL and xR

At the end of the 16th iteration, the key will be generated and this key can be used by the sender and receivers to perform encryption and decryption[15][16].

xR is generated by applying Fiestel Function F on xL .

The Fiestel Function F can be defined as:

$$F(xL) = ((S_1 \cdot a + S_2 \cdot b \text{ mod } 2^{32}) \text{ XOR } s_3 \cdot c) + s_4 \cdot d \text{ mod } 2^{32}$$

where a, b, c, d are four 8 bit blocks derived from xL .

The Fiestel function can be represented as :

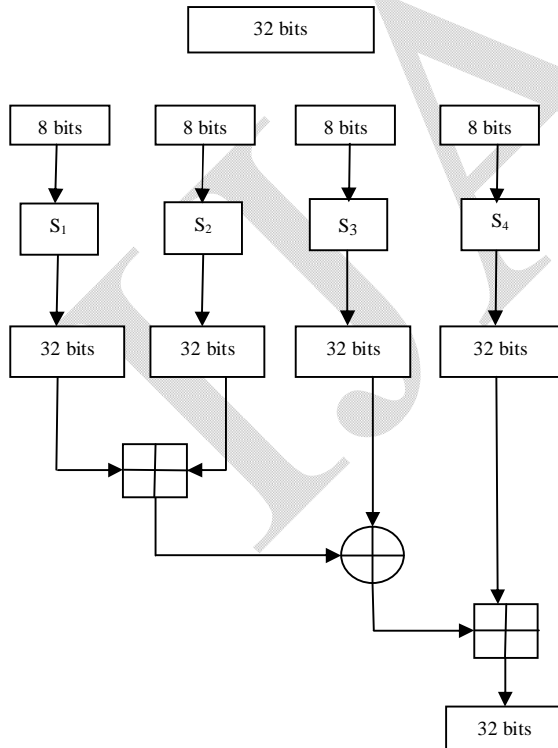



Fig 3: Fiestel Cipher

 denotes addition modulo 2^{32} .

The entire process can be represented as:

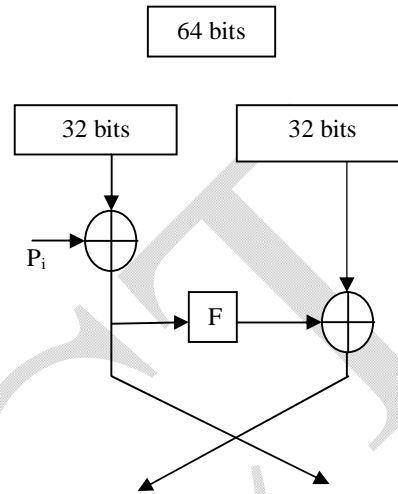


Fig 4: Blowfish algorithm

IV. RESULT

In a group communication, when one group member wants to communicate with others, the sender encrypts the message using the Blowfish algorithm with the help of a key supplied by the sender. This encrypted file is transmitted by the sender to the recipients using the multicast address. The multicast group is formed using Class D address. The sender executes the socket program and the receivers have to listen to this port address, by executing the socket program. The receivers can receive this encrypted file and which can be decrypted using the same key as that of that of the sender which is known to them already.

V. CONCLUSION

Using the Blowfish algorithm, the file to be multicasted is made secret. The secrecy of the file can be maintained as long as the key is not known to the unauthorized users. This works well in applications like military, where the officers have to share the file which contains very confidential information. The main concern of this is the key sharing task. As the network through which the key is to be shared is vulnerable, transmitting the key through the same is having security issues. So there should be some secure mechanism which helps the key to be made highly confidential.

References

- [1] Ramesh A.,Suruliandi A “ Performance analysis of encryption algorithms for Information Security” in <http://ieeexplore.ieee.org>, 10.1109/ ICCPCT .2013.6528957, 2013.
- [2] Verma O.P, Agarwal R, Dafouti D, Tyagi S “ Performance Analysis of Data Encryption Algorithms” <http://ieeexplore.ieee.org>, 10.1109/ ICECTE CH, 2011.5942029, 2011.
- [3] Kuen-Pin Wu, Shanq – Jang ruan, Feipei Lai, Chih- Kuang Tseng “ On Key distribution in secure multicasting “ in <http://ieeexplore.ieee.org>, 10.1109/LCN.2000.891029, 2000
- [4] M.K Kiran Kumar, B.N.V MadhuBabu,K.Nageswararao, “ Providing Security for Data in Multicasting Using Encryption” in International Journal of Engineering Inventions, ISSN : 2278-7461, www.ijejournal.com, Volume 1,Issue 2,September 2012.
- [5] Pratap Chandra Mandal, “ Superiority of Blowfish Algorithm” in International Journal of Advanced Research in Computer Science and Software Engineering,ISSN:2277 128X,www.ijarcse.com,Volume 2, Issu 9,September 2012
- [6] Jawahar Thakur, Nagesh Kumar, “DES,AES and Blowfish: 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
- [7] Monika Agarwal, Pradeep Mishra, “ A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm” in International Journal of Engineering and Advanced Technology, ISSN:2249-8958, Volume 1,Issue 6,August 2012
- [8] Mingyan Wang, Yanwen Que, “The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm”, International Forum on Computer Science – Technology and Applications, Vol 2,pp. 24-28,2009.
- [9] Savita D. Patil, Ashish T. Bhole, “ The Design and Implementation of Passwords Management System using Blowfish Cryptographic Algorithm” International Journal of Technology and Engineering System (IJTES), Vol 2,No. 2,pp. 193-196,Jan-March 2011.
- [10] Krishnamurthy G.N,Dr.V.Ramaswamy,Leela G.H, Ashalatha M.E, “ Performance Enhancement of Blowfish and CAST-128 Algorithms and Security Analysis of improved Blowfish Algorithm using Avalanche Effect”, IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No.3, March 2008.
- [11] B.Schneier, The Blowfish Encryption Algorithm, July 22, 2009 from <http://www.schneier.com/blowfish.html>.
- [12] Bruce Schneier, “Applied Cryptography – Protocol, Algorithm and Source Code in C”, Second Edition, John Wiley & Sons,2008.
- [13] Afaf M.Ali Al-Neaimi, Rehab F.Hassan, “New Approach for Modifying Blowfish Algorithm by using Multiple Keys”, IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No.3, March 2011.
- [14] Daa SALama Abd Elminaam, Hatem Mohamed Abdul Kader and Mohiy Mohamed Hadhoud, “Evaluating The Performance of Symmetric Encryption Algorithms”, International Journal of Network Security, Vol.10,No.3, pp.216-222,May 2010.
- [15] Simar Preet Singh and Raman Maini, “Comparison of Data Encryption Algorithms”, International Journal of Computer Science and Communication, Vol.2,No.1,pp.125-127, January – June 2011.
- [16] A.H. Al-Hamami, M.A. Al-Hamami and S.H. Hashem, “A proposed Modifications to Improve the Performance of Blowfish Cryptography Algorithm”, First National Information Technology Symposium (NITS 2006), 5-7 Feb.2006.