International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol 1 Issue 4 August 2015

Exchange of Encrypted Information Using Block Cipher Cryptography

Pritesh Kumar Agnihotri[1], Dr. Pratima Gautam[2]
Faculty of Information Technology, AISECT University, Bhopal, M.P., India[1]
Faculty of Information Technology, AISECT University, Bhopal, M.P., India [2]
dhawan.agnihotri@gmail.com[1], pratima.manit @yahool.co.in[2]

Abstract— In this Paper we proposing an encryption method in which transfer of files between two peer occur efficiently. This model propose downloading and uploading a file in encrypted form. This model proposed practical approach to transfer data efficiently and show the enhanced performance of system for better throughput. This proposed method predicts the performance of the system and computes the values of the technical parameters that achieve a desired performance. It increases the performance of network by reducing file transfer delay. This method is easy to implement and also provide good security for the information exchanged. This method is useful in peer to peer network for providing security as well as greater throughput.

Keywords- Peer-to-peer network, Encryption, Decryption, cryptography, Block cipher, throughput.

I. INTRODUCTION

This paper is proposing an efficient method that provides strong security for data transfer and uploading/downloading files. The proposed algorithm is based on the concept that users should be awarded for offering uploading and downloading files in minimum time. In this paper we dealt with the issue of how to design an algorithm regardless of the issue of how to implement this algorithm on a different networks. The paper describe this with the help of both theoretical and practical approach. Then, shows that the model is generally applicable to any computer network. We comment on how to implement it using either a local, or a global approach. Another important aspects of the paper is to analyze the performance of a networks practically. The analysis of the algorithm is based on set of equations that are used to predict the system's performance. The analysis is take place under a wide range of conditions, and tuned the parameters of the scheme. This algorithm is an efficient in terms of the performance and time. And also is very easy to use, it enforces users to be fair, and it can be implemented in a number of ways.

II. PROPOSED WORK

Encryption Approach used: - Here we are using Symmetric key Cryptography technique that use trivially related often identical, cryptographic keys for both encryption and decryption. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information.

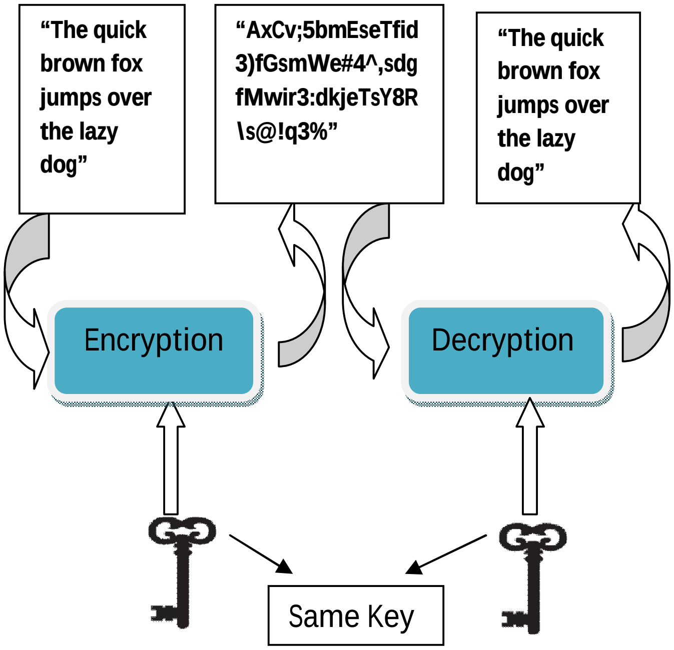

"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid 3)fGsmWe#4^,sdg fMwir3:dkjeTsY8R \s@!q3%"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same Key

Fig 1 :- Symmetric Key Cryptography

Why Symmetric key Approach is better for Encryption and Decryption:-

- The encryption process is simple.
- Keys for symmetric-key ciphers are relatively short.
- Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
- Symmetric-key ciphers can be composed to produce stronger ciphers.
- Symmetric-key encryption is perceived to have an extensive history.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.

Steps Before data transfer:-

Initially, the Peer-1 sends a Synchronization request to the Peer-2 for Communication.

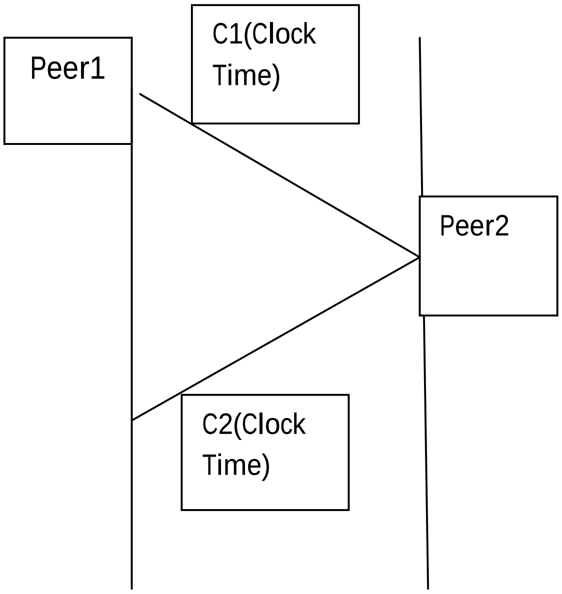


Fig. 2:- Time Synchronization

After verifying the acknowledgement time Peer-1 sends the link stable signal to The Peer-2 indicating that it is ready for the data transfer. In turn the Peer-2 also send link stable acknowledgement to indicate that it is also ready for data transfer.

Steps followed for First time data Transfer:-

- The Peer-2 calculates the time required to transfer the message from Peer-1 to Peer-2 (T1) i.e. propagation delay and reserved this time for the future use.
- Then the Peer-2 sends its clock (C2) and (T1) to the Peer-1.
- Peer-1 calculates the message transfer time from Peer- 2 to Peer-1 (T2) and sends it to Peer-2 and saves it for use in Encryption Process.
- After knowing the C1, C2, T1, T2 Peer-1 Encrypts the message by the help of key f(X) =C1+C2+T1+T2 and send to the Peer-2.
- In the Peer-2 Side since all the required values are already known, as a result the message is decrypted and converted to plaintext.

Steps Followed For Further Data Transfer:-

- First of all the Peer-1 encrypts the Message with f(x) =C1+C2+T1+T2 and sends this message to the Peer-2.
- The Peer-2 calculates the time required to transfer the message from Peer-1 to Peer-2 (T1) i.e. propagation delay and reserves this time for the future use.
- Peer-2 now have a knowledge of all the required things for decrypting the message i.e. C2, C1=C2-T1, T1, T2 now the client will Decrypts the message by the key f(x) =C1+C2+T1+T2 and get the Plaintext message.
- If the Peer-1 wants to send more messages then are replies to the Peer-2 otherwise it will disconnect the link.

Steps for Key Generation:-

Construct a Encoded matrix (3*3) and fill that matrix with C1, C2, T1 and T2 in the following manner:-

$$E = \begin{matrix} C1 & C2 & T1 \\ T2 & C1 & C2 \\ T1 & T2 & 1.0 \end{matrix}$$

Where,

C2 = System clock time of Peer-2 computer

C1 = System clock time of Peer-1 computer

T2 = Time take to transfer a message from Peer-2 to Peer-1.

T1 = Time taken to transfer a message from Peer-1 to Peer-2.

Calculate F(X) = C1 + C2 + T1 + T2

- Multiply the F(X) with the Encoded matrix.

$$F(x) * \begin{bmatrix} C1 & C2 & T1 \\ T2 & C1 & C2 \\ T1 & T2 & 1.0 \end{bmatrix}$$

- Now concatenate the values of F(X) and matrix contents in the following way to generate the key for encryption. Key (F1(x))= F(X) * C1 + F(X) * C2 + F(X) * T1 + F(X) * T2 + F(X) * C1+ F(X) * C2+F(X) * T1+F(X) * T2+ F(X) *1. (42 bit key in binary of one entry of matrix). Take the M1 matrix and find the transpose it.
- Matrix (EM1) = {(Encoded Matrix)}^{T}
- The above matrix EM1 now be multiplied with the F1(x) resulting in the generation of Final key Matrix

$$\mathrm{KM} = \mathrm{F1(x)} * \mathrm{EM1}$$

Characteristics of Proposed Key:-

- Our proposed key is 200 bits which is larger this will enhance the security aspect of this algorithm and make them more secure than other encryption Algorithms.
- The Encryption key having larger size but resulting in shorter encryption times, shorter encrypted messages and shorter transmission times.
- There is no constraint that only one key which is providing simple structure.

Step for Proposed Encryption Algorithm:-

- Select first 200 bits form Input file.
  InFile(A.txt)→ 200 Bits
- Arrange these 200 bits into 20 X 10 Matrix.
  200→ P [20] [10]
- Select a key of 200 Bits.
- Arrange these 200 bits of key into 20 X 10 Matrix.
  200→ K [20] [10]
- Select Plain Text matrix & sub divided it's into 8 sub matrix of 5 X 5 matrix
  P1 [5] [5], P2 [5] [5]…………P8 [5] [5]
- Select Key matrix & sub divided it's into 8 sub matrix of 5 X 5 matrix.

  K1 [5] [5],K2 [5][5]……..K8[5] [5]

- Perform Logical Operation.
- Perform XOR between Plain Text matrix and Key matrix.

$$P1 \oplus K1 \Rightarrow P1'$$

$$P2 \oplus K2 \Rightarrow P2'$$

•
•
•

$$P8 \oplus K8 \Rightarrow P8'$$

Again combine these sub matrix into a single matrix

- Combine P1', P3', P5', P7' into 10 X 10 matrix
- Combine P2', P4', P6', P8' into 10 X 10 matrix
- Perform Right Shift Operator Function- Apply right shift by 3 bits move the bits in the operand right by the specified number of bit positions.
- Now finally combine these two matrix into 20 X 10 cipher matrix.
- Exit.

Characteristic of Proposed Encryption:-

- Proposed algorithm having no complex structure.
- Easy to understand: Every user can easily understand what is happening in this algorithm but no one can find out how it's happening.
- Efficiency of proposed algorithm is very high due to its simple architecture.
- Reliability: proposed algorithm is very reliable
- Security: Proposed algorithm providing very high security because it's strongly support to confusion and diffusion property.

Advantages of P2P Network: -In p2p networks are the following benefits:

- Cost efficiency
- Organically Scaling
- No single point of failure
- Privacy
- Green Technology

Result Analysis:-I am using .Net implementation to present an evaluation system. For encryption time and decryption time of the known cryptographic algorithm with my proposed cryptography algorithm, it is necessary to describe the detailed evaluation method, as illustrated in Figure-7. Here I am taking only one evaluating modes to find whether the key and the plain text have impact on time consuming of cryptographic algorithms: DPSK (different plaintext in the same key).

For our experiment, we use a laptop Pentium® Dual-Core CPU T4400 @2.20Ghz and 32-bit Operating System, in which performance data is collected. In the experiments, the laptop encrypts a text data and calculates encryption time and decryption time. We are using some parameters for execution time which is shown in table 1and in table 2 respectively. Here I am doing compare execution time of encrypting plain text on different existing cryptographic algorithms with my proposed cryptography algorithm. During processing, the content of the plain text and the key are both written by the random number. For DPSK evaluation mode, there are two parameters: the number of evaluated plain text and the size of evaluated plain text, where the number of evaluated plain text is the number of text file that are generated randomly and the size of evaluated text file can be chosen from two kinds that mention above. In this mode, I do n cycles (that is, the number of the evaluated plaintexts). In each cycle, same plaintexts are repectively encrypted by "AES", "Blow-Fish", "RC6", "DES" and Proposed Algorithm (PA) by copying them. Finally, the outputs of the evaluation system are execution time and decryption time, and measured in numeric form. Actually, for an encryption algorithm, the execution time not only depends on the algorithm's complexity, but also the key and the plain text have certain impact.

Result Comparison in Tabular Form: **-** In this we are going to represent our result in the form of table.

In table1 and table 2 we are showing encryption time and decryption time in the form of hours then minute and then second (hh:mm:ss). After comparison the results that were obtained can be well represented in form of table 1-2 that describes the encryption time, decryption time.

Table-1
Encryption Time Comparison of various Encryption Algorithms with Proposed Algorithms

Plain Text File Size	AES	BFS	RC6	DES	PA
16 KB	0:00:09	0:00:7	0:00:04	0:00:12	0:00:02
46 KB	0:00:10	0:00:10	0:00:05	0:00:13	0:00:03
90 KB	0:00:12	0:00:12	0:00:03	0:00:17	0:00:04
187 KB	0:00:17	0:00:17	0:00:12	0:00:20	0:00:08
560 KB	0:00:35	0:00:35	0:00:30	0:00:39	0:00:26
1.66 MB	0:01:32	0:01:30	0:01:27	0:01:36	0:01:20

Table-2: Decryption Time Comparison of various Encryption Algorithms with Proposed Algorithms

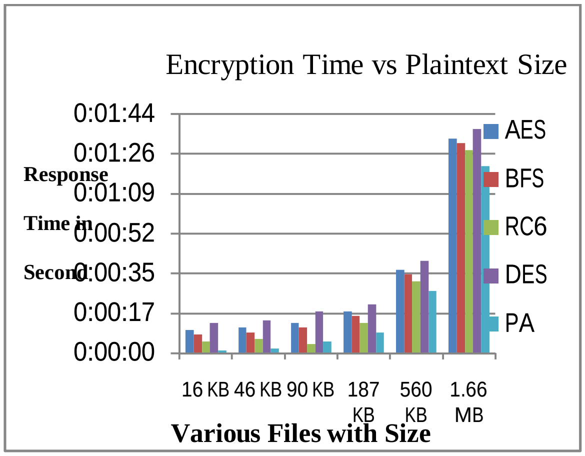
Plain Text File Size	AES	BFS	RC6	DES	PA
16 KB	0:00:09	0:00:7	0:00:04	0:00:12	0:00:02
46 KB	0:00:10	0:00:08	0:00:05	0:00:13	0:00:03
90 KB	0:00:12	0:00:10	0:00:03	0:00:17	0:00:04
187 KB	0:00:17	0:00:15	0:00:12	0:00:20	0:00:08
560 KB	0:00:35	0:00:33	0:00:30	0:00:39	0:00:26
1.66 MB	0:01:32	0:01:30	0:01:27	0:01:36	0:01:20

From both tables it's clear that our proposed algorithm is producing batter result as compare other algorithm in term of execution time. We have also notice that RC6 is better other then Blow Fish (BF), AES and DES.

Graphical Representation of Comparison:-

Representing result comparisons in the form of graph.

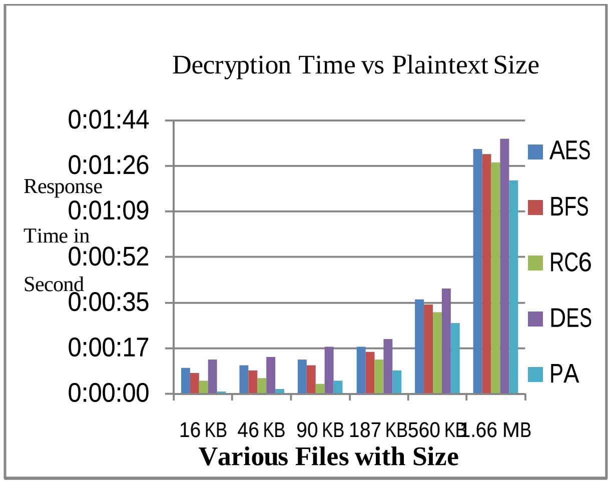
Encryption Time: The following Graph is drawn form Table-1 to reveal it. In this graph, the evaluated mode is DPSK, and the fixed size of the evaluated Plain text. At this point, the key length of all Encryption algorithms is 128-bit, which is less than from our proposed algorithm (PA).



Graph 1:-Encryption Time Comparison of Existing Algorithms with Proposed Algorithm

Decryption Time: The following graph is drawn from the Table-2 to reveal it. In this graph, the evaluated mode is DPSK, and the fixed size of the evaluated Plain text. At this point, the key length of all Encryption algorithms is 128-bit, which is less than from our proposed algorithm (PA).

Some typical results obtained by the evaluation system can be found in Table 1-2 and Graphs. That the Proposed Algorithm (PA) is better than other selected algorithms in DPSK evaluation mode firstly. Finally, it is not difficult to find that, in contrast with those Tables, the larger the key length is, and the bigger security as well as CPU utilization. This means that an eavesdropper can have a complete copy of the algorithm in use, but without the specific key used to encrypt that message, it is useless. Generally speaking, the security of cryptographic algorithm usually depends on the size of plain text, keys and structure of algorithm, while the evaluation model based on random number generating mechanism that can verify that the security of cryptographic algorithm not only depends on the size of plain text and keys.



Graph 2:-Decryption Time Comparison of Existing Algorithms with Proposed Algorithm

Another point can be noticed here, that Proposed Algorithm has good performance in terms of power consumption and throughput when compared with existing algorithm.

III. CONCLUSION

In this paper we studied a simple algorithm that provides strong security for cooperation in file sharing in computer networks. We are showing a logically cum mathematical model that describes the system's dynamics and which can be used for parameter tuning and performance prediction. We demonstrated the effectiveness of the algorithm via experiments. Future work consists of performing larger scale experiments, implementing the scheme in an operational P2P network, and extending our analytical methodology to compute other important performance metrics, e.g. the improvement on the expected upload and download delays and response times. Furthermore we will include more parameter to evaluate results on large scale like power consumption, memory utilization, throughput, security setting. Finally we will enhance design and implementation portion of our proposed algorithm stronger and we will work for globalization in future.

References

[3] Chithra Selvaraj & Sheila Anand "Peer profile based trust model for P2P systems using genetic Algorithm" published in Springer Science and Business Media, LLC, 13 September 2011.

[4] Georgios Exarchakos & Nick Antonopoulos "A peer-to-peer system for on-demand sharing of capacity across network applications" published in Springer Science and Business Media, LLC, 24 August 2011

[5] R. Steinmetz and K. Wehrle. What is this peer-to-peer about? In Peer-to-Peer Systems and Applications, volume 3485 of LNCS, pages 9–16. Springer-Verlag Berlin Heidelberg, 2005.

[6] A. Oram. Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2001.

[7] R. Steinmetz and K. Wehrle. Peer-to-peer-networking and computing. In Informatik-Spektrum, volume 27(1), page 5154. Springer-Verlag Berlin Heidelberg, 2004.

[8] J. Eberspacher and R. Schollmeier. First and second generation of peer-to-peer systems. In Peerto-Peer Systems and Applications, volume 3485 of LNCS, pages 35–56. Springer-Verlag Berlin Heidelberg, 2005.

[9] Napster. http://free.napster.com/. Last visited on Dec 30th 2007.

[10] BitTorrent. http://www.bittorrent.com. Last visited on Jun 30th 2007.

[11] Gnutella. http://www.gnutella.com. Last visited on Dec 30th 2007.

[12] Stefan Gotz Klaus Wehrle and Simon Riech. Distributed hash table. In Peer-to-Peer Systems and Applications, volume 3485/2005 of LNCS, pages 79–93. Springer-Verlag Berlin Heidelberg, 2005.

[13] R. Schifanella. A Legal and Efficient Peer-to-Peer Market Place: Exploiting Fairness and Social Relationships, PhD Thesis. University of Torino, 2006.

[14] James Li "A Survey of Peer-to-Peer Network Security Issues" http://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/index.html

[15] Allan Friedman, L Jean Camp "Peer-to-Peer Security".

[16] Baptiste Prˆetre "Attacks on Peer-to-Peer Networks" Dept. of Computer Science Swiss Federal Institute of Technology (ETH) Zurich Autumn 2005.

[17] Sedat Akleylek, Levent Emmungil, Urfat Nuriyev "A Modified Algorithm For Peer to Peer Security" published in Appl. Comput. Math. 6 (2007), no.2, pp.258-264

[18] Jian Liang, Naoum Naoumov, Keith W. Ross "The Index Poisoning Attack in P2P File Sharing Systems " published in 25th IEEE International Conference on Computer Communications. Proceedings In INFOCOM 2006.

[19] Li Gong. Jxta: A network programming environment. IEEE Internet Computing, 5(3):88–95, 2001.

[20] Li Gong. Jxta: A network programming environment. IEEE Internet Computing, 5(3):88–95, 2001.

[21] Megha Ojha, Priyank Dubey "Sharing of Encrypted Information in a Network Using Block Cipher Cryptography" published in International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013.

[22] Tech Law Advisor. News article. January 3, 2005. RIAA or Overpeer Seeding P2P Files with Spyware? http://techlawadvisor.com/2005/01/riaa-oroverpeer-seeding-p2p-files.html

[23] Computer Reseller News. June 28, 2004. Spyware support costs run into millions http://www.crn.vnunet.com/news/1156261

[24] Mika Suvanto "Privacy In Peer-to-Peer Networks" HUT T-110.551 Seminar on Internetworking 2005-04-26/27

[25] B.Udhaya and J.Jeysree "Implementation of Reputation Exchange Protocol in Peer to Peer System" published in International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3 No. 3 Mar 2011