Comparison of Symmetric Algorithms

P. Princy[1]
[1] Department of Computer Science and Engineering
[1] Bharathidasan University, Trichy

Abstract- *The data being carried via a network is insecure to various types of passive and active attacks. So the data security becomes a challenging problem in network data transmission. Cryptography algorithms encrypt data and provide a protection against the data trespassers and secure the network communication. Symmetric key algorithms shared the secret keys to sender and receiver's side. In this M.Phil thesis, a new algorithm called as ATB (Attribute Based Encryption) is proposed to reduce a transaction time in encryption and decryption process. Also a detailed analysis and comparison is made on Blowfish, DES, IDEA, and ATB symmetric key algorithms. The analysis and comparison is based on parameters Key size, Encryption time, Decryption time, Throughput and End-End delay for different format files.*

Keywords*:* Symmetric key algorithms, Blowfish, DES, IDEA, and ATB.

I. INTRODUCTION

1.1 NETWORK SECURITY

Privacy is a sore subject that touches everybody. Regular techniques to secure guard secrecy are: sensitive data is unlimited (e.g., assessment grades, financial accounts). With the Internet, the computer can be used comparable to a telephone or like a post office, with the drawback t connected to the network could have receiver to the data. This is why, particularly with computers, privacy is significant.

1.2 CRYPTOGRAPHY MECHANISM

Cryptography is a technique of caring secure information from unnecessary individuals by converting it into worthless form. It is an art of renovate the messages to make them secure and unchanged against security attacks. Cryptography is used for secure communication in the occurrence of third parties to continue information securities such as discretion, authentication, data integrity, access control and non-repudiation.

In the present era of Information Technology security is the key aspect while transmit classified information over the unsecured network. To beat this problem we necessitate some encryption techniques which can save from destruction our secret information. Cryptographic Algorithms supply end-end information security over unsecured communication networks. There are number of encryption techniques which can be habitually divided into two categories: Symmetric Key Encryption and Asymmetric Key Encryption. In Symmetric key Encryption same key is used to encrypt and decrypt data, while Asymmetric Key Encryption uses two different keys; public and private key. Symmetric algorithms are of two types Block Ciphers and Stream Ciphers.

For this a number of encryption techniques are offered which are used to keep left from the information robbery. In new days of wireless communication, the encryption of data plays a most important point in securing the data in online transmission focuses mostly on its security across the wireless. Different encryption techniques are used to maintain the secret data from undemocratic use. Encryption is a very common method for promoting the information security.

1.3 CLASSIFICATION OF CRYPTOGRAPHIC TECHNIQUES

The expansion of encryption is moving towards a approaching of infinite potential. Everyday new methods of encryption techniques are exposed. This research holds some of those recent presented encryption techniques and their comparison.

1.3.1 RC2

RC2 is a irregular key size block cipher which uses 64 bits blocks. It was premeditated to change DES. It is measured to be three times faster than DES. It accepts a changeable length key from 0 bytes to the greatest string length that the computer system can maintain. It uses 16 rounds of one type and two rounds of other type. The encryption speed of the algorithm is independent of its key size. It was proposed to replace DES.

1.3.2 DES (Data Encryption Standard):

Data Encryption Standard (DES) developed by IBM and normally used. Triple-DES is a interchange which uses DES thrice for ciphering data. DES operates with 56 bit key on 64 bit blocks of data. It is susceptible to security attacks and can be easily retrieved.

Data Encryption Standard is a block encryption algorithm available by NIST (National Institute of Standard and Technology). It encrypts data blocks of 64 bits each by captivating a 56 bit key. It uses same key for encryption and decryption. A 16 cycle Feistel system is used with a generally 56 bit key permuted into 16 48-bit sub keys, 1 for each cycle. To decrypt, the similar algorithm is used but the order of round keys are in overturn order.

1.3.3 AES

AES stands for Advanced Encryption Standard. It replaced DES as the authorized standard of US National Institute for Standards and Technology. AES operates on variable key sizes and variable block sizes of 128, 192 or 256 bits. Proper to the number of permutations and combinations in AES causal to its higher complexity, AES has a advanced security as compared to DES.

1.3.4 IDEA

It stands for International Data Encryption Algorithm. IDEA is a block cipher which operates on a 64 bit plaintext blocks. It is based on the thought of substitution permutation organization that uses block cipher of 64 bit plaintext and a key with128 bits. The algorithm used for encryption and decryption is the identical. The plaintext of 64 bits is separated into four parts. These four parts became the input for first round which consists of combination operations from special algebraic groups. The three algebraic operations which are performed in each round are XOR, Addition modulo 216 and multiplication modulo 216+1. All these operations work on 16 bit sub blocks. There are eight such rounds. The last step is an output transformation which produces four cipher text blocks of 16 bits each. These blocks are jointed to produce the 64 bit cipher text block.

1.3.5 BLOWFISH

It is a rapid administration substitute for DES and IDEA. It adopts key lengths in the array of 32 to 448 bits and block size of 64 bits. Blowfish was housing by Bruce–Schneider as an substitute to the presented encryption algorithms. It is a symmetric key block cipher which uses 64 bit block size and a changeable key coverage from 32 bits to 448 bits. It has 16 or less rounds. It is the greatest block ciphers inhabited till date. No attack is known to be unbeaten against Blowfish.

II. OVERVIEW OF ATTRIBUTE-BASED ENCRYPTION (ATB)

It is considerable to protected data that is uploaded in to different social sites are stored online. Attribute Based Encryption (ATB) is a talented cryptographic method that achieves a fine grained data access control. It gives a way of important access policies based on a variety of attributes of the requested user, scenario, or the data object.

Mostly, Cipher text Policy Attribute Based Encryption (CP-ATB) enables an encrypted to define the quality set over a creation of attributes that a decrypted requires to attain in order to decrypt the cipher text and realize it on the contents. Thus each user with a different set of attributes is permitted to decrypt different pieces of data per the security policy.

Although there are various techniques implemented for the encryption of the data in the network, one such technique is IBE. Identity Based Encryption is a technique which is based on the encryption of the data using personality of users. The idea is to make a key pairs which is based on the identity of the users and the encryption and decryption of the data is achievable using these identities.

In Attribute-Based Encryption an encryption will connect encrypted data with a set of attributes. An qualifications will concern users unlike private keys, where a user’s secret key is related with an access structure over attributes and reflects the access policy attributed to the user. In an ABE system, the various keys are generated based on the attribute of the users and also the personal cipher text.

III. RELATED WORK

Ritu Tripathi, Sanjay Agrawal performed a work “COMPARATIVE STUDY OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY TECHNIQUES” The cryptography techniques and various algorithms are used to make available the needed security to the applications. This research provides a comparison between some symmetric and asymmetric techniques. The factors are achieving a flexibility and security, an effectiveness, which is a face of researchers. In this research produce the better solution to the symmetric key encryption and the asymmetric key encryption is provided. The tunability and key length is higher at the Asymmetric encryption technique .The key length is high in asymmetric encryption algorithm to break the code is complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power expenditure algorithm hence speed is fast in the Symmetric key encryption is viewed as good. In conclusion, in the symmetric key encryption techniques the blowfish algorithm is specified as the better solution. In the Asymmetric encryption technique the RSA algorithm is more secure since it uses high prime number for key generation.

Chaitali Haldankar1, Sonia Kuwelkar "IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM" As a result, many algorithms have been proposed in order to tolerate strong security at lower cost. In this research we study the cryptographic algorithms like AES and Blowfish and compare different parameters and then do further implementation as the implementation of encryption or decryption algorithm is the most essential ingredient of the secure communication. The assessment is performed in terms of encryption speed, the CPU consumption with time and the battery power consumption. The experimental results point out the efficiency of the algorithms. More the throughput, more the velocity of the algorithm and less will be the power consumption. Finally in this research conclude that Blowfish is the best of all.

Mitali1, Vijay Kumar performed a work "A SURVEY ON VARIOUS CRYPTOGRAPHY TECHNIQUES" Security of wireless networks is main aspect and the process of cryptography plays an imperative function to provide the security to the wireless networks. There are various cryptography techniques both symmetric and asymmetric. The research is done on some of the more popular and interesting cryptography algorithms currently in use and their pro's and con's are also discussed. This research provides a reasonable performance comparison between the various cryptography algorithms of data packets. In this research we analyze the encryption and decryption time of various algorithms on different settings of data. This research presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points.

IV. PROPOSED WORK

ATTRIBUTE BASED ENCRYPTION (ATB)

In calculation to the field and equation of the curve require G a base point of prime order on the curve; n is the multiplicative order of the point G. Alice creates a key pair, consisting of a private key integer dA randomly selected in the interval [1, n-1] and a public key curve point QA=dA*G. Use * to denote elliptic curve point multiplication by a scalar.
For Alice to sign a message m follows these steps:

1. Determine e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1.
2. Let Z be the Ln leftmost bits of e, where Ln is the bit length of the group order n.
3. Select a random integer k from [1, n-1].
4. Determine the curve point(x1, y1) = k*G.
5. Determine r=x1(mod n). If r=0, go back to step 3.
6. Determine s=k-1(Z+rdA) (mod n). If s=0, go back to step 3.
7. The signature is the pair(r, s).

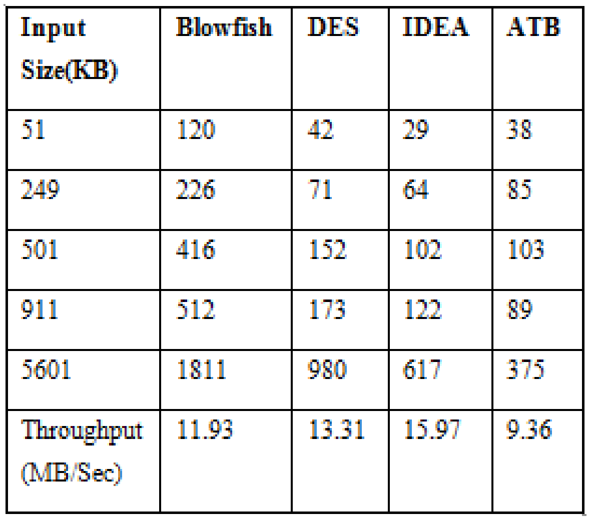
V. SIMULATION RESULTS

In the experiment, the system encrypts a different file size ranges from 51 KB to 12100 KB. In this research, the following factors are used as the performance criteria:

i. Input data (in the form of text, audio and video)
ii. Encryption Time
iii. Decryption Time
iv. Throughput of Encryption of different block ciphers with text, audio & video data
v. Throughput of Decryption of different block ciphers with text, audio& video data
vi. Power Consumption to encrypt different Block Cipher algorithms
vii. Power Consumption to decrypt different Block Cipher algorithms

Throughput Encryption time:

The time which an algorithm takes to exchange plain text to a cipher text is called encryption time. It is defined as total plain text in Megabytes divided by total encryption time of each algorithm.



Input Size(KB)	Blowfish	DES	IDEA	ATB
51	120	42	29	38
249	226	71	64	85
501	416	152	102	103
911	512	173	122	89
5601	1811	980	617	375
Throughput (MB/Sec)	11.93	13.31	15.97	9.36

Table 4.1 Comparisons of Blowfish, DES, IDEA and ATB based on Encryption Time (in Milliseconds)

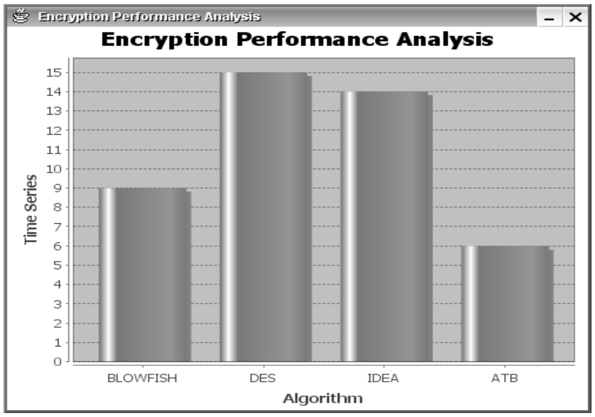


Fig 4.1 performance chart for encryption process

Throughput of a Decryption:

It is defined as total plain text in Megabytes divided by total decryption time of each algorithm. If throughput value of an encryption is increased then power consumption of that encryption is decreased. Similarly if throughput of an encryption is decreased then power consumption of that encryption is increased and hence the battery consumption is also increased.

Input Size(KB)	Blowfish	DES	IDEA	ATB
51	60	20	13	18
249	142	39	32	41
501	237	71	56	59
911	321	123	82	89
5601	1205	480	617	375
Throughput (MB/Sec)	11.91	12.10	14.47	9.28

Table 4.2 Comparisons of Blowfish, DES, IDEA and ATB based on Decryption Time (in Milliseconds)

By analyzing experimental results several points can be concluded. Find that ATB has more power consumption and fewer throughputs than the ATB due to its triple phase characteristics.

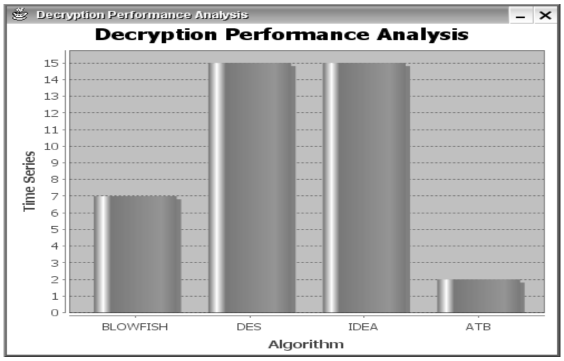


Fig 4.2 performance chart for decryption process

V. CONCLUSION

This research presents a performance and efficiency analysis of different block cipher algorithms (BLOWFISH, DES, IDEA and ATB) of Symmetric Cryptography based on different performance factors. By analyzing experimental results several points can be completed. Find that ATB has more power consumption and fewer throughputs than the DES due to its triple phase characteristics. ATB is faster for smaller sizes of input data as compared to BLOWFISH algorithm because of it has only one P-box for key expansion loaded into memory as compared to BLOWFISH which has one P-box and four S-boxes. Throughput value of BLOWFISH is greater than DES, IDEA and ATB.IDEA having the least throughput value and maximum Power Consumption value as compared to all block ciphers discussed in this project. From the tentative results it is also finished that by taking input data in the form of text, audio as well as video throughput of Encryption and Decryption of all block ciphers discussed here is almost same in all three forms of data. Finally by analyzing Encryption or Decryption time, Throughput and Power Consumption value conclude that ATB has better performance and efficiency than all other block ciphers compared in this project.

REFERENCES

[1] Bruce Schneier .Applied Cryptography, Protocols, Algorithms and Source Code in C..

[2] Behrouz A. Forouzan \Data Communications and Networking.

[3] Shasi Mehlrotra seth, Rajan Mishra \ Comparative Analysis of Encryption Algorithms For Data Communication., IJCST Vol. 2, Issue 2, June 2011

[4] Ali Makhmali, Hajar Mat Jani. Comparative Study On Encryption Algorithms And Proposing A Data Management Structure.INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 6, JUNE 2013 ISSN 2277-8616

[5] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram. COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS \ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

[6] B. Padmavathi1, S. Ranjitha Kumari2 \A Survey on Performance Analysis of DES, AES and RSA Algorithm

along with LSB Substitution Technique. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064Volume 2 Issue 4, April 2013 www.ijsr.net

[7] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader ,Mohly Mohamed Hadhoud, \Evalution the Performance of Symmetric Encryption Algorithms., international journal of network security vol.10,No.3,pp,216-222,May 2010.

[8] Pratap Chnadra Mandal e Superiority of Blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201

[9] J. Wu and F. Dai, “Broadcasting in ad hoc networks based onselfpruning,” In Proc. IEEE INFOCOM, pp. 2240–2250, 2011.

[10] W. Peng and X. Lu, “On the reduction of broadcast redundancy in mobile ad hoc networks,” In Proc. ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 129–130, 2010.

[11] I. Stojmenovic, M. Seddigh, and J. Zunic, “Dominating sets andneighbor elimination-based broadcasting algorithms in wireless networks,”IEEE Trans. on Parallel and Distributed Systems, vol. 13, pp. 14–25, 2012.

[12] M. Khabbazian and V. K. Bhargava, “Localized broadcasting with guaranteed delivery and bounded transmission redundancy,” IEEE Transactions on Computers, vol. 57, no. 8, pp. 1072–1086, 2013.

[13] J. Wu and F. Dai, “A generic distributed broadcast scheme in ad hoc wireless networks,” IEEE Transactions on Computers, vol. 53, no. 10, pp. 1343–1354, 2014.

[14] P. Nand and S.C. Sharma, “ Probability based improved broadcasting for AODV Routing protocol”, “ IEEE International Conference on Computational Intelligence and Communication Networks, 2011.

[15] D. Dembla and Y. Chaba, “ Performance Modeling of Efficient and Dynamic Broadcasting Algorithm in MANETs Routing Protocols”, IEEE International Conference on Computer Research and Development, 2010.