ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

A STUDY AND COMPARATIVE OF CRYPTOGRAPHY TECHNIQUES FOR SECURE OF COMMUNICATIONS

1. P. Sivagami
Asst.Professor
Dept. of Computer Science
D.K.M College for Women
(Autonomous)Vellore.
Mobile No: 9629999132

2. Dr. A. Priya
Asst.Professor
Dept. of Computer Science
Thiruvalluvar University college
Arts and science
Gajalnaikenpatti,Tirupattur.

Abstract: ***In today's world of internet technology that covers especially communication network security is a challenging issue. Hackers try to gain control over our system and steel data from it. To avoid this providing network security is an important task. Cryptography is one such technique which is responsible for secure transmission of the data. And, using cryptographic techniques the security to the information can be provided the main objective of this paper is to study the basic terms used in cryptography its goal and to compare the encryption techniques used in cryptography.***

Keywords: Cryptography, Plain text, Cipher text, Encryption, Decryption, Network security.

1.INTRODUCTION

Cryptography is the study of mathematical techniques related to various aspects of information security, such as confidentiality or privacy, data integrity and entity authentication. It is not the only means of providing information security, but rather one set of techniques. Cryptography systems can be broadly classified into two categories:

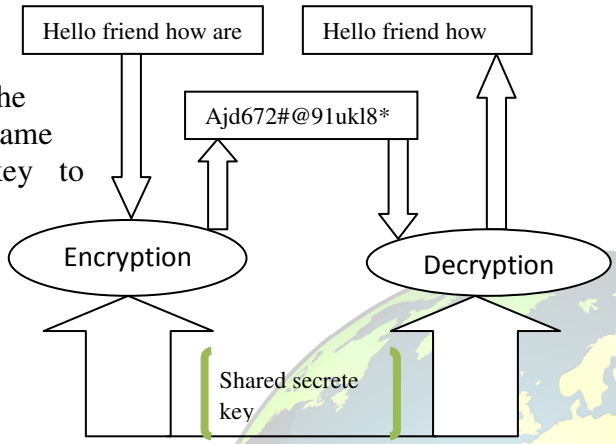
1.Symmetric-key systems: Private Key also known as symmetric cryptography refers to cryptography algorithms which require the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

2. Asymmetric-key systems: Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and other one is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plain text or to verify a digital signature, whereas the private key is used to decrypt cipher text or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions each being the inverse of the other

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both.



2. BASIC TERMS USED IN CRYPTOGRAPHY

2.1 Plain Text

The original message that the person wishes to communicate with the other is defined as Plain the original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Sakthi is a person wishes to send "Hello Friend how are you" message to the person Siva. Here "Hello Friend how are you" is a plain text message.

2.2 Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message.
For example,"Ajd672#@91ukl8*^5%" is a Cipher Text. produced for "Hello Friend how are you".

2.3 Key

A specific string of data that is used to encrypt and decrypt messages, documents or other types of electronic data. Keys have varying levels of strength. Keys having higher numbers of bits are theoretically tougher to break because there are more possible permutations of data bits. (Since bits are binary, the number of possible permutations for a key of x bits is 2x.)
The specific way a key is used depends on whether it's used with asymmetric or symmetric cryptography.

2.4 Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things - an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

2.5 Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

non – readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

3. GOALS OF CRYPTOGRAPHY

3.1 Confidentiality

It ensures that nobody can read the text except the proposed receiver. With this chattel, information is made available only to the authorized persons and is disclosed to unauthorized individuals. When more individuals are drawn in communication, the is enforced by mathematical functions applied to the message being transmitted.

3.4 Non-repudiation

A mechanism that proves that sender has really sent that message.

3.5 Access control

Access control is a property in which only authorized individuals can view the message that is sent. They are capable to do it with the help of a key and decryption technique.

4.ASSESSMENT OF DIFFERENT CRYPTOGRAPHY ALGORITHM

This section describes the recent and most secured cryptographic algorithms that are proposed enable network security are compared and a conclusion is made out of it.With the rapid growth of the internet both the wired and the wireless networks must and should provide security to the data's that is being transmitted. There are different purpose of cryptography is to give assurance that only those individuals can understand the data/information exchanged. It is done with the help of encryption.

3.2 Authentication

The process of providing one's identity is called authentication. It is used to find whether the information is coming from authorized individual or not.

3.3 Integrity

It is a property that gives assurance that the message that is received has not been changed by any unauthorized individuals or in an accidental manner from the original. It

types of cryptographic algorithms found to accomplish this task. A few algorithms amongst them are taken for comparison. Each algorithm has its own pros and cons. The following are the algorithms that are compared for network security. [12] discussed about a method, Sensor network consists of low cost battery powered nodes which is limited in power. Hence power efficient methods are needed for data gathering and aggregation in order to achieve prolonged network life. However, there are several energy efficient routing protocols in the literature; quiet of them are centralized approaches, that is low energy conservation. This paper presents a new energy efficient routing scheme for data gathering that combine the property of minimum spanning tree and shortest path tree-based on routing schemes. The efficient routing approach used here is Localized

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

Power-Efficient Data Aggregation Protocols (L-PEDAPs) which is robust and localized. This is based on powerful localized structure, local minimum spanning tree (LMST). The actual routing tree is constructed over this topology. There is also a solution involved for route maintenance procedures that will be executed when a sensor node fails or a new node is added to the network.

4.1 Diffie-hellman

factors with respect to the fact that solving the discrete algorithm is very challenging, and that the shared key is never itself transmitted over the channel. Drawback of it is the lack of authentication.

4.2 DES

Data encryption standard (DES) is a symmetric key algorithm which was found by IBM in the year 1977. This algorithm uses a key size of 56bits and a block size of 64bits. This algorithm is a block cipher and it uses feistel network to transfer messages. It takes about 16 rounds to convert messages and its network security can be broken by brute force attack. Benefit of this algorithm is that DES has been around a long time, even now no real weakness has been found, the most efficient attack is still found to be brute force attack. It is actually fast in hardware and relatively fast in software. Drawback of the algorithm is as technology is improving there is a possibility to break the encrypted code in DES and as we use private key for cryptography if it is lost we cannot get the readable data at the receiving end.

Diffie-hellman was found by whitfield diffie and martin hellman in the year 1976. This algorithm doesn't have specified key size because it uses key exchange management and has a block size of 64bits. It is a symmetric key cipher and uses common network to transfer messages. It takes nearly 14 round to convert a message and its security is broken by eaves dropping. Benefits of this algorithm is that security

4.3 RSA

Rivest-Shamir-Adleman (RSA) is asymmetric algorithm developed by Ron Rivest, Adi Shamir and Leonard adleman in the year 1977. This algorithm uses a key size greater than 1024bits and its block size depend on the key size that is being used. Block size is often calculated with a formula i.e 1+floor((x-1)/8)' where x is the key size. It is a block cipher and common networks are used to transfer messages. It takes 1 round to convert one message and its security is broken by timing attack. Benefit of this algorithm is that it uses public key to transfer messages and also provides security to digital signatures that cannot be repudiated. Drawback of the algorithm is that even though the public key is safe its speed is comparatively low.

4.4 Blowfish

Blowfish is a symmetry key algorithm was developed by Bruce Schneier in 1993 as an alternate to another encryption algorithm and providing effective data encryption. It has a variable key length up to 448 bits. It has a block size of 64 -bits. In encryption phase, a function is iterated 16 times and the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

encrypted text is obtained using EX-OR operation. Blowfish is a strong encryption algorithm. Benefit especially the password-hashing method used in OpenBSD uses an algorithm derived from Blowfish that makes use of the slow key schedule. Extra computational effort required gives Protection against dictionary attacks Drawback Each pair of users needs a unique, so as number of users increase, key management becomes complicated key. It also has weakness in decryption process over other algorithms. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput.

4.5 AES

Rijndael was selected as the (AES) Advanced Encryption Standard in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in Belgium NIST. This algorithm uses a key size of 128, 192 or 256bits and a block size of 128, 192 or 256bits. It is a rajndael cipher and uses feistel networks to transfer messages. It takes 10, 12 or 14 rounds to convert messages and its security is broken by chosen plain attack. Benefit of this algorithm is that it is more secure and faster in both hardware and software. Drawback of the algorithm is that it needs more processing and requires more rounds of communication when compared to DES.

Table 1. Comparative study of cryptography algorithm

Parameters	Diffie-hellman	RSA	Blowfish	DES	AES
Key size	Uses key Exchange management	1024 bits and above	32 – 448 bits	56 bits	128,192,256 bits
Block size	64 bits	Depends on keysize	64 bits	64 bits	128,192,256 bits
Rounds	14	1	16	16	10,12 or 14
Cipher type	Symmertic cipher	Neither a Stream nor a block	Block cipher	Block cipher	Block cipher
Network type	Common Network	Common Network	Feistel Network	Feistel Network	Feistel Network
Merits	The shared key is never itself transmitted over channel	Only intended user can read the message using their Private Key	Extra computational effort required gives protection against dictionary attacks	No real Weakness has been found	More secure and faster in both hardware and software
Demerits	Lack of	Speed is	users increase,	Possibility	Needs more

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

	authenication	comparatively low	key management becomes complicated key decyption.	to break the encryption code in DEs	processing

6. CONCLUSION

This paper present a comparative study of different key algorithms like AES, DES, Blowfish ,RSA and Diffie-Hellman .Each algorithm has been compared on different set of parameters. From the result it has been found that among the symmetric encryption algorithm, AES and Blowfish are more secure and efficient algorithm. In case of asymmetric encryption algorithm RSA is secure and speed in wireless networks. I would like to conclude by saying that all algorithm either symmetric and asymmetric algorithm all have their own way pros and cons. Each algorithm is unique in its own way and they are useful in real time encryptions. Each one is suitable in different applications, so its depends on the user to select the most appropriate algorithm that is best suited to his needs. Through our analysis on different cryptography algorithms we wish to provide a pathway for future researcher to promote the performance and security of cryptography algorithm.

REFERENCES

[1]William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] W. Stallings. "Cryptography and Network Security", Prentice Hall, 1995.

[3] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, VOL. 2, Issue 7 July 2012,Page 226-233

[4]Zirra Peter Buba & Gregory Maksha Wajiga "Cryptographic Algorithms for Secure Data Communication"in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.

[5]Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of AdvanceFoundation and Research in Computer (IJAFRC),volume 1,issue 6,june 2014, ISSN 2348 –4853.

[6]Ms. Ankita Umale, Ms. Priyanka Fulare, " Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", The International Journal Of Engineering And Science (IJES) ,volume 3,issue 3,page 7-12,2014, ISSN (p): 2319 –1805.

[7]Apoorva, Yogesh Kumar," Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

Engineering & Management (IJAIEM),volume 2, Issue 7,july 2013,ISSN 2319 –4847.

[8]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),volume2,issue 3,may-jun 2012 ISSN: 2248-9622.

[9]S.Abdul. Elminaam, H. M. Abdul Kader, M.M.Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" ,International Business Information Management Association (IBIMA),2009.

[10]M. Abolhasan, T. Wysocki andE. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks,Vol. 2, pp.1-22, 2004.

[11]Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[12] Christo Ananth, S.Mathu Muhila, N.Priyadharshini, G.Sudha, P.Venkateswari, H.Vishali, "A New Energy Efficient Routing Scheme for Data Gathering ",International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Vol. 2, Issue 10, October 2015), pp: 1-4.

[13]Harsh Kumar Verma, Ravindra Kumar Singh "Performance Analysis of RC5, Blowfish and
DES Block Cipher Algorithms", International Journal of Computer Applications, ISSN: 0975 -8887.

[14]Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877 -882.

[15]Shashi Mehrotra Seth, Rajan Mishra," Comparative Analysis Of Encryption Algorithms For
Data Communication", IJCST, Vol. 2, Issue 2, June 2011 pp.192-192.

[16].J. Bhalla, P. Nagrath , "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm," ISSN International Journal of Scientific and Research Publications, Vol. 3, pp.1-6,April 2013.

[17].A.Mousa , "Data Encryption Performance Based on Blowfish," IEEE ELMAR Symposium Zadar, pp.131-134, June 2005.

[18].M. Wang and Y. Que, "The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm," IEEE Computer Science-Technology App. IFCSTA Chongqing, Vol. 2, pp.24-28, December 2009.

[19].N.Palaniswamy, D.Dugar M, D.K. Jain, R. Sarabhoje, " Enhanced Blowfish Algorithm using Bitmap Image Pixel Plotting for Security Improvisation," Education Technology and Computer (ICETC) Shanghai, Vol.1, pp.V1-533 -V1-538, June 2010.

[20].National Institute of Standards and Technology, "Clipper Chip Technology," 30 Apr 1993.

[21].R.Rivest, A.Shamir, and L.Adleman, "A Method For Obtaining Digital Signatures

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

and Public Key Cryptosystems," ACM Transactions on Communications, Vol. 21, pp. 120-126, 1978.
[22].T. Nie and T. Zhang "A Study of DES and Blowfish Encryption Algorithm," IEEE TENCON Singapore, pp.1-4, Jan 2009.
[23].G.N. Krishnamurthy, V. Ramaswamy , G.H. Leela "Performance Enhancement Of Blowfish Algorithm By Modifying Its function," SPRINGER Innovative Algorithms and Techniques in Automation Industrial Electronics Telecom. Netherlands , pp 241
-244, 2007.