Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Cryptography Algorithms in Network Security

Yukti
M.Tech (CSE) & MIET, KUK
Haryana, India

Aman Arora
Assistant Professor (CSE) & MIET, KUK
Haryana, India

Abstract— Cryptographic algorithms are basically called as encryption algorithms, contains mathematical procedures for encryption data. There are numerous encryption algorithms techniques having different strengths. Mainly strength of algorithm depend on computer system used for generation of keys. Secret information is made with the help of hash functions, digital signature and key management. The main objective of this survey is to compare various encryption algorithms and then find the best available one algorithm for the network security.

Keywords— encryption, decryption, cryptography, cipher, key.

I. INTRODUCTION

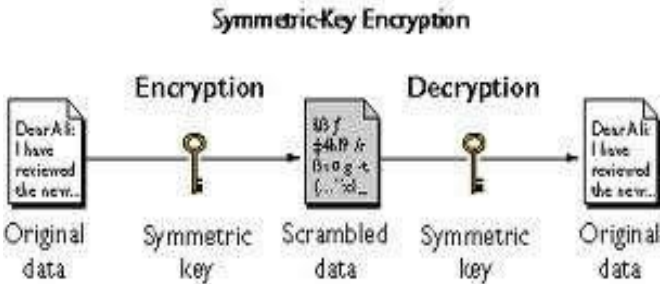
Network Security, nowadays, is the most important and challenging aspect in networking application. With the passage of each day, increasing number of users generate and interchange a large amount of information in different fields, such as legal, medical, financial, bank transaction with internetworking and information transfer which are meant to be confidential. These information transfer should be secure and needed a special treatment. Cryptography is the best means for secure transmission.

Cryptography is the study of Secret (crypto-)-Writing(graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into coded form or unreadable form and that coded form then transforming the message back to its original form. Cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances.

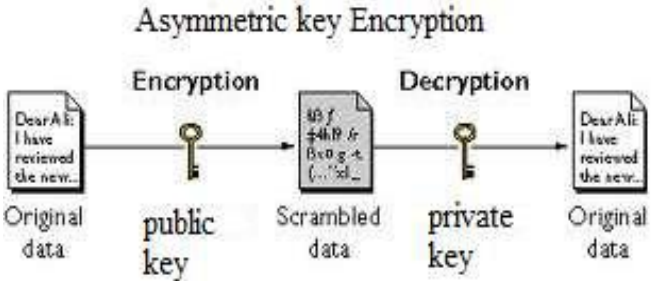
Steganography is the branch of information hiding in which secret information is camouflaged within other information. Steganography means"covered writing"(Greek words"stegos" meaning "cover"and"grafia"meaning"writing").The objective of steganography is to communicate securely in a way that the true message is not visible to the observer.

TYPES OF CRYPTOGRAPHY

A. *Symmetric key cryptography*:-In it only single key is used to encrypt and decrypt.The key is given before transmission between sender and receiver. The strength and weakness of key show how easily data is encrypted and decrypted.It is further classified into two types: block cipher and stream cipher.



B. *Asymmetric key cryptography*:- In it two keys are used public and private key.Encryption is done by public key and decryption is done by private key.Private key is only known to user and public key is known publically.Due to two keys used,asymmetric cryptography require more computational and processing power therefore is slower.



TERMINOLOGY

A. *Encryption*:- Encryption is defined as the process of coding a message so that it cannot be easily read without decoding,as shown in fig(a).
B. *Decryption*:- Decryption is defined as the process of retransforming and decoding an encrypted message back to normal readable message,as shown in fig(b).
C. *Cryptosystem*:- A defined system for encryption and decryption is called cryptosystem.
D. *Cipher Text*:- Cipher text is the encrypted form of message that is not in readable form.
E. *Plain Text*:- Plain text is the original form of message that can be easily readable.

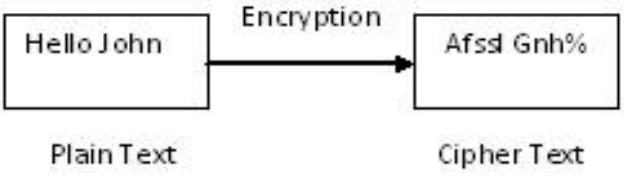


Fig (a) Encryption

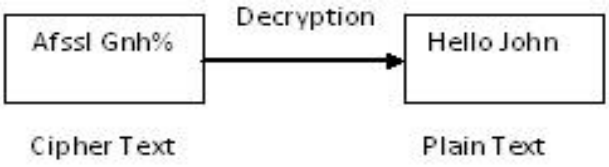


Fig (b) Decryption

GOALS

For an network to be fully secured,the goals of cryptography should be met properly.The 4 main goals of cryptography are:

A. *Authentication*: means that the sender and receiver of data must be authenticated before sending and receiving data.
B. *Confidentiality*: means that the authenticated user only can access the message or data or other authenticated user.
C. *Integrity*: means that the information can be only modified by authorized user and modification includes-writing,changing,deleting and creating.
D. *Non-Repudiation*: this goal assures that neither the sender nor the receiver can deny falsely that they have sent a certain message.

APPLICATION OF CRYPTOGRAPHY

A. *Monitoring communication*: Cryptography provide robust encryption, it can be helpful in governmental areas for secure communication for this key is escrowded with entrusted third party.
B. *Secure message transmission by proxy signcryption*: The signcryption is public key algorithm performing function of both digital signature and encryption. Proxy signature with signcryption public key provide secure transmission. It is very useful in lowpower computer for receiving and transmitting messages from any large number of other computer.
C. *Transferring files on network*: The files which are transmitted needed to be protected against attacks and viruses.The files are encrypted using symmetric key cryptography in which file is encrypted using public key and sent to sender. Then receiver decrypt the file using private key associated with sender.
D. *Quantum key distribution*: It is the best knowing application of quantum cryptography.
E. *Fractional observing of data*: Sometimes sender want only part of message to be encrypted and decrypted.In that case,Translucent cryptography is used.With it government can decrypt some messages and also gain communication privacy.

CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms are basically called as encryption algorithms,contains mathematical procedures for encryption data.there are numerous encryption algorithms techniques having different strengths. Mainly strength of algorithm depend on computer system used for generation of keys. Secret information is made with the help of hash functions, digital signature and key management. Various algorithmic techniques are:

A. *DES (Data Encryption standard):*IBM(International Business Machines)Corporation in late 60's found DES,which was result of cipher called LUCIFER and next version of LUCIFER was proposed as new encryption algorithm by NBS(National Bureau of standard) and finally in 1977, it is adopted as data encryption standard(DES). DES is symmetric block encryption algorithm and uses 64-bit key,in which 56-bit make independent key and remaining 8-bit are for detection of errors. Operation included in DES are permutation and substitution. Permutation are used in expansion of key part. Decryption in DES is just similar to encryption part but in reverse order and resulted output is a block of 64 bits.

B. *3DES(Triple DES*):It is also called TDEA(Triple Data Encyption Algorithm),works by applying DES three times, which increases encryption level as well as enhance security. Key length is 192-bit. The procedure is same as DES, data is encrypted with first key, decrypted by second key and again encrypted by third key.

C. *AES(Advanced Encryption Standard):* The Advanced Encryption Standard is the United State Government standard for symmetric encryption. AES is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (cipher text), or decrypts a 128-bit block (cipher text) to a 128-bit block (plaintext).AES uses a cipher key of length either 128or 192, or 256 bits. Hereafter encryption/decryption with a key of 128, 192, or 256 bits in cipher is denoted AES128, AES192, AES256.The notation AES128, AES192, AES256 process the data block in 10,12,14 iterations respectively of a pre-defined sequence of transformations, which are also called "rounds" (AES rounds) for short. The rounds are identical except the last one, which slightly differs from the others (by skipping one of the transformations). The rounds operate on two 128-bit inputs: "State" and "Round key". Each round from 1 to either 10or12or14 uses a different Round key. Eithe10or12or14 round keys are redeemed from the cipher key by the algorithm called "Key Expansion" .AES algorithm is not dependent of processed data, and can be easily carried out without depending on any encryption or decryption phase

D. *Blowfish* :Blowfish is a public domain encryption algorithm, designed by Bruce Schneider in 1993 as an alternative to already existed algorithm. It's key length vary from 32-bit to 448-bit. Any attack is not successful on blowfish.

E. *IDEA(International Data Encryption Standard Algorithm*):It is also a block symmetric algorithm and operate on 64-bit text block and key size is 128-bit.IDEA contains algebraic operations like XOR,addition modulo216 and multiplication modulo 216+1. This algorithm efficiently work on 16-bit processor. It is based on substitution & permutation but not include S-Boxes.

F. *RSA*: The full form of RSA is named on mathematicians who discovered it, Ron Rivest, Adi Shamir and leonard Adleman in 1997. Variable size key and encryption block is used to make public and private key. RSA is the most secure and convenient.

II. LITRATURE SURVEY

[1] Narender Tyagi in 2014, proposed a detailed theoretical study on cryptographic algorithms to provide secure transmission again malicious people who were trying to harm and gain some information. In paper comparison of algorithm DES, 3DES, AES, Blowfish have been made and also show how these algorithm consume computer resources like memory, battery, CPU time. The parameters for comparison are block size, speed, key size. The author concluded that blowfish is the most secure and provide superior performance as compared to other algorithm. 3DES have least performance.

[2] Anjula gupta in 2014, proposed that cryptography is a greek word and combined of two words crypto-"secret" and graphy-"writing". In the paper cryptography is defined and comparison had been done between various symmetric algorithms DES, AES, 3DES, IDEA, blowfish and asymmetric algorithm RSA. This paper is mainly for beginners and concluded that RSA is the securest and RSA can be combined with other algorithms like DES&RSA, AES&RSA, blowfish&RSA, Diffie Hellman&RSA to improve security.

[3] Ashwini.R.Tonde in 2014, proposed that how much cryptography is important and applied to security measure and discussed the AES algorithm. The author's AES design is coded with very high speed integrated circuit hardware descriptive language. The design use loop approach and key size is 128-bit. The AES design have low latency and high throughput. The author concluded that AES is not so much costly and perform high speed secure transmission.

[4] Obaida in 2013, proposed that most of the algorithms encounter some problems like lack of robustness and time added to packet delay to maintain security. The author show how security goals were enhanced with a new approach of encrypting and decrypting data that maintain security on channel of communication which makes it difficult for malicious user to know the pattern and increases the speed of encryption and decryption. This is a new approach as it is complex for encryption and decryption. This algorithm was tested against different attacks and resulted in secure cipher. Hence it is a good approach as alternative to existing algorithms and application because it has high level of security and small time for encryption and decryption.

[5] Mohammad Soltani in 2013,proposed a new robust cryptography algorithm to enhance security in the Symmetric-key producing algorithm. The features of cryptography algorithm defined as the ability to encode the secret file in successive loops, changing the physical structure of the secret file, the number of keys have no limitation, Creating five keys at each stage of cryptography, secret file is stored at one of the keys at each loop of cryptography,all keys are independent in all loops of encrypting and decrypting, for making the keys dependent on each other and to encrypt the secret file by each of them, there are 2 independent algorithms of type of algorithm needed to make the keys inter dependent by the user, big changes in the physical structure of the encrypted file In the case of false decryption and to make the resulting keys and encryption file unique after the cryptography.

[6] Amritpal Singh in 2013,proposed the main characteristics that differentiate and identify encryption algorithm from another are their ability to secure the protected data against attacks and the speed and effectiveness of securing the data. This review paper provides study of comparison between four widely used encryption algorithms DES, 3DES, AES and RSA on the basis of their ability to protect and secure data against attacks and speed of encryption/decryption.

[7] Pranab garg in 2012, proposed the cryptographic algorithm that fulfil condition of message authentication, digital signature and integrity. Algorithm like hash function, key exchange and PN number are used in cryptosystem. This system can be for block or stream format but the biggest constraint is key length. When all these algorithms are

taken on single time, the performance and security level can be increased to a higher extent. Here CDMA approach for private key generation can be used. Every user will be given an unique PN number, which is generated randomly at receiver side and that number is not known to any other user. This same PN number is sometimes used to decode the cipher text.

[8] Navraj Khatri in 2012,proposed the procedural safeguards in an organization to secure electronic data structure and describe the difference between AES and other algorithms by increasing key size by 200 bits. This algorithm is very good and have enhanced security. The algorithm performance is measured by power consumption in encryption and decryption and show strict avalanche increment in security of AES. The conclusion of this paper is that it measure the level of security by having larger block with 200 bits than 128 bits and block is made of 5*5 matrix unlike 4*4 matrix in AES, it require more multiplication and matrix transformation. The CPU cycle to encrypt is 30% less than other algorithms and the CPU cycle to decrypt are more than 20% of other algorithms. Therefore this model is more secure and used when high data rate communication is required.

[9] Shivangi Goyal in 2012, gave a summary of cryptography, where it is applied and its help in various forms. It gives advanced user authentication, integrity, confidentiality, electronic signatures of data. The algorithms in cryptography use mathematics for encryption and decryption to secure data**.**

[10] Akhil kaushik in 2010, developed a new algorithm BEST(block encryption standard for transfer of data) which is implemented in C++ and JAVA and resulting algorithm is compared with AES and DES and shows that it can easily protect from Replay attacks and Brute force attacks and, also it can change the key format when send it from one sender to reciever.

COMPARISION OF VARIOUS DETECTION APPROACHES CLASSIFIED BASED ON DETECTION ACTIVITY USED

DETECTION CATEGORY	COMPLEXITY	DETECTION ACCURACY	LIMITATION
PATTERN DETECTION	Low	High	Detection of the novel attacks are not possible
ANOMALY DETECTION	Medium	Medium	False positives and negatives rate is very high, since defining normal system behavior and setting threshold values is difficult
HYBRID DETECTION	High	High	Complexity and cost of implementation is very high to deployed in practice
THIRD PARTY DETECTION	High	Detection approach used by third party	Economic Factor, Security prone

III. CONCLUSION

Data Security is a challenging issue of data communications today and strong data encryption technique is required to maintain the data. Cryptography is important for network security and is an emerging technology. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication. There are many cryptography techniques available; among them AES is one of the most useful technique.

REFRENCES

[1] 2009 Third International Symposium on Intelligent Information Technology Application.By " Wentao Liu".

[2] International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012 By " Prajeet Sharma, Niresh Sharma, Rajdeep Singh".

[3] International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267 By "V. Priyadharshini, Dr.K. Kuppusamy".

[4] This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.By "Minda Xiang,Yu Chen,Wei-Shinn Ku, Zhou Su".

[5] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012 ISSN: 2277 128X By "A. Anna lakshmi, Dr.K.R.Valluvan ".

[6] This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings. By "Yinghua Guo, Steven Gordon, Sylvie Perreau".

[7] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012 ISSN: 2277 128X By "Saurabh Ratnaparikhi, Anup Bhange".

[8] International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847 By "Mukesh Kumar & Naresh Kumar".

[9] C. Douligeris and A. Mitrokotsa. DDoS attacks and defence mechanisms: classification and state of- the-art. Computer Networks, 44(5): 643-666, 2004.

[10] An effective prevention of attacks using giTime frequency algorithm under DDos by Dr.K.Kuppusamy,S.Malathi, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[11] Kamanshis Biswas and Md. Liakat Ali; Security Threats in Mobile Ad Hoc Network; Master Thesis; Thesis no: MCS- 2007:07; March 22, 2007.

[12] Stephen M. Specht "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures" Sep. 2004.

