Journal of Engineering and Applied Sciences 12 (21): 5527-5532, 2017
ISSN: 1816-949X

An Overview and Comparison of Various Cryptography Algorithms

Kritagya Sharma and Poonam Kumari
Department of Computer Science and Engineering, Manav Rachna International University,
121004 Faridabad, Haryana, India

Abstract: Network security and cryptography has received much attention in the recent past. As with the increasing threats, viruses and risks, number of people need to understand the basic security structure of network and the methods to deal with it. One of the approach is cryptography which is being discussed here. By this method we can secure information which cannot be understand or visualised by the human system. Using different cryptographic approaches we can share the message secretly to one another within the network. Network security policies are controlled by the administrator of network and it is used to provide authentication and authorization in order to access in a network for data. This study, presents an overview of various cryptography algorithms and further a comparison based on the various parameters.

Key words: Cryptography, DES, AES, Twofish, Threefish, parameters

INTRODUCTION

Network security and protection is one of the major headlines now a days. As the relation between users and Internet is increasing day by day, chances of threats is also increasing. There are number of ways to provide authentication in order to protect the network resource (Kaushik and Singhal, 2012). A secure network must have integrity, so that all of the information stored therein is always correct and protected without any redundant data. There are many tools and techniques which are used to reduce network threats. Cryptography is used to hide the information from the unauthorized users so that chances of threats are reduced. In fact when a message is sent it is encrypted before it is sent. The method of changing text is called a "cipher" and the changed text is called "cipher text". Good cryptography requires good random numbers. Almost all cryptographic protocols require the generation and use of secret values that must be unknown to attackers (Jun and Kocher, 1999). The generation of random numbers to cryptographic algorithms is very essential as it is dependent on generating true random information. Ramaraj *et al.* (2006) explored that the security of any cryptographic algorithm only depends on its key size. The safe key transmission is very essential. The key should be distributed fairly between the sender and the receiver. One should know redundancy and freshness are the two main principles of cryptography. It means the message that is encrypted should have accurate and full information and repetition of the words cannot harm the message but it maintains the accuracy of the message. Further, the information should be free from replay attacks, also known as playback attack which is a form of network attack in which the valid information transmission is delayed or fraudulently repeated. One such measure is including in every message a timestamp. The receiver can then just keep messages around for some seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than that timestamp be thrown out, since any replays sent more than that time later will be rejected as too old. The main goals of data security using cryptographic techniques are data integrity, data confidentiality, authenticity, no repudiation and access control. In data integrity, some receivers receive these data altered. Here, we assume that the data received by the receiver is not altered in any case from the original copy of data. A loss of data integrity is the modification in the data by unauthorized access. Data confidentiality ensures that there is no one participating in the data communication except the sender and the receiver and also ensure that the data being encrypted is safe. A loss of integrity is the disclosure of data to the unauthorized users. Authenticity is the procedure of letting know one's individuality. It provides authentication to authorised workstation for accessing the resources for their research. No repudiation is the process of refusing a communicated message by the receiver. When a message is being sent to the recipient than the sender can prove that the message has been sent to the alleged recipient or vice versa. In access control as the name signifies the power of controlling or accessing the data is for sender and the receiver only. No other

Corresponding Author: Kritagya Sharma, Department of Computer Science and Engineering,
Manav Rachna International University, 121004 Faridabad, Haryana, India

party can interfere. There are three kinds of cryptographic algorithms: symmetric key cryptography, asymmetric key cryptography and Hash function. Identical keys are used for both encryption and decryption purposes in symmetric key cryptographic algorithm, further a known key is shared between both sender and a recipient. It works rapidly and ideal for encrypting loads of data. In the asymmetric key cryptographic algorithm, two non-identical keys are used for encryption and decryption and every user who takes part in this cryptography has access to both a public key and a private key. This method is time consuming and can only encrypt small pieces of a like data. In hash functions, a cryptographic hash function or a mathematical function is needed to take a message and return stable size alphanumeric strings. This particular string is called the 'hash value'. It is tremendously uncomplicated to find hash value for any data. The main focus of hash function is message integrity. The objective of this study is to discuss various methods and algorithms of encryption.

MATERIALS AND METHODS

Methods of encryption: Before implementing an encryption process one should know the principles of encryption, i.e., the message which is transmitting should be safe and can be accessed by only receiver and sender. The most widely used encryption method is the symmetric key encryption method whose computational power is very small that's we use this method for network security. Two methods for this type of encryption are block ciphers or stream ciphers. A typical stream cipher encrypts plaintext one byte at a time. A block cipher encrypts one block at a time. The block may be of size one byte or more or less. Asymmetric key encryption is the method which comprises of both public and private keys. These are known as public keys because the people can be part of the transmission that is used as a transmitting medium between the two. The private keys are used by the owner only and no other person can access it. These keys are not in use because these are typically slow and are not workable with large amount of data. Now, the question arises that how this encryption works? Receiver can apply some mathematical operations on the data that is to be transmitted so that the unauthorized cannot understand the type of data and the meaning of data. The receiver can easily decipher it because he will know all the information about that data. Some algorithms are there to make it more secure which are as follows:

DES: DES (Data Encrypted Standards) is the best used algorithm, designed by Davis R of IBM, based on the block cipher which takes a fixed length of plaintext. This algorithm is used for encryption or decryption of a 64 bit size block of data by using a 56 bit size key and in this the every 8th bit is ignored of that 64 bit block of data and the remaining 8 bit is used for checking parity. It works in 16 rounds where each round consists of s-boxes. The fixed specifications of standards are known as s-boxes. S-boxes are used for mapping the bunch of 6 bits data into 4 bits data. The message block is divided into two halves. Using a fixed table, the first half of the string is enlarged from 32-48 bits. The other half is extracted by combining these bits using XOR operations. It has many disadvantages because of its short key length that leads to many attacks. This can be simplified by breaking the plain text using many searching algorithms. About 3DES is the triple times the original DES to increase the levels of encryption. It is also used to encrypt 64 bit block of data but by using 192 bits key size. Image steganography that is a type of digital technique uses DES for securing information (Ramaiya *et al*., 2013). It is used for hiding information into a cover picture. Singh and Parmar (2015) suggested that pipelines can be clocked at high frequency using MIPS cryptography which is based on 3DES. With the help of block diagrams encryption and decryptions gives a high performance in MIPS cryptography.

AES: AES stands for Advanced Encryption Standards. In 2001, DES and 3DES had been replaced by AES which was developed by Vincent Rijmen and Joan Daeman. It is a type of symmetric cryptography. It is capable of shuffling bits that are found from a chain of linked operations. This type of cryptography performs all its operation on byte unlike bit. Therefore AES (treats) 128 bits of block as 16 bytes which are arranged in four columns and four rows resulting as a matrix. It is also a block cipher and has a variable length of 128, 192 and 256 bits and takes default as 256. It is also used to encrypt blocks of 128 bits in 10, 12 and 14 round. Here, we use 16 bit key size. It is fast and flexible and further due to platform dependent it can be run easily in small devices. Hossain *et al*. (2016) examined that bio-molecular DNA aspects can be used to enhance the security level. This technique uses a DNA sequence table in which ASCII characters are assigned to each DNA and after that One Time Pad (OTP) are used for encoding the message.

Blowfish: A kind of encryption algorithm having a block of 64 bit size. It has an inconstant key length ranging from 32-448 bits. Its key size is bigger because of that it is very complicated to disintegrate the transmitting cipher which is an advantage here. Since, the key which is used does

not change much it is used in communication links. This algorithm has two main parts that are data encryption and key expansion. It consists of 16 rounds with feistel function network and each round has a permutation within it depending on the variable key length and the content. This feistel function provides many logical operations such as XOR, MOV and ADD which makes this algorithm faster. In key expansion, out of 4168 bytes it converts a key of 448 bits into different sub key arrays. Reddy *et al*. (2016) observed that the Optimal Blowfish Technique is used for successful coding and decoding which is very advantageous for cloud computing.

Twofish: This algorithm was designed by Bruce Schneier and his group members. It's the type of an encryption in which 128 bit block cipher is used. It contains 128, 192 or 256 bits variable key length. It has been mainly used for large microprocessors, 8 bit smart card microprocessors and dedicated hardware because of its high flexibility and high security. They use preassembled key dependent s-boxes and a key tangled schedule which makes it unique. In this algorithm partially divided n bit size key is used for encryption and other portion is used for recast the algorithm. It borrows elements from design likes PHT (Pseudo-Hadamard Transform) from ciphers. Twofish can be used in encryption schemes such as PG, Photo Encrypt and Truecrypt. Hingmire *et al*. (2016) suggested that Twofish block cipher can be used in image steganography with the help of B45 algorithm. Image steganography is the technique to hide images in other section of images when the communication is taking place.

Threefish: A tweakable block cipher under symmetric key cryptographic algorithm came to be known as Threefish which was developed by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare and Jesse Walker in the year 2008. This sort of block cipher only accepts three inputs: a block of message, a key and a tweak. Every block of information or message encryption is done by an identical tweak value of that message. The value of that particular tweak is 128 bits for each and every block sizes. Further, three kinds of keys are used in this encryption: 256, 512 and 1024 bits size. This type of encryption uses three block sizes that are equal to 1024, 512 and 256 bits. Encryption is done normally in 72 rounds but for 1024 size of block, it takes only 72 rounds as fixed size. There is a very uncommon thing in threefish that it does not use s-boxes or any other lookups of table to evade many timing attacks. Threefish is a special technique that uses Nr/4+1 various round keys. Threefish block cipher technique has also been used in achieving hash functions like Blake and Skein (At *et al*., 2014). These hash functions are used for creating lightweight coprocessors that can be further used for coding and decoding.

RC5: RC5 algorithms were proposed in 1994 by Professor Ronald Rivest. It is a block cipher algorithm for encryption. It is fast and symmetric key algorithm. For the implementation of hardware and software it is best suitable. It provides high level of security. The main feature about RC5 algorithms is that there is a use of dependent rotation of data. In RC5 the range of round number is from 0-255 similarly the range of size of key is from 6-2048 and size of block is 32, 64 or 128 bits. In term of security protocols of LSWN (Low Speed Wireless Network) RC5 receives higher support and favour. Routines are of three types in RC5, namely: encryption, key expansion and decryption. In encryption routine process XORing bitwise, rotation of variable and addition of integers are done. Other hand, secret key is provided to the user which the user can expand to fill the key table. The size of this key table depends on the round number. Then the process of decryption of message and encryption is completed by the filled table. RC5 is widely accepted in the term of simplicity and also it makes the analysis process easy. It is also used against differential and straight cryptanalysis. This algorithm has also been used in effective image encryption and securing wireless communications (Suresh *et al*., 2015).

RSA: RSA is a special type of asymmetric cryptography technique. RSA is formed on thinking that there is much difficulty in factorizing a big integer. Public key which is involved in this method contains two numbers from which one number is product of two big prime numbers and the key which is private is obtained from the corresponding prime numbers. The advantage of this cryptographic technique lies on the key area. If the size of the key gets doubled or tripled, the power of the key increases rapidly. RSA keys can be either of length 1024 bits of length 2048 bits but it has been researched that 1024 bits key could be broken in the future but till now it is a very difficult task. The result of RSA is a huge amount of bits that takes attackers much time to break it. Shehata *et al*. (2014) analyzed that there is a Field Programmable Gate Array (FPGA) execution of the RSA encryption algorithm in achieving e-passport application where e-passport is a special type of passport that has a smart card back in the year 2014.

ECC: ECC (Elliptic Curve Cryptography) was developed by Victor Miller and Neal Koblitz in the year 1985. It is a kind of public key cryptographic method which has been built on algebraic structures of elliptic theory of curve. This type of theory is used in creating quicker, minor and systematic cryptographic keys. It does not work on a conventional method of generating product of extremely huge prime numbers. ECC encryption is done using elliptic curve equation generally we use in mathematics. It is very conventional that it can supply a height of security using 164 bit size key rather than using 1024 bit size key that distinct system requires. It tenders highest security with minor bit key sizes which concludes to less power and that is why this cryptography is used for battery backup as well. Primarily, elliptic curve is meant to be a plane curve above finite number of fields. ECC has also been used in the analysis of RFID (Radio-Frequency Identification) authentication for IOT (Internet of Things) in healthcare domain (Farash *et al*., 2016). McGrew *et al.* (2014) analysed that ECC cipher is best suited within TLS (Transport Layer Security) to supply confidentiality and data authentication using AES-CCM algorithm where AES stands for Advanced Encryption Algorithm and CCM stands for Counter and CBC-MAC Mode. CCM is nothing but a encryption algorithm used for building a message verification code from a block code.

IDEA: IDEA (International Data Encryption Algorithm) is originally known as IPES (Improved Proposed Encryption Standard). This cryptographic algorithm was first explained in 1991 by J. Massey and Xuejia Lai. This is a block cipher and symmetric key cryptographic algorithms. Plain text in IDEA is of 64 bit similar to plain text and cipher text is also of 64 bit. Sub key uses in IDEA are 52. In IDEA algorithm there are 8 rounds where certain operations are conducted and 6 key is being used for each and every round. After these 8 rounds, the output becomes the input for transformation outputs. The final output is a 64 bit text, i.e., ciphers text. The process of decryption is as same as encryption. Here, different algorithms are used to derive sub keys unlike encryption process. About 128 bits is the actual size of cipher text. Against many cipher attack it has been proved as the most successful algorithms. IDEA algorithms also have an application in Pretty Good Privacy V2.0. It is considered as the best known publicly encryption algorithms. Ione may also refer to Jayashree *et al.* (2016) for the application of IDEA coding algorithm with high output. This can be achieved by using Verilog HDL which is a Hardware Description Language used for designing of digital circuits at the level of abstraction. High throughput can be achieved from IDEA algorithms by using its temporal parallelism.

RESULTS AND DISCUSSION

Comparison of different algorithms: The objective of this study is to compare the above discussed algorithms. In the existing literature several authors have also give a comparison among different algorithms. For an instance (Bhanot and Hans, 2015) presented an overview on cryptographic symmetric and asymmetric algorithms. In their work some of the symmetric algorithms were DES, AES, Twofish, RC5, blowfish and some of the asymmetric algorithms were ECC and RSA. Further, Mellu and Mali (2011) discussed about AES and the authors examined mathematical operations on AES algorithms. They observed the AES works with less complexity and has a high security level. Work of Soni *et al.* (2012) have also presented a comparison between DES and AES algorithms. Researchers observed that encryption and decryption time taken by AES is less than of DES algorithm. Singh *et al.* (2013) discussed about the performances of DES and RSA algorithms. DES is based on private key whereas RSA is based on public key. They studied that the time taken by DES for execution is less than the execution time of RES algorithm. In their research (Bisht and Singh, 2015) studied algorithms like DES, AES, DIFFIE HELLMAN and RSA. Researchers observed that AES algorithms are best known for security and cost among various symmetric key algorithms and RSA algorithms are best in security and speed among asymmetric key algorithms. The work of Verma *et al.* (2016) talk about the most effective and most secure symmetric algorithms among AES and blowfish. While talking about asymmetric encryption algorithm, RSA is best and secured. Rihan *et al.* have also compared the performance of DES and AES algorithms. Next, we present a comparison of all the considered algorithms based on the following parameters.

Development: Development of an encryption algorithm means that in which particular year it has been developed and by whom. Key length-key size or key length is the total number of bits in a particular key used by diff cryptographic algorithm. It mainly defines the upper bound of the security of an algorithm. It is directly proportional to security.

Round: Round of an encryption is the total time taken by an encryption function in executing complete process unless it gives block of cipher as its output.

Table 1: Comparison of various algorithms on the basis of different parameters

Parameters	Development	Key length (bytes)	Rounds	Block size (bits)	Attack found	Level of security	Encryption speed
DES	In early 1970 by IBM and Published in 1977	64 (56 usable)	16	64	Exclusive key search, linear cryptanalysis, differential analysis	Adequate security	Very slow
3DES	IBM in 1978	168,112	48	64	Related key attack	Adequate security	Very slow
AES	Vincent Rijmen, Joan Daemen in 2001	128,192,256	10,12,14	18	Key recovery attack, side channel attack	Excellent security	Faster
RSA	Ron Rivest, Shamir and Leonard Adleman in 1978	Key lengths depends on no of bits present in the module	1	Variable block size	Brute force attack, timing attack	Good level of security	Average
Blowfish	Bruce Schneier in 1993	Variable key length, i.e., 32-448	16	64	No attack is found to be successful against blowfish	Highly secure	Very fast
Twofish	Bruce Schneier in 1998	128, 192, 256	16	128	Differential attack, related key attack	Secure	Fast
Threefish	Bruce schneier, Niels Ferguson, Stefan Lucks in 2008	256, 512, 1024	For 256, 512 key = 72, For 124 key = 80	256,512 and 1024	Improves related-key boomerang attack	Secure	Fast
RC5	Ron Rivest in 1994	0-2040 bits key size (128 suggested)	1-255 (64 suggested)	34, 64, 128 (64 suggested)	Correlation attack, Timing attack	Secure	Slow
ECC	Victor Miller from IBM and Neil Koblitz in 1985	Smaller but effective key	1	Stream size is variable	Doubling attack	Highly secure	Very fast
IDEA	Xuejia Lai and James in 1991	128	8	64	Linear attack	Secure	Fast

Block size: The block cipher runs on a fixed length strand of bits which is known as block size. Both the plain text and the cipher text have the same block sizes. It is totally dependent upon the respect algorithm.

Attacks: The unlicensed access to the data is called as attacks. The main motive of these is to steal information at the time of transmission of information or message. Attacks are divided into two types active and passive based on the measures executed by the attacker. Active attacks include modifying the information by guiding some operation on that information. It includes unofficial deletion of the information. Passive attacks are passive in nature as they neither influence information nor derange the transmission channel.

Level of security: An algorithm security level of an algorithm is established on the famous known attack of the algorithm. Security level are interpretation of strength of security and are used in estimating a cipher capability to assure information based on diff estimated capabilities (above) time.

Encryption speed: It is the time required to encrypt the plain text into cipher text. It is totally dependent on the attacker. Based on all these parameters we present a comparison among all the considered algorithm in Table 1.

CONCLUSION

In this study, we analyse that the cryptography is an emerging technology in the real world and can be used in many ways. Some popular and existing cryptographic algorithms have been studied in this study to show the basic difference between the current encryption ways. only mathematical calculations are not important, best documented algorithms are called good as they are tested in the best way. Good cryptographic algorithms are best tested by the passage of time. The strength of the better encryption technique can be judged by the selection of a key, i.e., long keys holds an advantage over short keys as they can resist attacks well as compared to the short ones. An encryption algorithm can be chosen depending on the data being exchanged or transferred and the channel through which it is done. The basic objective of this research is to make us understand the concept and working of the various cryptographic algorithms. It also compares the currently existing encryption ways (symmetric ones) based on certain specifications. They could be how much prone they are towards an attack, unlikeness of the way and many more.

ACKNOWLEDGEMENTS

Researchers are thankful to the Editor, Associate Editor and anonymous reviewers for several constructive

suggestions. We also would like to express our sincere gratitude to Dr. Sukhdev Singh, Accendere Knowledge Management Services Pvt. Ltd., for his valuable comments that led to substantial improvements on an earlier version of this manuscript.

REFERENCES

At, N., J.L. Beuchat, E. Okamoto, I. San and T. Yamazaki, 2014. Compact hardware implementations of ChaCha, BLAKE, Threefish and skein on FPGA. IEEE. Trans. Circuits Syst. Regul. Pap., 61: 485-498.

Bhanot, R. and R. Hans, 2015. A review and comparative analysis of various encryption algorithms. Intl. J. Secur. Appl., 9: 289-306.

Bisht, N. and S. Singh, 2015. A comparative study of some symmetric and asymmetric key cryptography algorithms. Intl. J. Innovative Res. Sci. Eng. Technol., 4: 1028-1031.

Farash, M.S., O. Nawaz, K. Mahmood, S.A. Chaudhry and M.K. Khan, 2016. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. J. Med. Syst., 40: 165-165.

Hingmire, A., S. Ojha, C. Jain and K. Thombare, 2016. Image steganography using adaptive b45 algorithm combined with Pre-processing by twofish encryption. Intl. Educ. Sci. Res. J., 2: 11-12.

Hossain, E.M.S., K.M.R. Alam, M.R. Biswasa and Y. Morimoto, 2016. A DNA cryptographic technique based on dynamic DNA sequence table. Proceedings of the 19th International Conference on Computer and Information Technology (ICCIT) 2016, December 18-20, 2016, IEEE, Khulna, Bangladesh, ISBN:978-1-5090-4091-9, pp: 270-275.

Jayashree, M., I. Poonguzhali and S.S. Agnes, 2016. An efficient high throughput implementation of IDEA encryption algorithm using VLSI. Aust. J. Basic Appl. Sci., 10: 337-344.

Jun, B. and P. Kocher, 1999. The intel random number generator. Cryptography Research, San Francisco, California. http://decuslib. com/decus /vmslt99a/sec/intelrng.pdf

Kaushik, S. and A. Singhal, 2012. Network security using cryptographic techniques. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 105-107.

McGrew, D., D. Bailey, M. Campagna and R. Dugal, 2014. AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS. Internet Eng. Task Force, 1: 1-10.

Mellu, P. and S. Mali, 2011. AES: Asymmetric key cryptographic system. Intl. J. Inf. Technol. Knowl. Manage., 4: 113-117.

Ramaiya, M.K., N. Hemrajani and A.K. Saxena, 2013. Security improvisation in image steganography using DES. Proceedings of the IEEE 3rd International Conference on Advance Computing (IACC) 2013, February 22-23, 2013, IEEE, Jaipur, India, ISBN:978-1-4673-4527-9, pp: 1094-1099.

Ramaraj, A., N. Laitha and S. Karthikeyan, 2006. An analysis of key management in cryptographic algorithms. Asia J. Inform. Technol., 5: 963-967.

Reddy, P.D.K., R.P. Sam and C.S. Bindu, 2016. Optimal blowfish algorithm-based technique for data security in cloud. Intl. J. Bus. Intell. Data Min., 11: 171-189.

Shehata, K., H. Hussien and S. Yehia, 2014. FPGA implementation of RSA encryption algorithm for E-passport application. World Acad. Sci. Eng. Technol. Intl. J. Comput. Electr. Autom. Control Inf. Eng., 8: 82-85.

Singh, K.P. and S. Parmar, 2015. Design of high performance MIPS cryptography processor based on T-DES algorithm. Intl. J. Eng. Res. Technol., 1: 1-6.

Singh, S., S.K. Maakar and S. Kumar, 2013. A performance analysis of DES and RSA cryptography. Intl. J. Emerging Trends Technol. Comput. Sci. IJETTCS., 2: 418-423.

Soni, S., H. Agrawal and M. Sharma, 2012. Analysis and comparison between AES and DES cryptographic algorithm. Intl. J. Eng. Innovative Technol., 2: 362-365.

Suresh, S., M. Varghese and D. Aju, 2015. An efficient and optimized RC5 image encryption algorithm for secured image transmission. Intl. J. Imaging Rob., 15: 116-125.

Verma, A., P. Guha and S. Mishra, 2016. Comparative study of different cryptographic algorithms. Intl. J. Emerging Trends Technol. Comput. Sci. IJETTCS., 5: 58-63.