International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206453

A Study on Cryptographic Techniques

Anjali Krishna A*[1], Dr. L. C. Manikandan[2]
*[1]PG Scholar, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
[2]Professor and HoD, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Article Info
Volume 6, Issue 4
Page Number: 321-327
Publication Issue :
July-August-2020

Article History
Accepted : 20 July 2020
Published : 27 July 2020

ABSTRACT

In current scenario, to store data securely on online is a tedious task as a result proper security over the network. Cryptography is a technique that masks the data over the channel of communication. Hiding the data to outsiders is an art. As the technology grows day by day, the need for data security over the channel of communication is greatly increased. Several cryptographic schemes are used for secure communication. The cryptographic technique and various algorithms are used to ensure the application has the necessary security. Cryptography is the science of both encryption and decryption. This paper describes all of the cryptographic techniques in detail.

Keywords: - Cryptography, Symmetric key, Asymmetric key, Encryption, Decryption.

I. INTRODUCTION

Now a day's all works related to banking, ATM card, credit card, marketing, E commerce etc. is doing with the aid of internet. So there must be protection provided over the network. Therefore for secure communication we have several cryptography techniques are used. We apply these cryptographic techniques to sensitive information in order to provide protection from an unauthorized access. In cryptosystem, data are protected via encryption method for keeping communication is private. Every one send the private message by encrypting the message and intended receiver decrypts it by its key [9]. Cryptography perhaps the most important element of communication's security and is becoming increasingly important as a basic building block for computer security. Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages. These are all focused on the use of secrets called keys. A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be broken without the knowledge of the key. Encryption is the method of encoding a message in order to encrypt its contents.

A plain or normal text sent over the network is converted into cipher text so that the information can only be used by the sender and the receiver. The method of converting plain text messages into cipher

text messages is called encryption, in technical terms. The method of converting cipher text into plain text again is known as decryption. Decryption is exactly the opposite of encryption. The computer at the end of the sender normally converts a plain text message into cipher text messages in computer to computer communications by performing encryption. Then, this message is sent over the network to the receiver. To get plain text, the receiver's computer takes the encrypted message and performs the decryption method. The encryption and decryption process is called cryptography. Cryptography in general is the art and science of achieving protection by encoding messages to make them unreadable [1]. It can be used in any way to mask the significance of the information. It can also be applied to software, graphics or voice. The encryption origins date back to the days of the great Julius Caesar. Caesar used this strategy to send his messages confidentially. One of the easiest methods of encryption is the Caesar's form, commonly known as Caesar's Cipher. The encryption methods of today are much more complex and advanced compared with it. In order to convert sensible information into an incomprehensible format, extremely complex algorithms are being applied today. When encrypted; only the proper keys, known as' Cryptographic Keys,' can decrypt the message / data. A cryptographic key is simply a password which is used to encrypt and decrypt information.

Substitution technique and Transposition technique are the types of operation used for converting plain text into cipher text. A substitution technique is one in which plain text letters are replaced with other letters, numbers or symbols. In Transposition Technique the plaintext letters perform some kind of permutation. Cryptographic process is show in Fig 1.

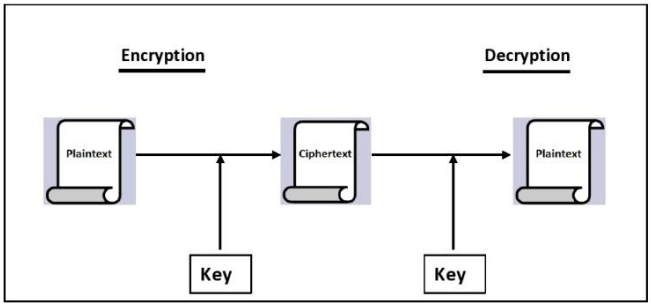

Fig 1. Cryptographic process

II. TERMINOLOGY

Plain text: Original message is known as plain text.

Cipher text: Coded message is known as cipher text.

Encryption: The process of converting the plain text to cipher text is known as encryption.

Decryption: The process of restoring the plain text from the cipher text is known as decryption.

Key: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography.

Steganography: It is actually the science of hiding information from people who would snoop on you. The difference between Steganography and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place.

Cryptography: The study of both encryption and decryption.

III. CRYPTOGRAPHIC TECHNIQUES

There are two basic information encryption techniques: symmetric encryption, which is also

called secret key encryption, and asymmetric encryption, also called public key encryption.

A. Symmetric Encryption

Symmetric-key cryptography refers to methods of encryption, in which the sender and the receiver share the same key. Symmetric key ciphers are either used as block ciphers, or as stream ciphers. A block cipher enciphers the input type used by a stream cipher, in plaintext blocks as opposed to individual characters. Symmetric cryptography is much faster than asymmetric. The symmetric encryption is shown in Fig 2.

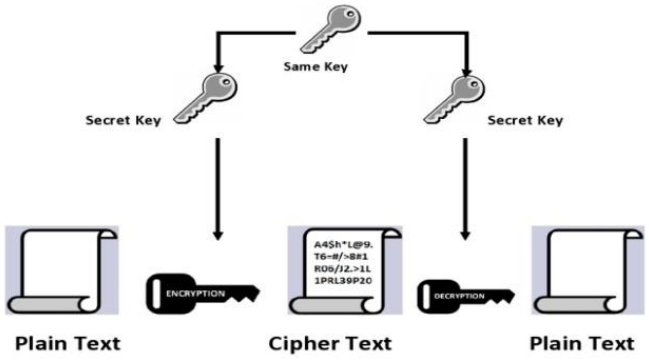

Fig 2. Symmetric Encryption

This is the simplest method of encryption, requiring only one secret key for ciphering and deciphering information. Symmetrical encryption is an old technique and is best known. Uses a secret key that can be a number, a phrase, or a random letter string. To modify the material in a particular way is a blended with the plain text of a document. The sender and the receiver would know the secret key used to encrypt and decrypt all the messages. Examples of symmetric encryption include DES, TDES, AES, Blowfish, and RC4. The AES-128, AES-192, and AES-256 are the most commonly used symmetric algorithms.

- **Data Encryption Standard (Des)**

DES was the first encryption standard developed in 1973 and was recommended by the National Institute of Standards and Technology (NIST) in 1976 to be the most efficient method for data encryption. This was the most commonly used standard worldwide [6]. It is a block cipher that encrypts a plaintext of 64 bits at a time and uses 56 bit key. This was based on symmetric key algorithm which means that both encryption and decryption will use the same key. DES can operate in modes CBC, ECB, CFB, and OFB. DES has 16 rounds, meaning that cipher text is generated using a total of 16 processing steps on the plaintext input. First, 64 bit data is passed through the initial permutation phase and then 16 processing rounds are performed and finally the final permutation step is performed on the plain text input which results in 64 bit cipher text. The drawback of this algorithm is that by adding all possible combinations it can be easily vulnerable to Brute Force Attack in which the hacker tries to crack the key. There are only 2^56 possible combinations in DES that are fairly easy to crack. And DES is not so safe [5].

- **Triple Des (TDES)**

Due to advances in key searching, the Triple DES (3 DES) algorithm was introduced as a replacement for DES. TDES uses DES encryption in three rounds and has a key length of 168 bits (56*3). The Encrypt-Decrypt-Encrypt (EDE) series uses either two or three 56 bit keys. First alternative is to produce cipher text on plaintext message t using three different keys for the encryption algorithm.

C (t) = Ek1 (Dk2 (Ek3 (t))) ---------- **eqn(1)**

Where C (t) is plaintext message cipher t, Ek1 is the method of encryption using key k1, Dk2 is the method of decryption using key k2 and Ek3 is the

method of encryption using key k3. The choice is to use the encryption algorithm with two distinct keys. This reduces the keys ' memory requirement in TDES.

C (t) = Ek1 (Dk2 (Ek3 (t))) ---------- **eqn(2)**

TDES with three keys needs 2 ^ 168 possible combinations, and that of two keys requires 2 ^ 112 possible combinations to be checked for brute force attack is virtually impossible. It provides TDES as the strongest algorithm of encryption that gives its application in banking industry. The drawback of this algorithm is that it consumes too much time [3].

- **Advanced Encryption Standard (AES)**

In 1998, the US National Standards and Technology Institute (NIST) proposed using the Advanced Encryption Standard to replace the Data Encryption Standard. AES is a variable bit block cipher that uses the 128, 192 and 256-bit variable key range. If both the length of the block and the length of the key are 128 bits, AES will do 10 rounds of processing. If the block and key are 256-bit long then 14 processing rounds are performed [4]. AES is a symmetrical block cipher capable of blocking size128bit, 128,192 and 256-bit cipher keys. Generally, algorithms of encryption are divided into three main categories of technique of transposition and substitution. AES algorithm uses a round function which is compared to four different byte-oriented transformations such as Sub line, Shift row, Switch column, Add round key. Number of rounds to use depends on key duration e.g. 10 rounds for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit key. Each round of processing includes 4 steps:

Substitute bytes: Uses an S-box to perform a byte by byte substitution of the block.

Shift rows: A simple permutation.

Mix column: A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix

Add round key: The key for the processing round is XOR with the data.

AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices.

- **Blowfish**

Blowfish algorithm is the important form of symmetric key encryption which has a block size of 64 bit and a key length variable of 32 bits to 448 bits in general[10]. It is based on a network of 16 round fiestel cipher, using the large key size. The key size is bigger, as the code in the blowfish algorithm is hard to break. However, apart from the low main class attack, it is exposed to all of the attacks. This algorithm has the advantage that it is highly secure and has not yet been broken. It's suitable for hardware implementation and is effective. There are two sections to the algorithm-Key expansion and data encryption. Main stage of expansion transforms 448 bit main into 4168 bytes. A P series of sizes 18 and 4 S stacks, each of which have a size of 256 and is initialized to hexadecimal π digits. XOR per 32-bit main entry in P array and S boxes [7]. There are total 16 rounds of data encryption. In each round, XOR with the leftmost 32 bits of plaintext is a 32 bit sub key, and the result is then transferred to the Blowfish F function.

B. Asymmetric Encryption

Asymmetric key cryptography refers to methods of encryption, in which the sender and the recipient share the same key. A key is used to encrypt, and the other to decrypt. It gives greater stability than the symmetrical systems. Asymmetric Encryption is a relatively new and complex Encryption style. Complex, because it uses two cryptographic keys for

data security implementation. Such keys are referred to as a public key, and a private key. As the name suggests, the Public Key is open to anyone wishing to send a message. On the other hand, the public key owner keeps the private key in a secure place. The asymmetric encryption is show in Fig.3.

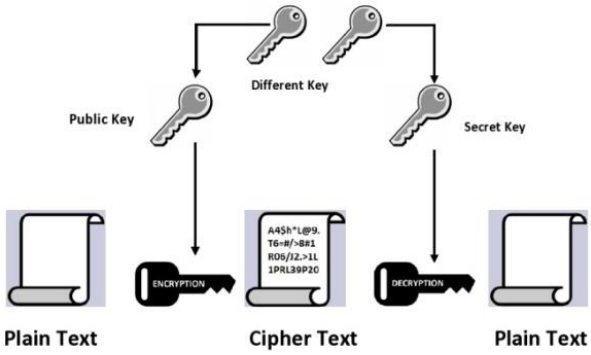

Fig. 3 Asymmetric Encryption

Asymmetric encryption is also known as public key cryptography, opposed to symmetric encryption, which is a relatively new technique. For asymmetric encryption, two keys are used to encrypt a plain text. Hidden keys are shared over a large network or over the Internet. This means the keys are not misused by malicious people. It is important to note that anyone with a secret key can decrypt the message and that is why asymmetric encryption uses two related keys to improve security. Anyone who might want to send you a message will be given a public key free. The second private key is kept a secret for you to know only. A message encrypted using a public key can only be decrypted using a private key, while using a public key can also decrypt a message encrypted using a private key. Public key protection is not needed since it is available to the public and can be transmitted over the internet. Asymmetric key has a far better power to ensure that information exchanged during communication is secure.

- **Rivest-Shamir-Adleman (RSA)**

RSA stands for the name of three inventors Rivest Shamir and Adleman [11]. RSA is the most commonly used algorithm for the public key encryption. It can be used for both digital signatures and the encryption. RSA's protection is commonly seen as factoring. RSA is one of the first functional cryptosystems with a public key and is commonly used for secure data transmission. The encryption key is available in such a cryptosystem, which varies from the decryption key that is kept secret. In RSA this asymmetry is based on the practical complexity of factoring two large prime numbers product, the question of factoring. The problem for the attacker is that it is presumed that computing the inverse d of e is no simpler than factorizing n. For a reasonable level of safety, the key size should be greater than 1024 bits. Size keys, say, which provide 2048 bits.

a. Key Generation

ss(1) Select p and q both prime number, p is not equal to q.
(2) Calculate n = p x q.
(3) Calculate ø (n) = (p -1) x (q-1).
(4) Select integer e whose gcd (Ø (n), e) = 1; 1 < e
(5) Calculate private key d = ℮-1 (mod Ø (n)).
(6) Public key PU = {e, n}.
(7) Private Key PR = {d, n}.

b. Encryption Procedure

C= M ^e mod n.

c. Decryption Procedure

M = C ^d mod n.

Where, M is message, p and q are prime numbers, n is common modulus, e and d are public and private keys.

- **Diffie-Hellman (DH)**

It's that algorithm for public key encryption, using discrete logarithms in a finite field. Two parties allow a secret key to be shared without prior secrets over an unreliable medium. Diffie-Hellman (DH) is a key exchange algorithm that is commonly used. Two

parties wish to begin communicating in many cryptographically protocols. Diffie-Hellman protocols are exchange keys and allow common secret key to be created over an unconfident communication channel. This issue is related to discrete logarithms; its name is Diffie-Hellman issue. This problem is complicated, as contrasted with the problem of the discrete logarithm. Diffie-Hellman key exchange, also known as exponential key exchange, is a digital encryption system that uses numbers raised to specific powers to generate decryption keys based on components that are never transmitted directly, thereby mathematically overcoming the task of a would-be code breaker. The Diffie-Hellman algorithm relies on the computational complexity of discrete logarithms for its effectiveness In short, the discrete logarithm can be defined in the following way. Next, we define a prime number p's primitive root as one whose powers modulo p generates all the integers from 1 to p 1. That is, if the primitive root of prime number p is "a".

Users A and B would like to share one key. User A selects XA < q at random and calculates YA= α^ XA mod q. Likewise, user B selects a random integer XA < q independently, and calculates YB= α^XB mod q. Every side keeps the value of X private, and makes the value of Y publicly available to the other side. User A calculates the key as K= (YB) X A q and user B calculates the key as K= (YA) ^XB mod q. These two calculations produce identical results: K = (YB) ^XA mod q [12].

- **Elliptic Curve Cryptography (ECC)**

ECC is the counterpart of modular multiplication in RSA and the counterpart of modular exponentiation is multiple additions. In order to form a cryptographic scheme using elliptic curves, we must consider a "hard problem" that corresponds to factoring the product of two primes or taking the discrete logarithm. Consider the Q= kP equation where Q, P E p (a, b), and k < p. Calculating Q given k and P is relatively easy but determining k given Q and P is relatively difficult. For elliptic curves, this is called the discrete logarithm problem.

A prefers an integer n A less than n. This is the privately held key of A. A then generates a public key PA=nA Elliptic Curve Cryptography G; the public key is a point in Eq(a, b).B selects a private key nB similarly, and calculates a public key PB. A generates K= nAx PB as the secret key. B generates K= nBx PA as the secret key.

IV. CONCLUSION

In the world of computer science, Cryptography is a very interesting field because the amount of work performed is kept only secret. There are different techniques and algorithms researched, and various types of work have been performed. In this paper briefly discussed cryptography and its form of symmetric key cryptography and algorithms for asymmetric key cryptography.

V. REFERENCES

[1]. Shivani Sharma, Yash Gupta“ Study on Cryptography and Techniques” , IJSRCSEIT, Vol.2, 2017.

[2]. Preeti Singh, Praveen Shende, “Symmetric Key Cryptography: Current Trends”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014.

[3]. O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, “Peformance Analysis of Data Encryption Algorithms”, IEEE Delhi Technological University India, 2011.

[4]. Himani Agrawal and Monisha Sharma, “Implementation and analysis of various symmetric cryptosystems”, Indian Journal of Science and Technology Vol. 3, No. 12, December 2010.

[5]. Diaa Salama, Abdul Minaam, Hatem M.Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, PP.78-87, Sept. 2010.

[6]. Tingyuan Nie and Teng Zhang, " A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[7]. Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", IEEE, 2008.

[8]. Ms. Ritu Patidar1, Mrs. Rupali Bhartiya, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", Vol.3, 2003.

[9]. W. Stallings "Cryptography and network security", vol.2, prentice hall, 2003

[10]. 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, ISSN: 2277-128X.

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

[12]. W. Stallings "Cryptography and network security", Vol.4, prentice hall.

[13]. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

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

AUTHOR PROFILE

ANJALI KRISHNA A is doing M Tech at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India. She has received B Tech degree in Computer Science and Engineering from APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India. Her main research area of interest includes Cryptography and Network security.

Dr. L. C. Manikandan is working as Professor at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, INDIA. He has received Ph.D. degree in Computer and Information Technology from Manonmaniam Sundaranar University, M.Tech. Degree in Computer and Information Technology from Manonmaniam Sundaranar University, M.Sc., Degree in Computer Science from Bharathidasan University and B.Sc. Degree in Computer Science from Manonmaniam Sundaranar University. His main research interest includes video surveillance, image compression and video coding in image processing.

Cite this article as :

Anjali Krishna A, Dr. L. C. Manikandan, "A Study on Cryptographic Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 321-327, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206453
Journal URL : http://ijsrcseit.com/CSEIT206453