Techniques and Services Provided by Cryptography

Anusha C S[1] Namratha Kalasannavar[2]
[1]MCA Student [2]Assistant Professor
[1,2]Department of Master of Computer Application
[1,2]Sambhram Institute of Technology, Bangalore, India

Abstract— Nowadays, Cryptography plays a very important role to secure the secret information. In the growth of technology, we use number of ways to secure information over the network. The message which is sent should be secured from hackers. Here, we use the techniques of cryptography to keep details secure. Cryptography is derived as secret writing. Unauthorized people could not extract any information which is hidden. We have to protect the message from the unauthorized peoples. Here, we have mentioned about the private key and public key for encryption. Cryptography is one of the best ways to keep our information secretly. So, it's the best way to send the information in secured network. There are multiple number of techniques in cryptography .To secure the information we use some services like confidentiality, authentication, integrity, nonrepudiation, access control. We study about the different cryptosystems which will be helpful for the people to access the message and security. The information will be secured by the authorizer from the unauthorized peoples and it can be accessed by the authorizer by giving the private key and outsource key. Hence both keys should match to access the message.

Key words: Security Services, Asymmetric Cryptosystem and Symmetric Cryptosystem, RSA Algorithm

I. INTRODUCTION

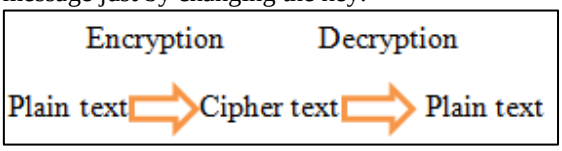
The art of coding secretly is Cryptography. Cryptography is derived from Greek word 'krypto' means hidden and 'graphine' means writing[5]. Claude E. Shannon is considered as the father of mathematical cryptography. Shannon's work impacted modern designs of secret key ciphers. It is an effective way of protecting sensitive information. Here, the authorized person will send and retrieve the information. Unauthorisers cannot get the secured information over the network. The mechanism of storing and transmitting data in a form that is intended to read and process is called as Cryptography. It specifies some important number of services to secure the information. Cryptography is an emerging technology.

It is widespread use for computerized data storage, processing, transmission make sensitive. It requires protection against the unauthorized users. The networks had been globally useful for protecting the useful communication. The information has taken in the digital form of bits and bytes. To break the codes into pieces we use decryption. Hence, the critical information gets stored, processed and transmitted in digital form on systems. In military, government organizations they use cryptography techniques to guard the secret information. To create awareness for the common people the internet has brought effective cryptography technique. The algorithm is mathematical function used in encryption and decryption process. Public Key is made freely available to anyone to send a message. Private Key is kept secret from the unauthorized peoples.

II. TERMINOLOGY

1) Plain text: The message which is in original (unencrypted) format.
2) Cipher text: The message which is in encrypted format.
3) Cipher: It is a method of hiding words or text with encryption by replacing original letters with other letters.

A key gives us flexibility in using an encryption scheme. We can create different encryptions of one plain text message just by changing the key.



4) Encryption: The process of converting a plain text into a cipher text.
5) Decryption: The process of converting a cipher text into a plain text.

Alternatively, we use encrypt or decrypt instead of encode or decode.

6) Key: It is the transferring of information from cipher text to plain text.

III. SECURITY SERVICES

A. Confidentiality:

This is service provided to keep some content of the information accessible to only for the authorized peoples [2]. Here nobody can understand the information because it is protected from the un-authorizers.

B. Authentication:

This is a process of proving identity of the user. It confirms the receiver that data has been sent only by the verified sender. Authentication service has two varieties: Message authentication identifies the message system that has sent the message. Entity authentication is the assurance that data has been received from a particular entity.

C. Data Integrity:

This is a service ensures that the message cannot be changed from its original form [4]. The message can be changed from any of the unauthorized peoples. It just confirms whether the data is created, stored. Hence, recipient and sender will compare the message into the one who have received. Here if you want to modify it includes delete, create, storing purpose.

D. Non-Repudiation:

This is a mechanism used to prove that sender sends the message and the message was received by the authorized

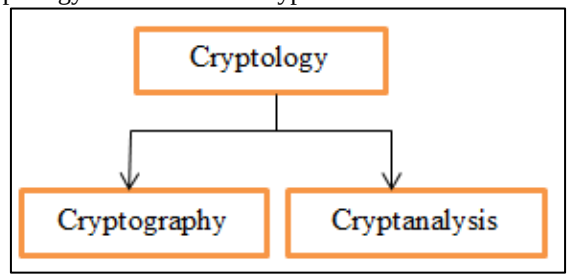
people, so the recipient cannot claim that the message was not sent. For e.g. once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

E. Access Control:

It is the process of preventing an unauthorized use of resources. This goal controls the resources in accessing. If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access. There are two types of access control. They are physical and logical.

IV. CRYPTOLOGY CONCEPTS

Cryptology is divided into 2 types:



The science of studying and breaking the secrecy of encryption algorithms is called as the cryptanalysis. The solving secret code is called as cryptology.

A. Types of Cryptosystem

The mechanism that carries out the encryption process is called cryptosystem. Cryptosystems is of two types:

- Symmetric Cryptosystems
- Asymmetric Cryptosystems

1) Symmetric Cryptosystems

Symmetric cryptosystem (private key cryptosystem) used only one key for both encryption and decryption of the data [3]. The key which is used for encryption and decryption is called as the private key. In a symmetric cryptosystem, the encrypted message is sent over private keys. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key [1] .Symmetric key ciphers are implemented as either block ciphers or stream ciphers. Symmetric are much faster than asymmetric cryptography. Symmetric encryption is the oldest and best-known technique.

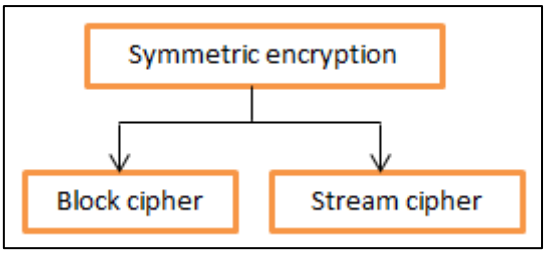
Advantages

- Symmetric key ciphers can also be combined to produce stronger ciphers.
- Symmetric cryptosystem uses password authentication to prove receiver's identity.
- A system only which possesses the secret key can decrypt a message.

Disadvantages

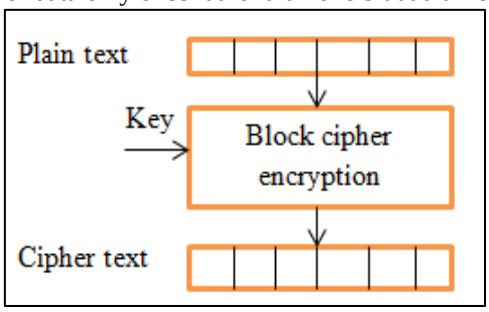
- The key must remain secret at both ends.
- In large networks, many key pairs have to be managed.
- It cannot provide digital signatures so that it cannot be rejected.

Symmetric encryption is of 2 types,



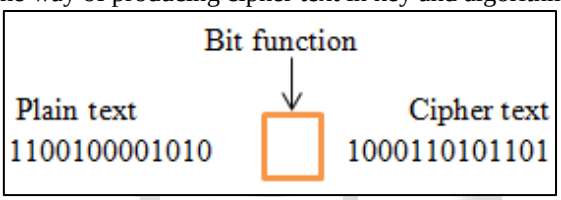
a) Block Cipher:

It is a method of encrypting that applies algorithm along with symmetric key to encrypt block of text. It is applied to a block of data only once rather than one bit at a time.



b) Stream Cipher:

The key and algorithm is applied to both in data stream, it is the way of producing cipher text in key and algorithm



2) Asymmetric Cryptosystems

Asymmetric cryptosystem (public key cryptosystem) is of two different keys. One key is used for the encryption and another for decryption of data. It provides more stability than public key. The key which is used for encryption is public. So it is called as called public key. The key used for decryption is secret. So it is called private key. The transmitter and the receiver both have two keys in a public key cryptosystem.

Advantages

- In public key, cryptography there is no need for exchanging keys.
- The primary advantage of public-key cryptography is increased security.
- It can provide digital signatures so that it can be rejected.

Disadvantages

- Key sizes are typically much larger.
- Public key cryptography does not have an extensive history in the public world.
- It costs more to encrypt and decrypt the message.

3) RSA Cryptosystem

RSA system invented by the scholars Rivest, Shamir and Adleman. This is one of the first cryptosystem. It is used to protect the transmission of the data. This is one of the algorithms which are used to encrypt and decrypt the message. Mainly it is used to secure the secure the message which is passed in insecure network. Firstly, generate RSA Key Pair. The peoples who are interested in communication use the encryption keys. This encryption will generate a pair of keys i.e., private key and public key.

Here is the process to generate the following keys.

a) Generate the RSA modulus (n)

Choose two large primes, p and q.

Calculate n=p*q. For strong unbreakable encryption, let n be large.

b) Find Derived Number (e)

Number e must be greater than 1 and less than (p − 1) (q − 1).

There must be no common factor for e and (p − 1) (q − 1) except for 1.Hence, two numbers e and (p – 1) (q – 1) are coprime. It forms the public key.

c) The pair of numbers (n, e) forms RSA public key.

Here n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find infinite time the two primes (p & q) used to obtain n. This is strength of RSA.

d) Generate the private key

Private Key d is calculated from p, q, e. For n and e, there is unique number d.

Number d is inverse of e modulo (p − 1) (q − 1). This means that d is the number less than (p − 1) (q − 1) i.e., when multiplied by e, it is equal to 1 modulo (p − 1) (q − 1).

Calculate mathematically as follows, de = 1 mod (p − 1) (q − 1)

Example:

To generating RSA Key pair is given below. (The primes p and q taken are small values. These values are high).

1) Choose two primes, p = 7 and q = 13. Thus, modulus n = p x q = 7 x 13 = 91.
2) Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p − 1) (q − 1) = 6 × 12 = 72, except for 1.
3) The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
4) Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
5) Check that d calculated is correct by computing: d x e = 29 × 5 = 145 = 1 mod 72
6) Public key is (91, 5) and private keys is (91, 29).

V. Conclusion

Cryptography is the best technology which keeps our information secure. We studied the various techniques and algorithm. The best algorithms are well studied in this paper. It protects the users by providing functionality for the encryption of the data. We studied about the different ciphers in symmetric key encryption and RSA algorithm in this paper. In future we will study about the other new technique which has evolved in our paper. Computers are used for many purposes such as banking, shopping, military and student records. Privacy is a critical issue in many of these applications. We have to make ensure that unauthorized parties cannot modify the messages. These parties cannot read the messages.

References

[1] [5] Shivani Sharma, Yash Gupta "Study on Cryptography and Techniques" International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2017

[2] Prashant singh, Pratik kr. Sharma, Tanuj kr. Aggarwal "Cryptography And Network Security Principles And Practices" International Journal Of Engineering And Computer Science Volume1 Issue 1 Oct 2012 Page No. 01-10

[3] A.Nath, S.Ghosh, M.A.Mallik, "Symmetric key cryptography using random key generator", Proceedings of International conference on SAM2010 held at Las Vegas (USA) 12-15 July,2010,Vol-2,P-239-244.

[4] Sarita Kumari "A research Paper on Cryptography Encryption and Compression Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919

