A SURVEY PAPER ON CRYPTOGRAPHY MECHANISMS AND ENCRYPTION TECHNIQUES

K. Tejaswini [1] G. Sai Ganesh[2] M. Vyshnavi [3]

[1,2&3] Student(B.Tech.), Department of Computer Science and Engineering, Vivekananda Institute of Technology and Science, Karimnagar, Telangana.

[1]email: teju.kodithyala@gmail.com

[2]email: saiganesh876@gmail.com

[3]email: vyshnavi.madishetti@gmail.com

1.ABSTRACT

In today's internet world security plays an important role in securing data from intruders. The susceptible nature of information against forthcoming threats has become a maladroit affair for the professionals of this field. Information security is the most extreme basic issue in guaranteeing safe transmission of data through web. Also network security issues are now becoming important as security is moving towards digital information era. As more and more users connect to the internet it attracts a lot of cyber-attacks. After noticing constant reports of data, theft and hacking, enhancing security of data has become mandatory. The encryption techniques and various algorithms are used to provide the required security to the applications. This paper deals with the overview on network security and various techniques through which network security can be enhanced i.e. Cryptography. Cryptography provides Confidentiality, Integrity, Non-repudiation and Authentication.

KEYWORDS: Encryption, Decryption, cryptography, Cipher text, Information Security, Threats.

2.INTRODUCTION

Today we are in a world where there is no area that does not use internet technology. The usage of technology has been increasing drastically day by day, which is in turn increasing the number of unauthorised users. They target, attack and destroy the network by using fake mails, fraud websites, viruses and illegitimate techniques. Their main intent is to interrupt the data or modify the data or even denial of service to the receiver exclusively in some cases.

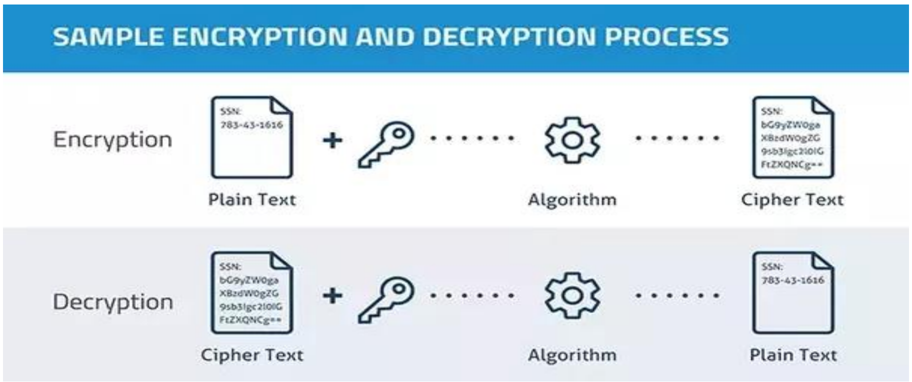

SAMPLE ENCRYPTION AND DECRYPTION PROCESS
Encryption
SSN: 783-43-1616
Plain Text
+
Algorithm
SSN: bG9yZWOga XBzdWOgZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
Decryption
SSN: bG9yZWOga XBzdWOgZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
+
Algorithm
SSN: 783-43-1616
Plain Text

Fig: Sample Encryption and Decryption Process

To accomplish security phenomenon, we follow the technique called Cryptography. The word cryptography belongs to greek origin, where ‘crypto’ means ‘hidden secret’ and ‘logy’ means ‘to write’. Cryptography is a study of techniques that are responsible for secure communication in the presence of third parties called adversaries or intruders. It is all about constructing and analysing protocols that prevent third parties from reading private messages. Various aspects of information security such as confidentiality, integrity, authentication, and non-repudiation are objectified in modern cryptography. Cryptography uses many areas of study like mathematics, computer science, electrical engineering, communication, physics etc.

a .APPLICATIONS OF CRYPTOGRAPHY:

- e-commerce.
- Chip based payment cards.
- Digital currencies.
- Computer passwords.
- Military communication.

b. BASIC NOMENCLATURE OF CRYPTOGRAPHY:

- **Plain text:** Plain text is a message which is in a form that is easily understood by humans. It can be also called as ‘clear text’.
  Eg: Hai.
- **Encryption:** Encryption is the process of encoding plain text or information in such a way that only authorised users can access it.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plain text.
- **Secret key:** The secret key is an input to the algorithm. The substitutions and transformations that are performed are completely based on the key.
- **Cipher text:** Cipher text is the scrambled message which is produced as output. It depends on plaintext and secret key.
- **Decryption:** Decryption is the process of decoding the cipher text into plain text with the help of secret key.
- **Decryption algorithm:** Decryption algorithm is essentially the encryption algorithm run in revere. It takes cipher text and the same secret key and produces the original plain text.

3. NETWORK ACCESS SECURITY MODEL:

A general model is used to protect information from illegitimate access. The readers are mostly concerned about the hackers who penetrate into the system and access the information. A hacker or intruder is one whose intent is to damage or crash the database or to exploit computer assets for financial gain.

A model basically designs tasks to provide security-

1. Design an algorithm.
2. Generate secret information.
3. Develop methods of distribution.
4. Specification of protocols.

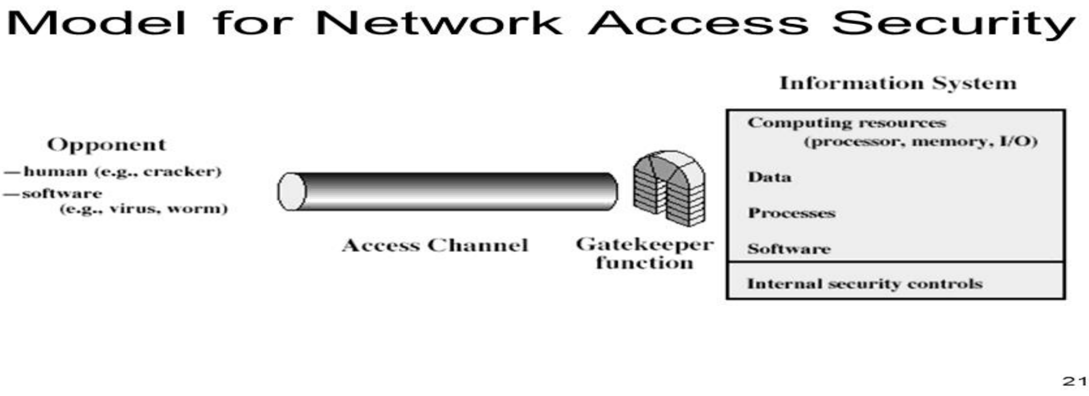

Model for Network Access Security
Opponent
—human (e.g., cracker)
—software (e.g., virus, worm)
Access Channel
Gatekeeper function
Information System
Computing resources (processor, memory, I/O)
Data
Processes
Software
Internal security controls
21

Fig: Model for Network Access Security

4.SECURITY SERVICES:

A service that enhances the security of the data processing systems and the information transfers of an organisation. The services are intended to counter security attacks. There are six services.

a. Confidentiality: Confidentiality ensures that the information in a computer system and transmitted information is accessible only to the authorised users. This type of access includes printing, displaying etc.

b. Authentication: Authentication ensures that the origin of the message is correctly identified and genuine, with an assurance that the identity is not false.

c. Integrity: It ensures that only authorised parties are able to modify computer system assets and transmitted information.

d. Non Repudiation: It requires that neither the sender nor the receiver of a message will be able to deny the transmission.

e. Access control: It requires that access to information resources is controlled by the target system.

f. Availability: It requires that computer assets be available to authorised parties when needed.

5. TYPES OF ENCRYPTIONS:

There are two types of techniques that are used in cryptography. They are

a.SYMMETRIC KEY CRYPTOGRAPHY:

It is a technique which allows the use of only one key for performing both encryption and decryption and the decryption of the message is shared over internet. It is also known as 'conventional method for encryption'.

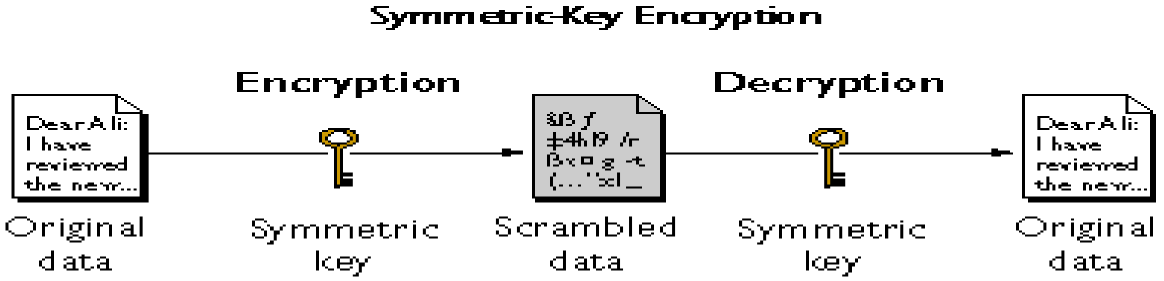


Fig: Symmetric key encryption

Symmetric encryption algorithm executes faster and is less complex. They are used for bulk data transmission. The hosts that are participating in the communication already have the secret key that is received through external means. The sender of the information will use the key for encrypting the message and the receiver will use the key for decrypting the message.

Some examples of symmetric algorithms are:

- DES
- 3DES
- AES
- RC4

b.ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric encryption is an encryption technique that uses a pair of keys i.e., 'private and public keys' for encryption and decryption. It uses public key for encryption of the message and private key for the decryption of the message.

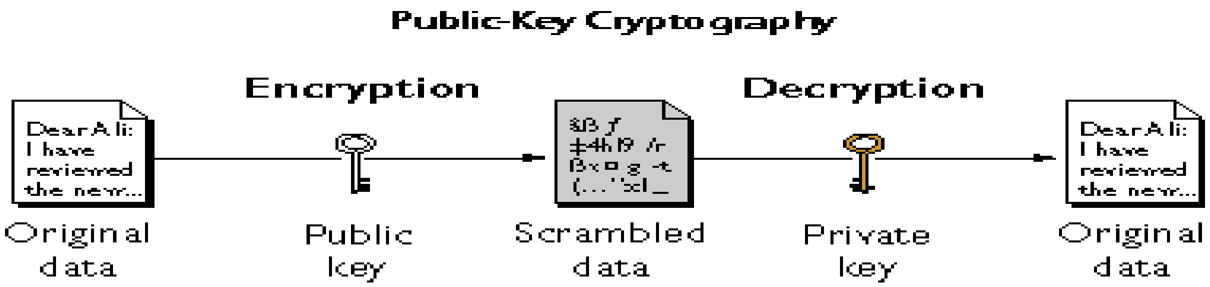


Fig: Public-Key Cryptography

The public key is freely available to anyone who is interested in sending the message. The private key is kept secret with the receiver of the message. Any message that is encrypted by public key has to be decrypted by matching the private key of corresponding public key.

If we want to provide security to the message then the private key is made available to the receiver, but if we need to provide authentication to the message then the private key is made available to the sender.

Its execution is slow. These are complex in nature and have high computational burden. Because of that reason, it is mainly used for securely exchanging the keys instead of the bulk data transmission.

Examples of asymmetric key cryptography:

- Diffic-Hellman algorithm
- RSA algorithm.

6.TYPES OF ENCRYPTIONS ALGORITHMS:

a.Data Encryption Standard [DES] Algorithm:

DES is published by National Institute of Standards and Technology [NIST]. It is an implementation of Feistel cipher and works by encrypting groups of 64 message bits, which is same as 16 hexadecimal numbers. DES uses 'keys' which are also 16 hexadecimal numbers long or apparently 64 bits long. However, every 8th key bit is ignored. So the effective key size is 56 bits (+8 parity bits). It has a block size of 64 bits and 16 rounds.

b.Advanced Encryption Standard [AES] Algorithm:

AES is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. It's supports both hardware and software and has a key length that varies from 128, 192 and 256 bits. It has block size of 128 bits and 10, 12 or 14 rounds depending on the key size.

c.Triple Data Encryption Standard [3DES] Algorithm:

In cryptography, triple DES is a symmetric key block cipher, which applies the block cipher three times to each block. It was presented in 1998 and was described as s standard ANS X9.52. It has a key size of 168, 1112 or 56 bits and block size of 64 bits and 48 equivalent DES rounds.

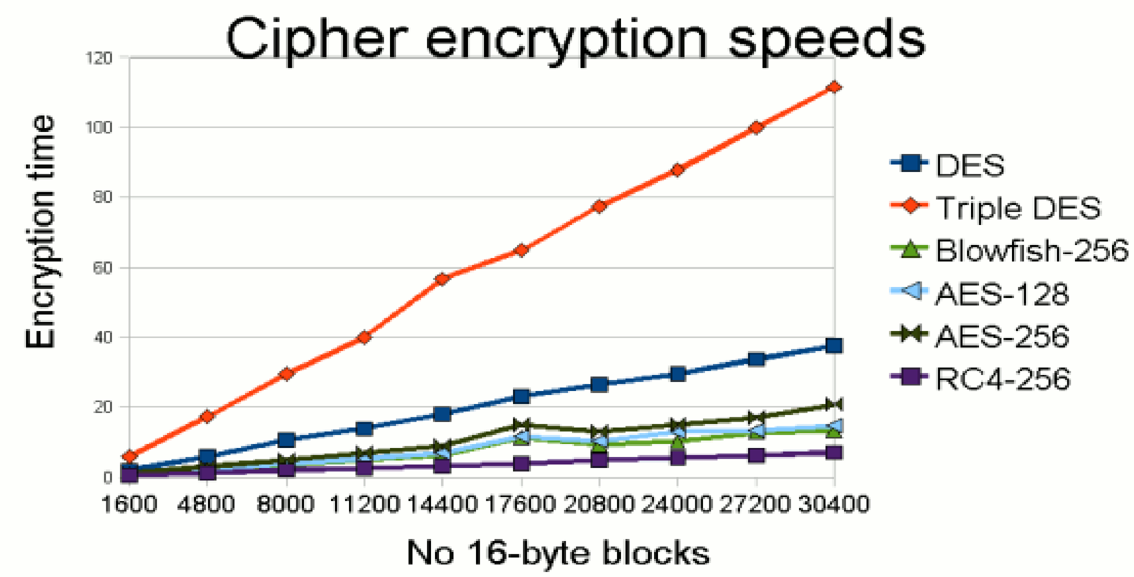
d.Rivest Cipher 4 [RC4] Algorithm:

RC4 algorithm was developed by Ronald Rivest. It comes under the category of shared key stream cipher algorithm which requires a secure exchange of shared key. This algorithm is used by standards like IEEE 802.11. it uses 40 and 128-bit keys. Its key size ranges from 40-2048 bits. It has only 1 round.

e.Blowfish Algorithm:

Blowfish is a symmetric block cipher encryption algorithm. It was designed by Bruce Scheier in 1993. It can be used as a replacement for DES algorithm. It has a key size ranging from 32 to 448 bits and a block size of 64 bits. It has a total of 16 rounds.

COMPARISION OF ENCRYPTION ALGORITHMS:



7.FUTURE PROSPECTS:

To overcome certain drawbacks of the existing encryption algorithms, development of more secure algorithms is on process. Some of those algorithms are

- Honey Encryption
- Quantum Cryptography

a.Honey Encryption:

Honey encryption is a data encryption in which if an incorrect plaintext is provided when the intruder decrypts the data with a false key. Thus, it makes it difficult for the intruder to know whether he has provided the correct key or not. It was developed by Ari Julis and Thomas Ristenpart.

b.Quantum Cryptography:

Quantum cryptography is the first cryptography mechanism that uses photons to transmit the messages. It is the most secure encryption technique in which the intruder has zero knowledge about the transmission. It relies on two major elements of quantum mechanics

i.e., Heisenberg's un certainity principle and principle of photon polarisation.

8.CONCLUSION:

As there is a rapid increase in the emerging technologies, there is also a fatal increase in the rate of cybercrimes. So, we are in a vital need of securing the information from adversaries. We need information security to reduce the risk of unauthorised information disclosure, modification, and destruction. So, in order to achieve this, we use different types of encrypting algorithms. This paper provides different types of encryption techniques like AES, DES, 3DES, Blowfish and RC4 and their efficiencies.

This paper also includes the upcoming prospects in cryptography, in which the cons of the existing algorithms are removed and vulnerability is reduced. These algorithms can be used to secure the sensitive information.

9.REFERENCES:

[1] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram "Comparative analysis of performance efficiency and security measures of some encryption algorithms".

[2] S. Pavithra, Mrs. E. Ramadevi "Study and performance analysis of cryptography algorithms".

[3] Prof. Vasanthi S, Surekha M H, Vachana G N, Vandana C, Vathsala V "Cryptography: a review".

[4] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubam Garg, Shudhanshu Yadav "Methods for protection of key in private key cryptography".

[5] Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal "A review paper on network security and cryptography".

[6] William Stallings "Cryptography and network security principles and practices", second edition.