International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Cryptography in Network Security

SEEPANSHU RAJPUT

Department of Computer Science and Engineering, ABES Institute of Technology Ghaziabad, India

---

Abstract - *This paper aims to provide broad view of usage of cryptography in network security. Cryptography is defined as the science of protecting the data. On other hand network security is the process of keeping the information private, secret and secure from unauthorized and illegal access. Cryptography and network security is used to protect network and data communication takes place over wireless network and data which is stored in our systems. Security in this modern scenario has become a more and more sensible and critical issue, because the usage of computers and data networks go on increasing. Network security and cryptography is the subject which provides solutions to protect our information and data in digital form and to avoid security attacks and offers security services. Cryptography and network security is used in various applications like banking, shopping, government agencies, organization, military, secret services, enterprises, business, and in daily lives of peoples. In Cryptography various techniques and algorithms are used to provide security to networks and data. In this paper, we discussed about various encryption and decryption techniques, cryptographic principles, cryptosystem types and cryptographic model and its algorithm. There are six main security services which are availability, confidentiality, authentication, integrity, non-repudiation and access control. There are various security threats for our information like interception, interruption, unauthorized access and modification.*

Keywords - Cryptography, Compression, Network Security, Encryption, Decryption

1. INTRODUCTION

The present our whole globe is relying upon web and its application for their all aspects of life. Here comes the prerequisite of making sure about our information by methods for cryptography. Network security implies an insurance of the system resources. It is responsible for providing security to all the information passed over the internet from one computer to other.

The term cryptology has its beginning in Greek kryptos logos, which means "hidden word." Cryptography is the science of securing information and protecting data. It is the process of using algorithms and mathematics to encrypt and decrypt data. It is the push to make a protected processing stage. Cryptography is one of the rising innovation utilized for giving security to information. The approved client ought to give client ID and secret key or any other special information to get to made sure about data. It used to protect the data increasingly secure and safe. There are four organize security issues, non-repudiation, mystery, classification and validation. Cryptography allows us to store sensitive information or transmit it across unreliable systems and insecure networks.

2. SECURITY SERVICES

Network security issues can be separated generally into six interlaced territories:-

- **Authentication** - affirmation that the conveying substance is the one guaranteed.
- **Access Control** - protection of illegal use of a resource.
- **Data Confidentiality** - anticipation of the unapproved utilization of an asset.
- **Data Integrity** - affirmation that information got is as sent by an approved substance.
- **Non-Repudiation** - assurance against refusal by one of the gatherings in a correspondence.
- **Availability** - ensures that frameworks, applications and information are accessible to clients when they need them.

3. SECURITY ATTACKS

1. **Passive Attack** - the goal of attacker is to obtain the information that is being transmitted.

Some of the dangers under this classification are :-

- Unauthenticated access
- Unauthorized access
- Spoofing (fabrication or impersonation)
- Attack (making resources unavailable)
- Malicious software

2. **Active Attack** - it involves some modification of data stream or the creation of false data stream.
   Some of the dangers under this classification are:-

- Interception or sniffing
- Modification
- Denial of action (repudiation)

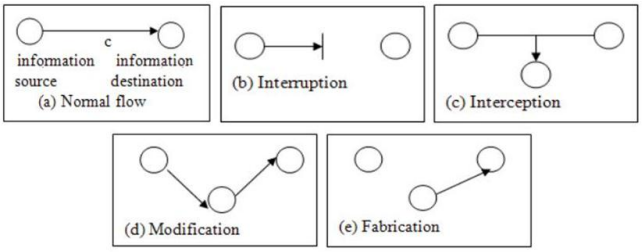

Fig - 1: Security Attacks

4. SECURITY MECHANISM

- **Specific Security Mechanisms** - encipherment, advanced marks, get to controls, information honesty, confirmation trade, traffic cushioning, directing control, legally approbation.

- **Pervasive Security Mechanisms** - confided in usefulness, security marks, occasion discovery, security review trails, security recuperation.

Three essential structure squares are utilized :-

Encryption is utilized to give classification, can give confirmation, mystery and trustworthiness insurance. Digital signatures are utilized to give verification, uprightness security, and non-denial. Checksums/hash calculations are utilized to give honesty insurance, can give validation. At least one security instruments are joined to give a security administration.

5. CRYPTOGRAPHY PROCESS

- **Plain text** - The messages to be encoded known as plain content or clear content.
- **Encryption** - The way toward delivering cipher content is called encryption.
- **Cipher text** - Encoded message is called cipher content.
- **Decryption** -The procedure of recovering the plain content from the cipher content is called decoding.

Encryption and unscrambling normally use a key, for instance the messages to be encoded are changed by a limit that is parameterized by a key. The forte of breaking figures is called cryptanalysis. The forte of considering figures and breaking them is known as cryptology.

6. CRYPTOGRAPHIC PRINCIPLES

- **Redundancy** - All the encoded message contain some repetition, there is no need of understanding the message by data.

- **Freshness** - Timestamp is utilized in each message. For example the time stamp is of 10sec fore very message. The recipient keeps the message around 10sec to get the message and channel the yield inside that 10sec. The message surpasses the timestamp it is toss out.

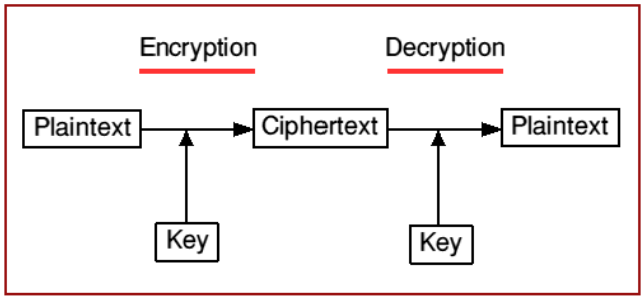

Fig - 2: Cryptography

Ciphers are broken into two categories :-

1. **Substitution ciphers** - is a technique for encoding by which units of plaintext are supplanted with cipher text.
2. **Transposition cipher** - is a strategy for encryption by which the positions held by units of plaintext are moved by a normal framework, so that the cipher text comprises a change of the plaintext.

7. TYPES OF CRYPTOGRAPHY

1. **Secret Key Cryptography** - The point of process when just one key is utilized for encryption and decoding process, it is called secret key cryptography. The key is called secret or shared key. It is also called symmetric cryptography. For Example, DES, Triple DES, AES, and RC5.

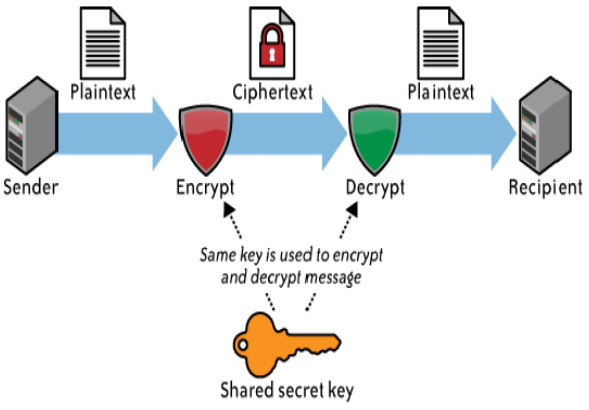

Fig – 3: Secret Key Cryptography

Advantages

- Widely used and very popular.
- Faster than public key cryptography.
- Cipher text is compact.

Disadvantages

- Administration of keys become extremely complicated.
- Key can be captured by hackers.

2. **Public Key Cryptography** - At the point when two unique keys are utilized for encryption and decoding process, it is called open key cryptography. Public key is utilized for encryption procedure and private key is utilized for unscrambling process. It is also called asymmetric cryptography. For example, RSA and Elliptic Curve.

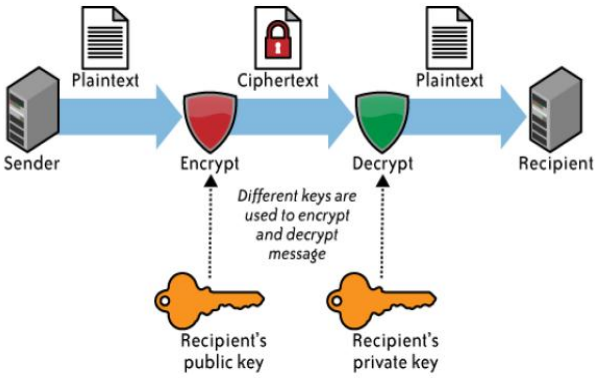

Fig – 4: Public Key Cryptography

Advantages

- Progressively secure and simple to arrange the frameworks.
- Supports non-repudiation.

Disadvantages

- Slower compared to secret key cryptography.
- Cipher text content is lot bigger than plain text content.

3. **Hash Cryptography** - Hash algorithms are also known as one-way transformations. It is a scientific change that takes a message of discretionary length and processes from it a fixed length number. It is an enhancement over the public key plan. For improving the asymmetric cryptography, one-way hash function is included in the process. A single direction hash work takes variable length input. For this situation, a message of any length, even thousands or a huge number of bits and produces a fixed-length yield, 160-bits. The hash work guarantees that, if the data is changed in any capacity even by only the slightest bit a completely extraordinary yield esteem is created. Up to a protected hash work is utilized, its absolutely impossible to take somebody's mark starting with one record and join it then onto the next, or to adjust a marked message in any capacity. The smallest change in a marked archive will cause the computerized signature confirmation procedure to come up short.

Fig - 5: Hash Cryptography

8. ADAVNCE CRYPTOGRAPHIC TECHNIQUE

Over the recent year's steganography has been the wellspring of a ton of conversation. Steganography is one of the central ways by which information can be kept secret. Steganography shrouds the presence of a message by transmitting data through different transporters. Its will probably forestall the discovery of mystery message.

8.1 What is Steganography ?

The word steganography comes from the Greek words "stegnos" meaning covered or mystery and "graphy" meaning compossng or drawing and virtually suggests that hidden writing. Stegenography uses techniques to speak data in an exceedingly approach that's hidden.

Steganography is the procedure of concealing mystery information inside a customary, non-mystery, record or message so as to maintain a strategic distance from location; the mystery information is then separated at its goal. The utilization of steganography can be joined with encryption as an additional progression for covering up or ensuring information. The most widely recognized utilization of steganography is concealing data picture or sound inside the data of another document by utilizing a stegokey, for example, secret word is extra data to additionally disguise a message.

9. APPLICATIONS

Application of Cryptography -

1. Defense Services
2. Secure Data Manipulation
3. E – Commerce
4. Business Transactions
5. Internet Payment Systems
6. Pass Phrasing Secure Internet Comm.
7. User Identification Systems
8. Access Control
9. Computational Security

10. Secure access to Corp Data
11. Data Security

Application of Network Security -

1. Banking
2. Shopping
3. Filling their tax returns

10. RELATED WORKS

- **DES** -

DES is a square figure that utilizations shared mystery key for encryption and unscrambling. DES calculation as depicted by Davis R takes a fixed length of string in plaintext bits and changes it through a progression of activities into figure content piece string of a similar length and its each square is 64 bits.

- **3DES** -

3DES is an improvement of DES and it is 64 piece square size with 192 bits key size. In this standard the encryption of technique is like the one in the first DES and increment the encryption level and the normal safe time.

- **AES** -

AES then again which scrambles every one of the 128 bits in a single emphasis. This is one motivation behind why it has an equivalently modest number of rounds. AES encryption is quick and adaptable. It tends to be actualized on different stages particularly in little gadgets

- **Blowfish** -

Blowfish is one of the most widely recognized open space encryption calculation gave by Bruce Schneier one of the universes driving cryptologists, and the leader of counterpane systems and a counseling firm represent considerable authority in cryptography and PC security.

Blowfish scrambles 64-bits square figure with assortment length key and its contains two sections :-

Data Encryption - It includes the cycle of a straight forward capacity of 16 times. Each round contains a key ward change and information subordinate substitution.

Subkey Generation - It converts the key upto 448 bits long to 4168 bits.

- **RSA** -

RSA is invented by Rivest, Shamir, Adleman. RSA includes two keys - public key which is used for encoding and private key which is used for decoding the secret data.

Algorithm	Created by	Key Size (in bits)	Block Size (in bits)
DES	IBM in year 1975	56	64
3DES	IBM in year 1978	112 (or) 168	64
AES	Joan Daemen and Vincent Rijmen in year 1998	256	128
Blowfish	Bruce Schneier in year 1993	32 (or) 448	64

Table -1 : Comparison of Cryptographic Algorithm

11. CONCLUSION

Cryptography ensures clients by giving usefulness to the encryption of information and confirmation of different clients. This innovation lets the collector of an electronic message check the sender, guarantees that a message can be perused distinctly by the expected individual, and guarantees the beneficiary that a message has not be modified in travel. The cryptography attacking methods like cryptanalysis and brute force attack.

Network security is a troublesome subject. Everybody has an alternate thought of what "security" is, and what levels of hazard are satisfactory. The key for building a safe system is to characterize what security intends to your association. Activities and frameworks would then be able to be separated into their parts, and it turns out to be a lot more straight forward to choose whether what is proposed will struggle with your security arrangements and practices. Security is everyone's the same old thing, and just with everybody's collaboration, astute approach, and reliable practices, will it be feasible.

12. FUTURE SCOPE

As a last word, we realize that future will be organized all over .Hence "System Security" is picking up significance all around. So with everybody's activity and with steady practices, will it be feasible. Presumably, Science and Technology creates step by step. We have to use the headways in developing fields of Science and Technology to think of profoundly made sure about and reliable practices with the goal that we can difficulties at the Bad folks, who need to separate our layers of security safeguard.

There are various newly and advanced developed cryptography techniques which provide security and helps us to develop secure system. Quantum cryptography is better and advanced than the classical cryptography in various ways. Quantum cryptography based on Heisenberg uncertainty principle. Steganography is one of the central ways by which information can be kept secret. Steganography shrouds the presence of a message by transmitting data through different transporters. Its will probably forestall the discovery of mystery message.

REFERENCES

[1]. BalaIyer, Sharad Mehrotra, Einar Mykletun, Gene Tsudik, and Yonghua Wu, A Framework for Efficient Storage Security in RDBMS, Advances in Database Technology - EDBT 2004Volume 2992 of the series Lecture Notes in Computer Science pp 147-164.

[2]. Alan O. Freier, Philip Karlton, and Paul C. Kocher, the SSL protocol version 3.02, 1996.

[3]. T. Dierks and E. Rescorla, the TLS protocol version 1.2, 2006.

[4]. Brintha Rajakumari, S. Nalini, An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[5]. Udayakumar, R., Khanaa, V., Saravanan, T., Saritha, G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[6]. Preneel, B. (2010, September). Cryptography for network security : failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54). Springer, Berlin, Heidelberg.

[7]. Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science, 6(4).

[8]. Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495.

[9]. Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763-770.

[10]. Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

[11]. Dhamdhere Shubhangi, T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

[12]. Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.

[13]. Kaur, S., Kaur, R., & Raina, C. K. (2017). Review on Network Security and Cryptography.

[14]. Computer Networks and Network Security by Andrew S. Tanenbaum.

[15].Fighting Steganography detection by Fabian Hansmann.

[16]. Applied Cryptography by Bruce Schneier, John Willey and Sons Inc,

[18]. Networks for Computer Scientists and Engineers by Youlu Zheng, Shakil Akhtar.