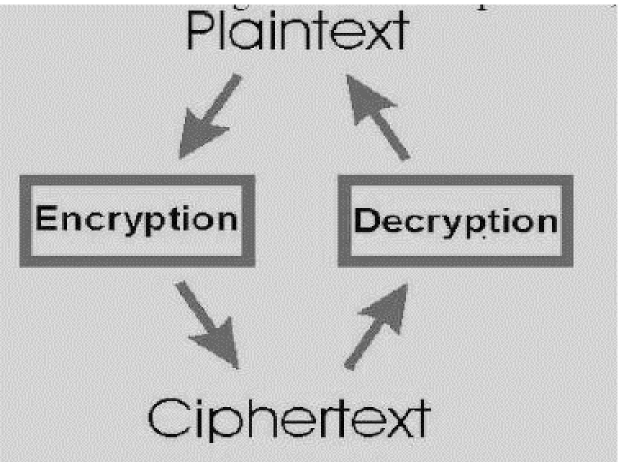
A Review Paper on Network Security and Cryptography

Mohith C M , Anujna Y M

Abstract: With the advent of the World Wide Web and the emergence of ecommerce applications and social networks, organizations across the world generate a large amount of data daily. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Also, network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-attacks. It's required to protect computer and network security i.e., the critical issues. The pernicious hubs make an issue in the system. It can utilize the assets of different hubs and safeguard the assets of its own. In this paper we provide an overview on Network Security and various techniques through which Network Security can be enhanced i.e., Cryptography.

Introduction:

Network Security: - Earlier computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers, faxing. But in this modern world, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem. The requirements of information security within an organisation have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. With the introduction of computer, the need for automated tools for protecting files and other information stored on the computer became an evident. This is especially the case for a shared system, such as time-sharing system and the need is even more acute for systems that can be accessed for a public telephone or a data network. The generic name for the collection of tools to protect data and high protection
levels against malicious attack is "computer security".



The testing issue is the way to successfully share scrambled information. Encode message with unequivocally secure key which is known just by sending and

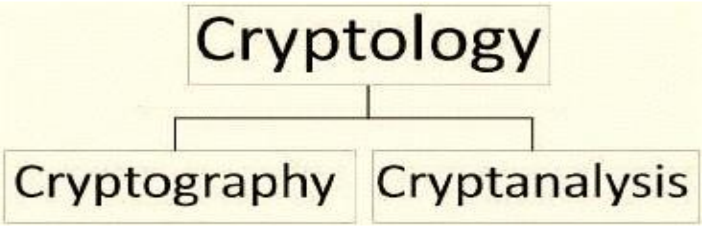
beneficiary end is a noteworthy perspective to get strong security in sensor organize. The safe trade of key amongst sender and recipient is a lot of troublesome errand in asset imperative sensor arrange. information ought to be scrambled first by clients before it is outsourced to a remote distributed storage benefit and both information security and information get to security ought to be ensured to such an extent that distributed storage specialist organizations have no capacities to unscramble the information, and when the client needs to pursuit a few sections of the entire information, the distributed storage framework will give the availability without recognizing what the segment of the encoded information came back to the client is about. This paper surveys different system security and cryptographic methodologies.

1.1 Characteristics of Modern Cryptography:

We can characterize modern cryptography in 3 ways:

Classic Cryptography	**Modern Cryptography**
It manipulates fixed characters like letters and digits directly.	It operates on binary bit sequences.
The techniques working for coding was kept secret and only the members involved in communication knew about them. It was mainly based on ‘security through obscurity’.	It depends on arithmetical algorithms for coding the information. Confidentiality is obtained through a secret key. e difficulty of algorithm and the secret key makes the malicious hacker difficult to access the data even though they have the code.
requires the entire cryptosystem for communicating in secret.	Modern cryptography require parties paying attention in secure message to have the secret key only.

1.2 Subdivision of Cryptography:



1.3 What is Cryptography? *Cryptography is the art and science of making a cryptosystem that is able of providing information safety.*

Cryptography is used to secure the digital information. It is based on algorithms which secures the information.

1.4 What is Cryptanalysis?

The art or process of deciphering coded messages without being told the key.

Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. Cryptanalysis is generally thought of as exploring the weaknesses of the underlying mathematics of a cryptographic system, but it also includes looking for weaknesses in implementation, such as side channel attacks or weak entropy inputs.

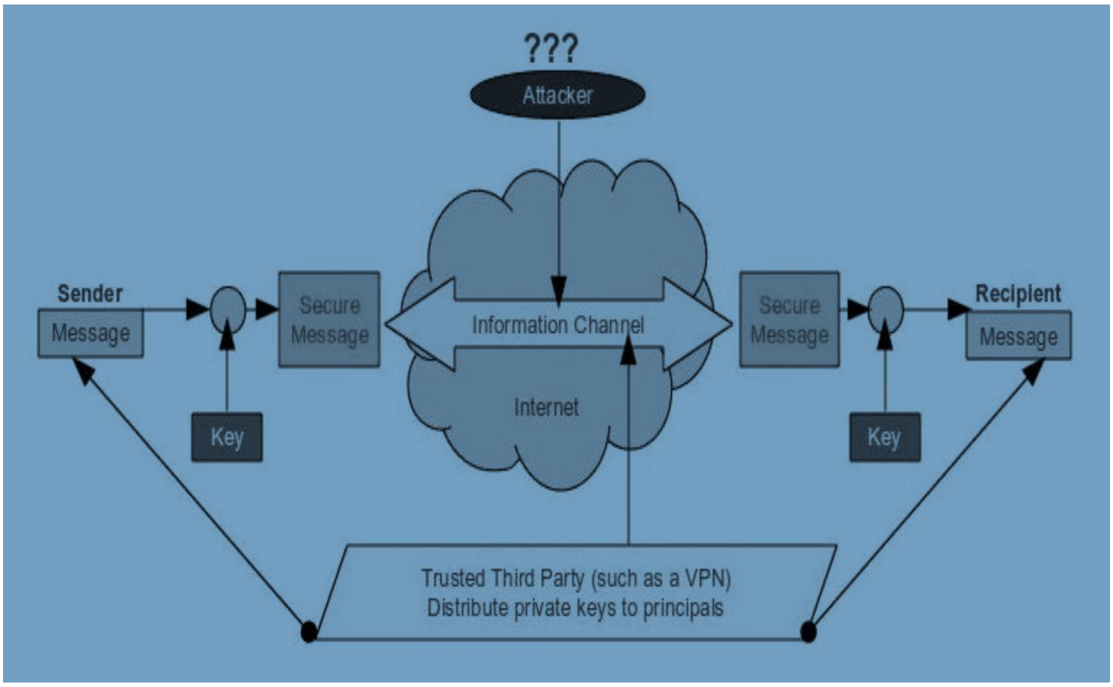
There are various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation

1.5 Confidentiality

Confidentiality is the basic security service provided by cryptography. It is a safety service that keeps the in order from an unauthorized person. It is from time to time referred to as privacy or secrecy. Confidentiality can be achieve through many means starting from physical secure to the use of arithmetical algorithms for information encryption.

1.6 Data Integrity

It is safety service that deals with identify any alteration to the data. The information may get modified by an illegal entity intentionally or accidently. Integrity service confirm that whether data is whole or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the change of data but provides a means for detect whether data has been manipulate in an illegal manner.



1.7 Authentication

Authentication provides the recognition of the originator. It confirm to the receiver that the data established has been sent only by an recognized and established sender. Authentication service has two variants –

- Message authentication identifies the creator of the message with no regard router or scheme that has sent the message.
- Entity authentication is pledge that data has been received from a specific entity, say a exacting website.
- Apart from the originator, authentication may also provide declaration about other parameter related to data such as the date and time of formation/transmission.

1.8 Non-repudiation

In digital security, non-repudiation means: A service that provides proof of the integrity and origin of data. An authentication that can be said to be genuine with high confidence. Proof of data integrity is typically the easiest of these requirements to accomplish.

Non-repudiation is a property that is most attractive in situations where there are probability of a argument over the exchange of data. For example, once an arrange is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation repair was enable in this transaction.

1.9 A quick guide about Asymmetric Encryption.

Ever since the market transition from physical to digital is increasing, the security issue is becoming graver than ever. Digitalization has completely enhanced the data collection technique by making it easy to preserve, access and share. Computers and hard disks have become storages of data and eliminated the need for files and folders.

But this data is at risk of being invaded by hackers and cyber-criminals, either from their storage locations or during the transfer process.

The best way to secure in-transit data is to encrypt the same by installing an SSL certificate.

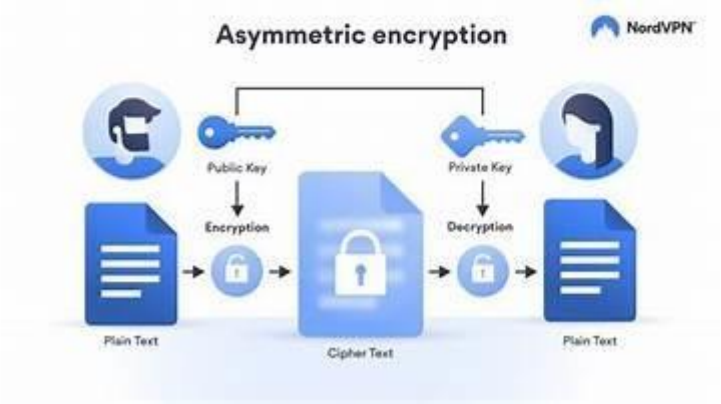
There are two types of encryption.

- Symmetric Encryption
- Asymmetric Encryption

1.10 What Is Encryption?

Encryption is a data protection process, which encodes the information using cryptographic keys and encryption algorithms and creates a non- readable text (ciphertext).

The beauty of encryption security is that only the authorized recipient can decode and access the message since it requires a secret key for the same, which is with the recipient only.



The above image clearly states how the encryption key encrypts the data into an encrypted ciphertext and how the decryption key deciphers the message into plain text again.

There are two types of encryptions, and hence the keys used in the process are either symmetric or asymmetric depending on the type of encryption used.

The digital security key is a string of characters.

Conclusion:

Network security should be a high priority for any organization that works with networked data and systems. In addition to protecting assets and the integrity of data from external exploits, network security can also manage network traffic more efficiently, enhance network performance and ensure secure data sharing between employees and data sources.

There are many tools, applications, sand utilities available that can help you to secure your networks from attack and unnecessary downtime.
Forcepoint offers a suite of network security solutions that centralize and simplify what are often complex processes and ensure robust network security is in place across your enterprise.

Reference:

[1] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[2] Ritu Pahal, Vikas Kumar,”Efficient implementation of AES”, International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[3] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014