International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307
Theme : Technical Note

# A Review on Cryptography

**Rizwan Maqbool, Mohammad Saleem, Tajamul Ali, C. K. Raina**
Adesh Institute of Technology, Chandigarh, Kharar, Punjab, India

## ABSTRACT

With the appearance of the globe Wide net and also the emergence of e-commerce applications and social networks, organizations across the globe generate an oversized quantity of knowledge daily. Data security is that the utmost important issue in guaranteeing safe transmission of knowledge through the web. Conjointly network security problems square measure currently turning into necessary as society is moving towards digital modern era. As a lot of and a lot of users hook up with the web it attracts plenty of cyber-criminals. It includes authorization of access to data in a very network, controlled by the network administrator. The task of network security not solely needs guaranteeing the protection of finish systems however of the whole network. In this paper, an effort has been created to review the varied Network Security and cryptanalytic ideas. This paper discusses the state of the art for a broad vary of cryptanalytic algorithms that square measure utilized in networking applications.

**Keywords:** Network Security, Cryptography, Decryption, Encryption

## I. INTRODUCTION

Internet has become more and additional widespread, if associate degree unauthorized person is in a position to induce access to the present network, he cannot solely spy on us however he will simply wash up our lives. Network Security & Cryptography could be a construct to guard network and data transmission over wireless network. A network security system usually depends on layers of protection and consists of multiple elements as well as networking observance and security code additionally to hardware and appliances.

All elements work along to extend the general security of the pc network. Security of information will be done by a method known as cryptography. therefore one willsay that cryptography is associate degree rising technology, that is vital for network security.

Cryptography is that the study of data concealment and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication. People who study and develop cryptography are called cryptographers. The study of how to circumvent the use of cryptography for unintended recipients is called cryptanalysis, or code breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella term cryptology, encompassing the entire subject. In observe, "Cryptography" is additionally usually accustomed ask the sector as a full, particularly as associate degree engineering science. At the dawn of the twenty one century in associate degree ever additional interconnected and technological world cryptography began to be omnipresent furthermore because the reliance on the advantages it brings particularly the hyperbolic security and verifiability.

Cryptography is that the science of writing secretly code. Alot of usually, it's regarding constructing and analyzing protocols that block adversaries; numerous aspects in info security like information confidentiality, information integrity, authentication, and non-repudiation are central to trendy cryptography. modern cryptography exists at the intersection of the disciplines of arithmetic, engineering, and applied science.

Applications of cryptography embrace ATM cards, pc passwords, and electronic commerce. the event of the globe Wide internet resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely associated with the disciplines of science and cryptanalytics. Techniques used for decrypting a message with none data of the encoding

details fall under the realm of cryptanalytics. cryptanalytics is what the common man calls "breaking the code." The aras of cryptography and cryptanalytics along are referred to as science. encoding is that the method of changing normalinfo (called plaintext) into unintelligible text (called ciphertext). decipherment is that the reverse, in alternative words, moving from the unintelligible ciphertext back to plaintext. Cryptosystem is that the ordered list of components of finite potential plaintexts, finite potential cyphertexts, finite potential keys, and also the encoding and decipherment algorithms that correspond to every key.

## II. TYPES OF SECURITY ATTACKS

**Passive Attacks**

This type of attacks includes observation or observance of communication. A passive attack makes an attempt to find out or build use of data from the system however doesn't have an effect on system resources. The goal of the opponent is to get info that's being transmitted.

Sort of passive attacks:

**Traffic Analysis:**The message traffic is distributed associate degree received in an apparently traditional fashion, and neither the sender nor receiver is aware that a 3rd party has browse the messages or ascertained the path.

**Release of Message Contents:**browse contents of message from sender to receiver

**Active Attacks**

An active attack tries to change system resources or have an effect on their operation. It involves some modification of the information stream or the creation of a false stream.

Varieties of active attacks:

**Modification of Messages:** some portion of a legitimate message is altered, or that messages area unit delayed or reordered.

**Denial of Service:** associate degree entity could suppress all messages directed to a selected destination

**Replay:** It involves the passive capture of a knowledge unit associate degreed its resulting retransmission to providean unauthorized impact.

**Masquerade:** It takes place once one entity pretends to be a unique entity.

**Security Services**

**Data Integrity**

It will apply to a stream of messages, one message, or chosen fields inside a message. A loss of integrity is that the unauthorized modification or destruction of data.

**Data Confidentiality**

Preserving licensed restrictions on info access and revealing, as well as suggests that for safeguarding personal privacy and proprietary info. A loss of confidentiality is that the unauthorized revealing of data.

**Authenticity**

Provide authentication to any or all the node and base station for utilizing the out there restricted resources.It additionally ensuresthat solely the licensed node will participant for the communication.

**Non repudiation**

It prevents either sender or receiver from denying a transmitted message. Thus, once a message is shipped, the receiver can prove that the alleged sender if truth be told sent the message. Similarly, once a message is received, the sender will prove that the alleged receiver if truth be told received the message.

**Access Control**

It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

## III. DATA ENCRYPTION

A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique. Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a

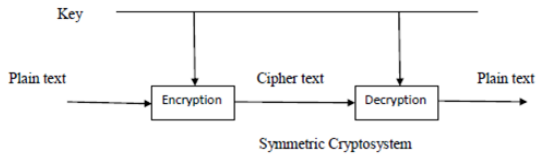
time. Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

## IV. DATA DECRYPTION

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

## V. SYMMETRIC KEY CRYPTOGRAPHY

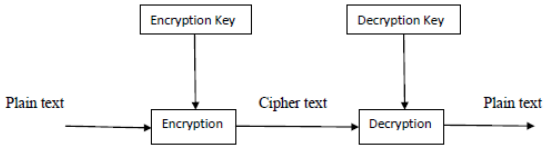
In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.



Symmetric Cryptosystem

## VI. ASYMMETRIC KEY CRYPTOGRAPHY

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.



Asymmetric Cryptosystem

## VII. COMPRESSION

Data compression offers an attractive approach for reducing communication costs by using available bandwidth effectively. Compression algorithms reduce the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs etc. Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time. Many methods are used for this purpose, in general these methods can be divided into two broad categories: Lossy and Lossless methods. Lossy Compression generally used for compress an images. In this original data is not identical to compressed data that means there is some loss e.g. Block Truncation Coding, Transform Coding, etc... Lossless Compression used for compress any textual data.

## VIII. CONCLUSION

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified.

## IX. REFERENCES

[1]. Swarnalatat Bollavarapun and Rucchita Sharma- Data Securityy using Compression and Cryptography Techniiques‖

[2]. Manoj Patiil, Prof. Vinay Saahu-A Survey of Compressionn and Encryptionn Techniques fo SMS
[3]. Bobby Jaasuja and Abhiishek Pandya-Cryptoo-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding
[4]. https://msdn.miicrosoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx
[5]. https://www.techopeedia.com/definition/1773/decryption
[6]. www.computerhoope.com/jargon/d/decrypti.htm
[7]. https://en.wikipediia.org/wiki/Cryptography
[8]. https://www.techoopedia.com/definition/25403/encryption-key
[9]. http://searchsecurity.teechtarget.com/definition/private-key
[10]. https://www.tutoriialspoint.com/cryptography/cryptography_tutorial.pdf