# CRYPTOGRAPHY & NETWORK SECURITY ASSIGNMENT.

Name : Narmatha N

Reg No : 2015056

## CRYPTOGRAPHY :

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain text messages. The simplest method uses the symmetric or "secret key" system.

## Real time example of public key cryptography :-

Email encryption is a method of securing the content of emails from anyone outside of the email conversation looking to obtain a participant's information. In its encrypted form, an email is no longer readable by a human. Only with your private email key can your emails be unlocked and decrypted back into the original message.

Email encryption works by employing something called public key cryptography. Each person with an email address has a pair of keys associated with that email address, and these keys are required in order to encrypt or decrypt an email. One of the keys is known as "public key", and is stored on a keyserver where it is tied to your name and email address and can be accessed by anoyone. The other key is your private key, which is not shared publicly with anyone.

When an email is sent, it is encrypted by a computer using the public key and contents of the email are turned into complex, indecipherable scramble that is very difficult to crack. This public key cannot be used to decrypt the send message, only to encrypt it. only the person with the proper corresponding private key has the ability to decrypt the email and read its contents.

## Authentication / Digital Structures :-

Authentication is any process through which one proves and verifies certain information. Sometimes one may want to verify the origin of a document, the identity of the sender. the time and date a documents was sent and / or signed the identity of a computer or user, and so on. A digital signature is a cryptographic means through which many of these may be verified. The digital signature of a document is a piece of information based on both the document and the signer's private key. It is typically created through the use of hash function and a private signing functions.

Time stamping:-

Time stamping is a technique that can certify that a certain electronic document or Communicatio existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allows the sender to get a message receipted by another party without revealing any information about the message to the other party.

Time Stamping is very similar to sending a registered letter through the U.S mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include patent applications, copyright archieves, and contracts. Time stamping is a critical application that will help make the transition to electronic legal documents possible.