CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY

Mr.Kaushal Kishor

Hi-Tech Institute of Engineering College GZB.

Mr.Vihung Garg

Hi-Tech Institute of Engineering College GZB.

ABSTRACT

Cryptography is the only known practical method for protecting information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. Administrative and physical security procedures often can provide adequate protection for offline data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection.

A basic task in **cryptography** is to enable users to communicate securely over an insecure channel in a way that guarantees their transmissions' privacy and authenticity.

We live in an era of unimaginably rapidly advancing and amazing technologies that enable instantaneous flow of information - anytime, anywhere. The convergence of computers and networks has been the key force behind the development of these awe inspiring technologies. Increasing use of systems built using these information technologies (IT) is having a profound impact on our everyday lives. These technologies are becoming all pervasive and ubiquitous. An illustration of this is provided by the development of mobile communication. There is a flurry of activity in the development of novel applications that run on this infrastructure. Phones have gone from wireless to small to smart to a situation where they can be used as entertainment devices (games, radios, mp3 players, cameras and now television), for serious personal applications(for location services, messaging and authentication, banking) in addition to being used also to talk to people. The fast paced development of these applications has been enabled by the flexibility of the underlying computing platform and the communication infrastructure. The key perquisite for the continued development and successful exploitation of IT is the notion of assurance. Information Assurance involves - Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.