**Section 3-A: Digital Signature/Electronic Signature:**

Digital Signature/Electronic Signature is a technique which is highly reliable such that it should be highly difficult to forge by unauthorized person and cannot be repudiated by its creator.

The Digital Signature can be created by using a technology known as Asymmetric Crypto System which includes a Key Pair (i.e. a combination of Public Key and Private Key). The user who wants create a legal valid electronic record should have a key pair. Here Private Key is used for Digital Signature and Public key is used validation of Digital Signature.

For any legal valid electronic document two requirements are there: First, integrity of document i.e. document has not changed; second, authentication of document i.e. document is signed.

To create a legal valid electronic document involves two steps process:

1. Hash Function or known as Hashing is used for integrity of document

2. Digital Signature used for Authentication of documents.

**HASH FUNCTION:**

Hash Function is an algorithm which is executed over the message or content of agreement and it generates a big alphanumeric number known as message digest. This message digest is a unique value for one message or content. If someone will change even a character in the original message then this message will not provide the same message digest number, if hash function is executed again over this message. This change in message digest or number value will indicate that the original message has changed. But, there will always be same message digest number generated when hash function algorithm will be executed over the unchanged original message.

**Objectives of National Cyber Security Policy 2013:**

To strengthen the Regulatory framework for ensuring a Secure Cyberspace system.

To create a secure cyber ecosystem in the country and generate adequate trust & confidence in IT systems and transactions in cyberspace and enhance adoption of IT in all sectors of the economy

To comply with best global security standards and best practices. To enhance and create 24x7 ICT (Information Communication and Technology) infrastructure for response and crises management related to information security.

To enhance protection of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC)