Cybercrimes and Cyber Security

* Explain Information Technolgy Act 2000 with its features.

-> This act is deals with cybercrime and electronic commerce in india.

-> Objective :

1 Legal Recognition of Electronic Transactions:

The Act recognizes electronic transaction treating them with the same legal validity as traditional paper-based transaction.

Electronic contracts, emails and data exchanges become legally binding under the IT act.

2 Authentication through Digital Signatures:

The IT act formalizes the use of Digital signature for authenticating electronic records.

Digital Signatures under the Act ensure the identity fo the sender and the ~~id~~ integrity of the message.

3 Facilitation of E-Commerce:

The Act creates a secure environment for conducting ~~bs~~ business online promoting e-commerce.

4 Prevention of Cybercrime:

The It Act includes previsions for penalizing cybercrimes like hacking, data theft and unauthorized access.

5 Regulatory Framework for Electronic Governance:

The Act set up to regulatory for e-governane allowing goverment services to the belivered electronically.

-> Features:

1 Legality of Electronic Contracts:

The IT act declares that all Contracts made electronically through secure electronic channels are legally valid.

2 Recognition of Digital Signatures:

The IT act grants digital signatures the same legal status as handwritten signatures.

3 Police Powers for Cyber Crimes:

The act provides law enforcement with special powers to act swiftly in cybercrime-related cases.

4 Cyber Regulations Advisory Committee:

The Act mandates the creation of the cyber regulations Advisory committee to advise the central Government.

5 Cyber Appellate Tribunal:

The act provides for the establishment of a cyber Appellate tribunal to resolve disputes related to cyber crime or laws violations.

* Digital Signature:

-> Digital Signature is used to Authenticate the identity of the person to prove the integrity of the information.

Digital Signature includes Owner's public key, name, issued date and serial number of Digital Signature.

-> Digital Signature Algorithm:

1 Key Genaration:

This process generates two keys - a public key and private key using the kryptographic algorithm.

The private key is kept secret by the signer, while the public key can be shared with anyone.

The private key must be stored securely to prevent unauthorized access.

2 Signing:

The signing process is where the actual digital signature is created using the signer's private key.

Before signing, the document or message, a cryptographic hash function converts the original message into a fixed-length hash value.

The signer uses their private key to encrypt the hash value and this process create digital signature.

3 Signature Verification:

Signature Verification ensures that the digital signature is valid.

To verify the signature, signer's public key is necessory to decrypt the digital signature.

The recipient applied the same hash function using the public key and get new hash value.

The two hash value are compared. IF they matches, it confirms that the message does not altered.

-> Use of Digital Signature:

1 Secure Online Transactions

2 Email Authentication

3 Electronic Contracts and Documents

4 Government E-service

5 Software Distribution.