Lecture 25 (Public Key)

1 Digital Signatures

1. Sender digitally signs document
2. The message is verifiable and nonforgeable
3. The signing is done using the private key
4. The digitally signed message is also non-repudiate-able

2 Message Digests

1. Digital fingerprint is created by creating a fixed length hash of the message
2. This hash is then digitally signed instead of signing the entire message which might be long and hence slow

2.1 Hash Functions in Use

1. MD5 hash function - 128-bit hash
2. SHA-1

3 Preventing Man in the Middle Attacks

1. We need a centralised system to store public keys so that man in the middle attacks are not possible
2. Certification Authorities (CA) bind public key to particular entity
3. Bob's public key and identifying info are encrypted using CA's private key and stored as the digital signature