DIGITAL SIGNATURES

URK17CS054
Noel Reeves E

PROPERTIES:

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible.

- * It must verify the author and the date and time of the signature.
- * It must authenticate the contents at the time of the signature.
- * It must be verifiable by third parties, to resolve disputes.

ATTACKS AND FORGERIES:

The term forgery usually describes a message related attack against a cryptographic digital signature scheme. That is an attack trying to fabricate a digital signature for a message without having access to the respective signer's private signing key.

Key-only attack | Known message attack | Generic chosen message attack

types : Directed chosen message attack | Adaptive chosen message attack | Total break
Universal forgery | Selective forgery | Existential forgery