Applied Cryptography & Network Security

Digital Signatures

Dr. Anuj Kr. Singh
Associate Professor
AMITY UNIVERSITY MADHYA PRADESH

1

Digital Signatures

- 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.

- Forgery
- Denial
- Both scenarios are of legitimate concern.

In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature.

2

Properties of Digital Signatures

- 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.

3

Requirements of Digital Signatures

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

4

Digital Signature (Generic Model)