Information security

Lecture-10

Eng. Taghreed Harfoush

Digital Signature

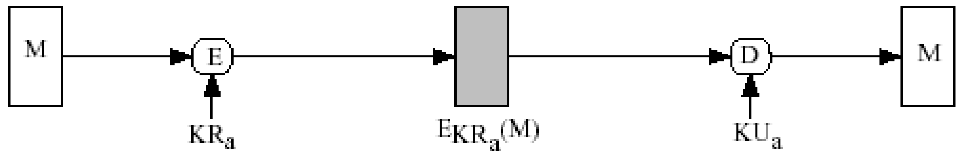
- Digital signatures must have the following properties
  - **Must be able to verify the author and the date/time of the signature**
  - **Must be able to authenticate the contents at the time of the signature**
  - **The signature must be verifiable by third parties, to resolve disputes**

Digital Signatures Requirements

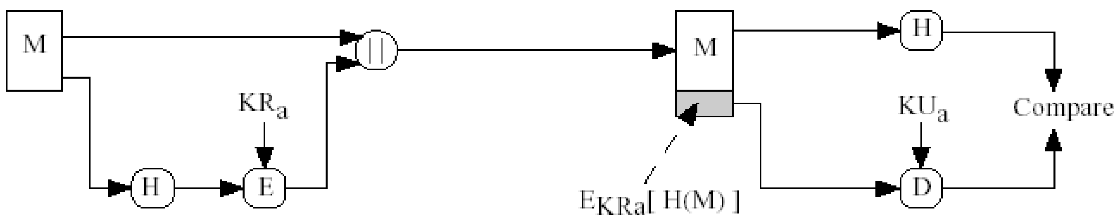
- Must be a bit pattern that depends on the message being signed
- Must use some information unique to the sender, to prevent both forgery and denial
- Must be relatively easy to produce
- Must be relatively easy to recognize and verify
- Must be computationally infeasible to forge
- Must be practical to retain a copy of the digital signature in storage

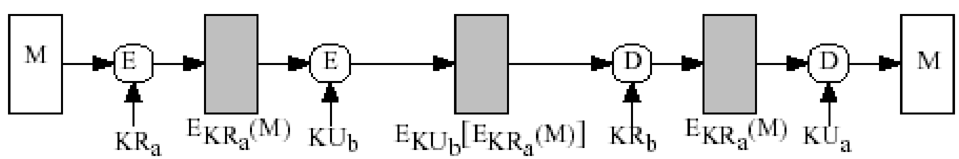
Direct Digital Signatures

- Involves only the communicating parties (no arbiter)

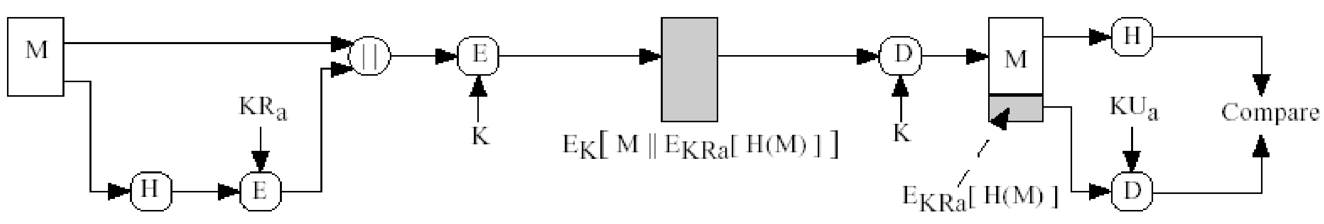


Public-key encryption: authentication and signature





Public-key encryption: confidentiality, authentication, and signature



Direct Digital Signatures

- Direct schemes have some problems
  - Validity of the schemes depends on the security of the sender’s private key
  - Sender may deny sending a particular message by claiming that the private key was lost or stolen and that someone else forged the signature
  - Some private key might be actually stolen, and the opponent may send a message signed with the stolen key

Arbitrated Digital Signatures

- There is an arbiter between the communicating parties
  - Every signed message from sender X to receiver Y goes to first arbiter A
  - A verifies the message and signature performing a number of tests
  - The message is then dated and sent to Y with an indication that it has been verified to the satisfaction of the arbiter
  - The presence of A solves the problem faced by direct signature schemes

Arbitrated Digital Signatures

- Examples of arbitrated digital signatures…

(a) Conventional Encryption, Arbiter Sees Message

(1) $X \rightarrow A: M \Vert E_{K_{xa}}[ID_X \Vert H(M)]$

(2) $A \rightarrow Y: E_{K_{ay}}[ID_X \Vert M \Vert E_{K_{xa}}[ID_X \Vert H(M)] \Vert T]$

(b) Conventional Encryption, Arbiter Does Not See Message

(1) $X \rightarrow A: ID_X \Vert E_{K_{xy}}[M] \Vert E_{K_{xa}}[ID_X \Vert H(E_{K_{xy}}[M])]$

(2) $A \rightarrow Y: E_{K_{ay}}[ID_X \Vert E_{K_{xy}}[M] \Vert E_{K_{xa}}[ID_X \Vert H(E_{K_{xy}}[M])] \Vert T]$

(c) Public-Key Encryption, Arbiter Does Not See Message

(1) $X \rightarrow A: ID_X \Vert E_{KR_x}[ID_X \Vert E_{KU_y}(E_{KR_x}[M])]$

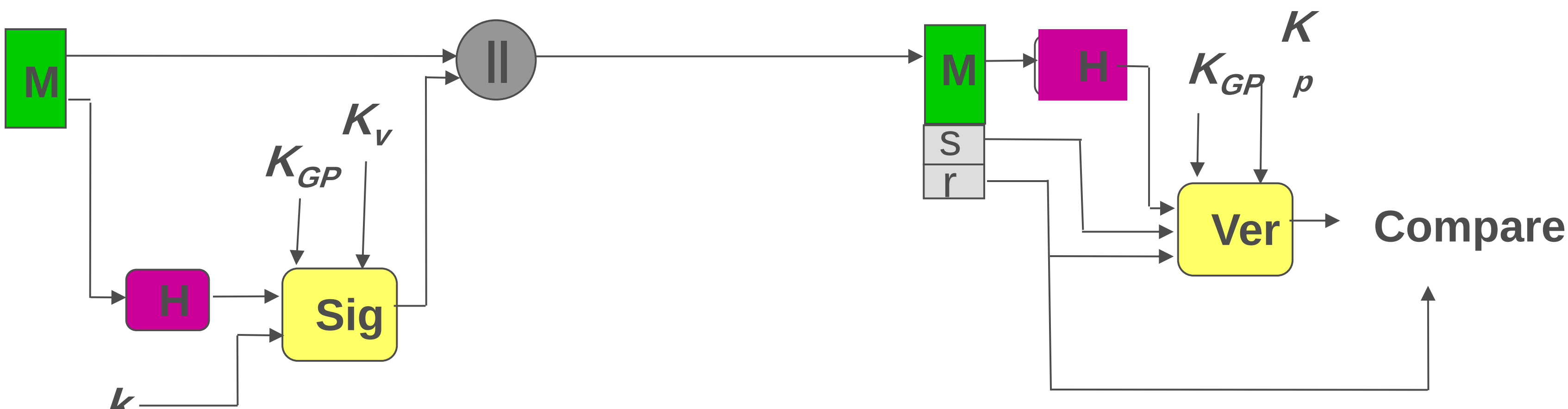
(2) $A \rightarrow Y: E_{KR_a}[ID_X \Vert E_{KU_y}[E_{KR_x}[M]] \Vert T]$

Digital Signature Standard (DSS)

- New Digital signature technique
- NIST FIPS 186 Digital Signature Standard (DSS)
- DSS is a variant of ElGamal signature scheme
- DSS makes use of SHA-1

DSS Approach

- DSS depends on:
  - A hash function H
  - A random number k, (used once).
  - The sender’s key pair (K_v: private, K_p: public)
  - Global public parameters, K_{GP}



Signature generation

Signature verification

DSS Signature Generation

- Signing: if an entity A wants to send a signed message m to another entity B.
  - Assume that (p,q,g): the global public parameters, x: A's private key, and y: A's public key.
  - 1st A randomly picks an integer k: $1 < k < q$
  - 2nd A computes r and s
    - $r = (g^k \bmod p) \bmod q$
    - $s = k\text{-}1\ (H(m) + x^r) \bmod q$
  - The signature is (r,s)
  - A sends to B [m || (r,s)]

DSS Signature Verification

- Verification: assume that B receives [m'+(r',s')], i.e., m', r' ,s' are the received versions of m, r, s.
  - Assume that B has an authentic copy of A's public key, y, and GP parameters (p, q, g).
  - 1st, B computes w, u1 , u2 such that :
    - $w = (s')^{-1} \bmod q$,
    - $u1 = w.H(m') \bmod q$,
    - $u2 = (r')w \bmod q$
  - 2nd B computes $v = [(g^{u1}y^{u2}) \bmod p] \bmod q$
  - 3rd B checks if $v = r'$ then signature is authentic


Questions