1.6 DIGITAL SIGNATURE AND AUTHENTICATION PROTOCOLS

The most important development from the work on public-key cryptography is the digital signature. Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. A digital signature is analogous to the handwritten signature. It must have the following properties:

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

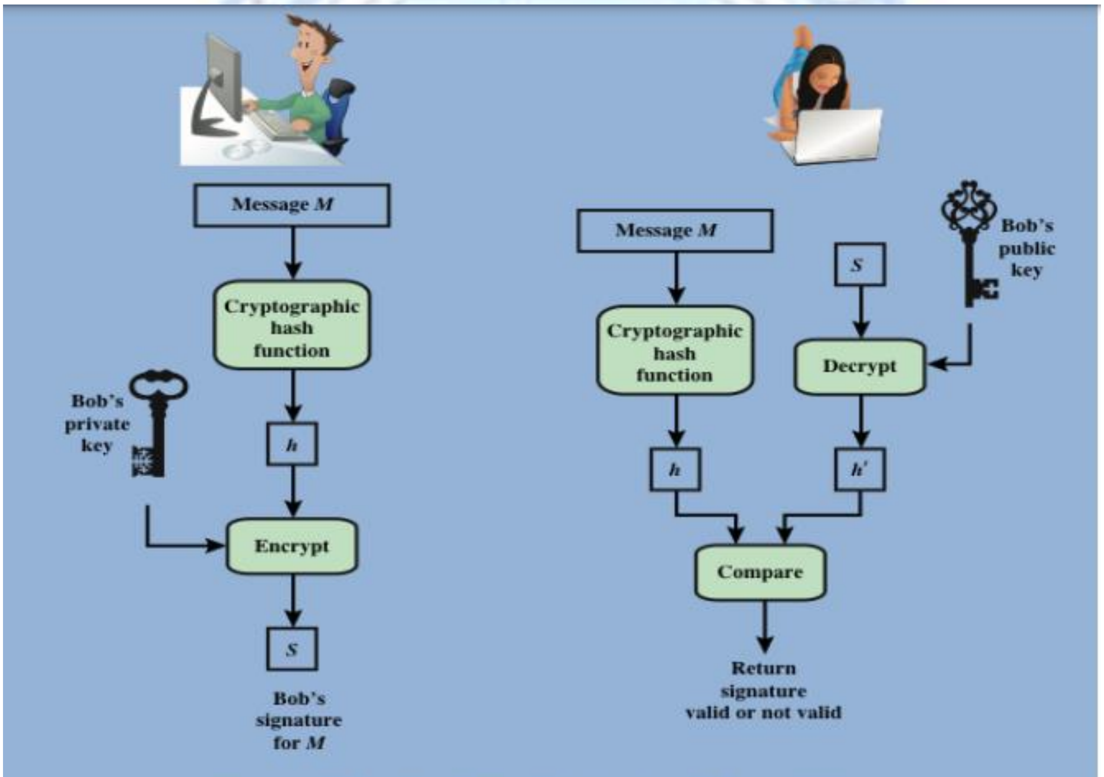


Figure 13.2 Simplified Depiction of Essential Elements of Digital Signature Process

Requirements for a digital signature:

- 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.
- It must be practical to retain a copy of the digital signature in storage.

Types: Direct and arbitrated

Direct Digital Signatures

- involve only sender & receiver
- assumed receiver has sender's public-key
- digital signature made by sender signing entire message or hash with private-key
- security depends on sender's private-key
- Drawback: Forgery

Arbitrated Digital Signatures

- involve use of arbiter A
    - validates any signed message
    - then dated and sent to recipient
- requires a great deal of trust in arbiter
- can be implemented with either private or public-key algorithms
- arbiter may or may not see message

Digital Signature Scheme

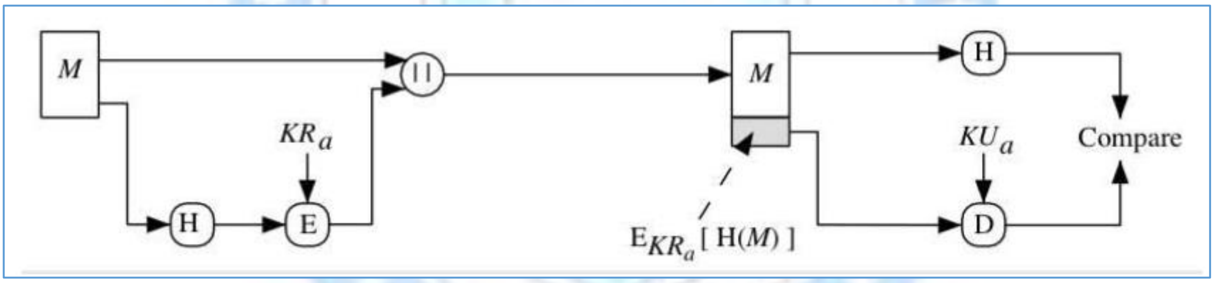
- The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the Digital Signature Standard (DSS).
- The DSS makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, the Digital Signature Algorithm (DSA).
- The DSS uses an algorithm that is designed to provide only the digital signature function and cannot be used for encryption or key exchange, unlike RSA.

Two approaches of Digital signature

- RSA approach
- DSS approach

RSA APPROACH

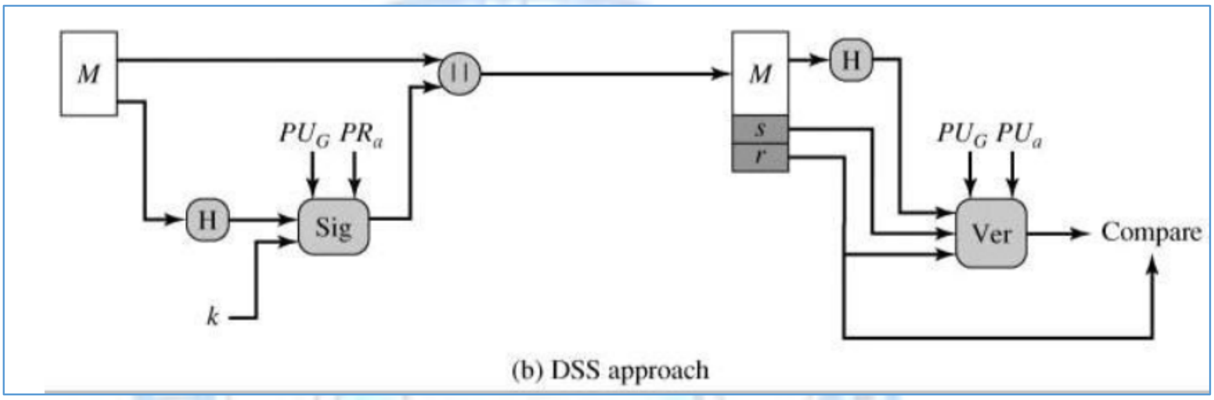
In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid. Because only the sender knows the private key, only the sender could have produced a valid signature.



DSS APPROACH

- DSS uses an algorithm that is designed to provide only digital signature function. Unlike RSA, it cannot be used for encryption or key exchange. The DSS approach makes use of a hash function.
- The hash code is provided as input to a signature function along with a random number k generated for this particular signature.
- The signature function also depends on the sender's private key (PRa) and the global public key (PUG)
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated. This plus the signature is input to a verification function.

- The verification function also depends on the global public key as well as the sender's public key (PUa), which is paired with the sender's private key.
- The output of the verification function is a value that is equal to the signature component if the signature is valid.
- The signature function is such that only the sender, with knowledge of the private key, could have produced the valid signature.



(b) DSS approach

THE DIGITAL SIGNATURE ALGORITHM

1. Global Public key Components

p- prime no. where $2^{L-1} < p < 2^{L}$ for $512 \leq L \leq 1024$

q – prime divisor of (p-1)

Choose $g = h^{(p-1)/q} \mod p$

where h is any integer with $1 < h < (p-1)$ such that $h^{(p-1)/q} \mod p > 1$

2. User's Private key

x - random or pseudo random integer with $0 < x < q$

3. User's Public key

$y = g^{x} \mod p$

4. User's Per Message Secret Number

k = random or pseudo random integer with $0 < k < q$

5. DSA Signature Creation

To sign a message M the sender: the sender generates a random signature key k, k<q

Computes signature pair:

$r = (g^{k} \bmod p) \bmod q$

$s = [k^{-1}(H(M) + xr)] \bmod q$

Signature = (r,s)

6. DSA Signature Verification

After received M & signature (r,s)

Verify a signature, recipient computes:

$w = (s')^{-1} \bmod q$

$u1 = [H(M')w] \bmod q$

$u2 = (r'w) \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

If v=r then signature is verified.