Information Security
CS3002

Lecture 10
26th September 2023

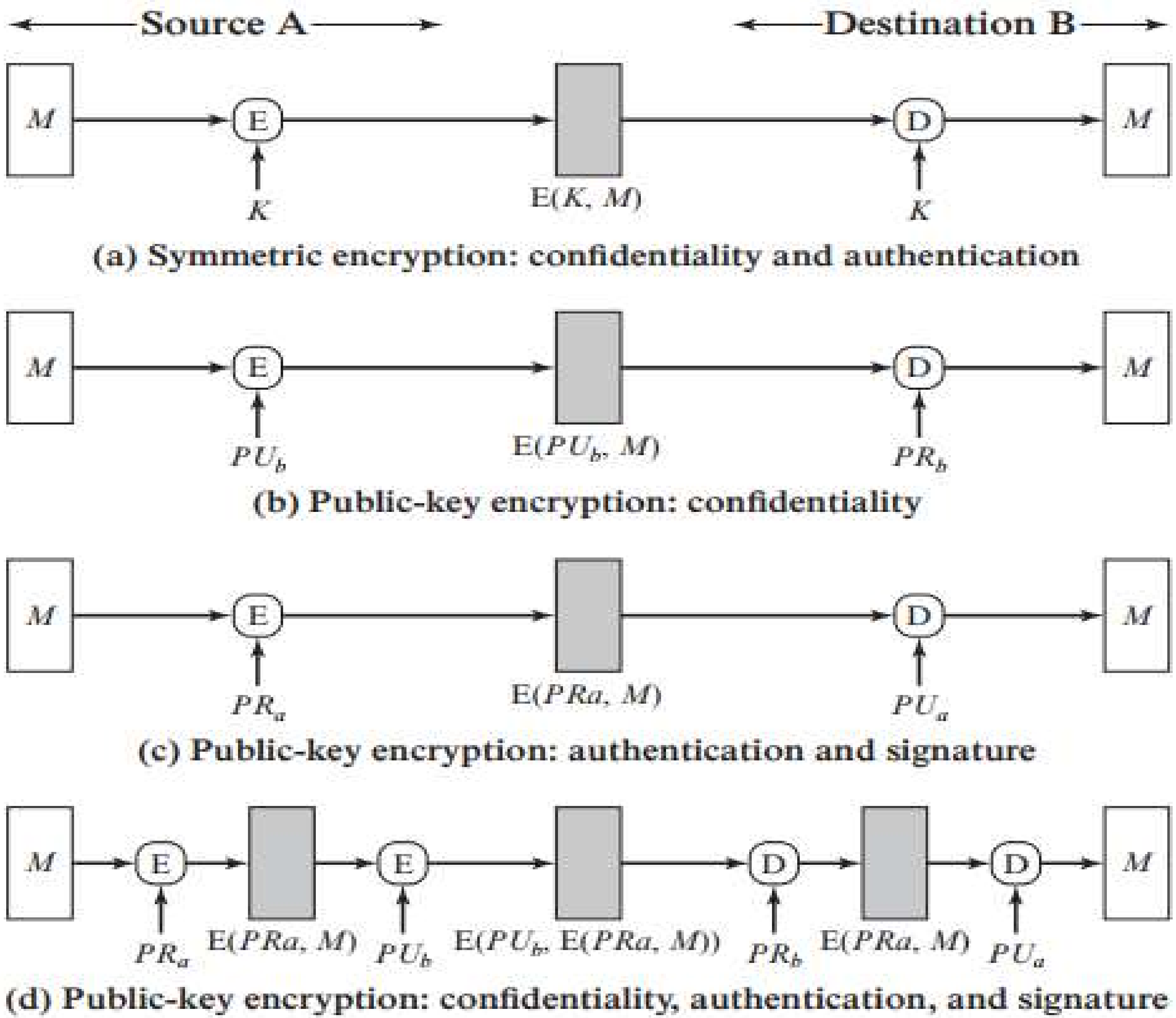
Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk

DIGITAL SIGNATURE

Some Clarification

- Electronic Signatures vs. Digital Signatures:
  - An electronic signature is simply an image of your signature added to a document.
  - A digital signature is encrypted data that proves the document came from you.
    - For some purposes, a simple electronic signature will be fine, but for more important documents, a secure digital signature is highly recommended.

Digital Signature by Using of Encryption



Digital Signature

- Operation is similar to that of the MAC.
- The hash value of a message is encrypted with a user's private key.
- Anyone who knows the user's public key can verify the integrity of the message.
- An attacker who wishes to alter the message would need to know the user's private key.
- Implications of digital signatures go beyond just message authentication.

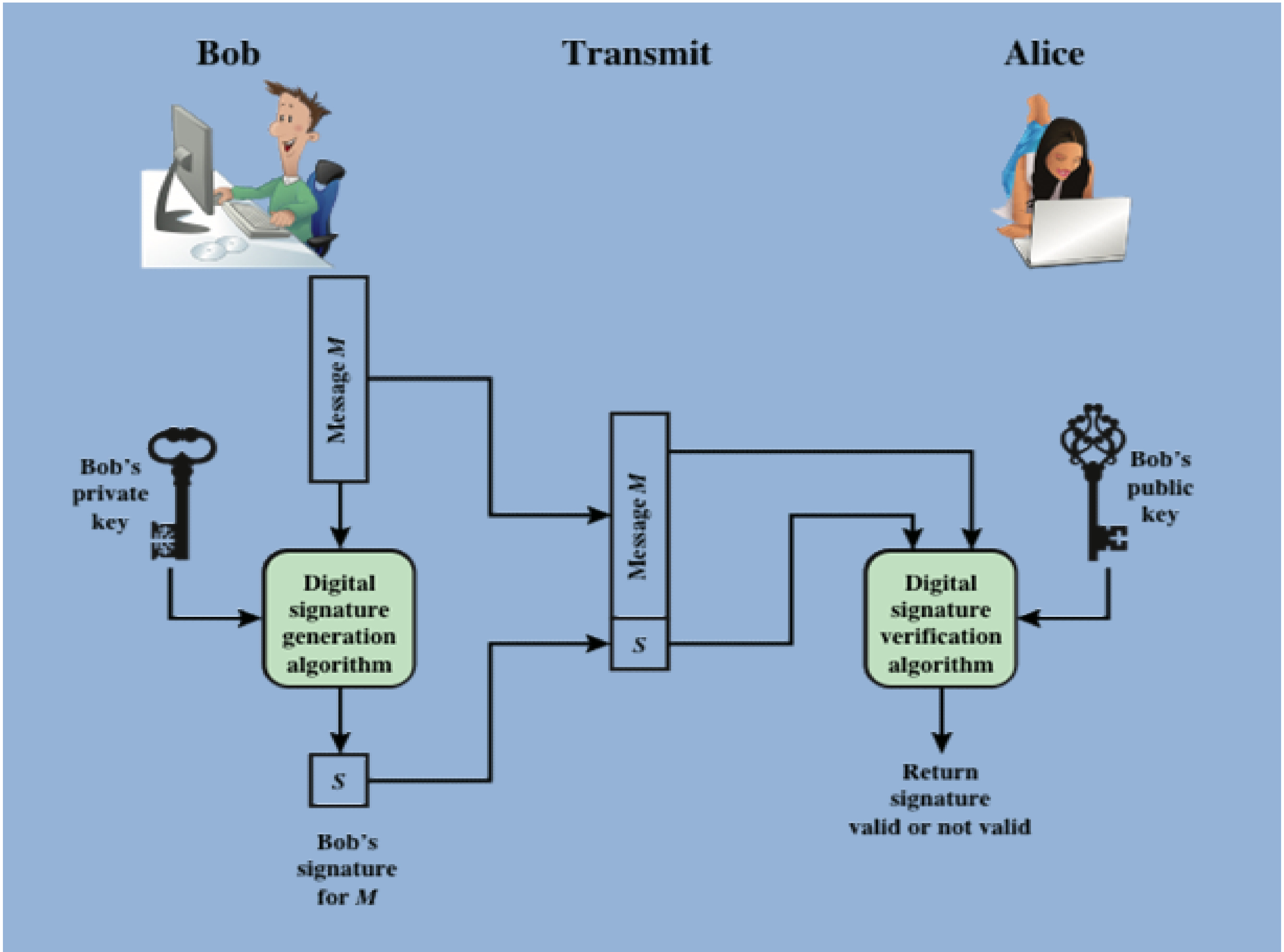


Figure 13.1 Generic Model of Digital Signature Process

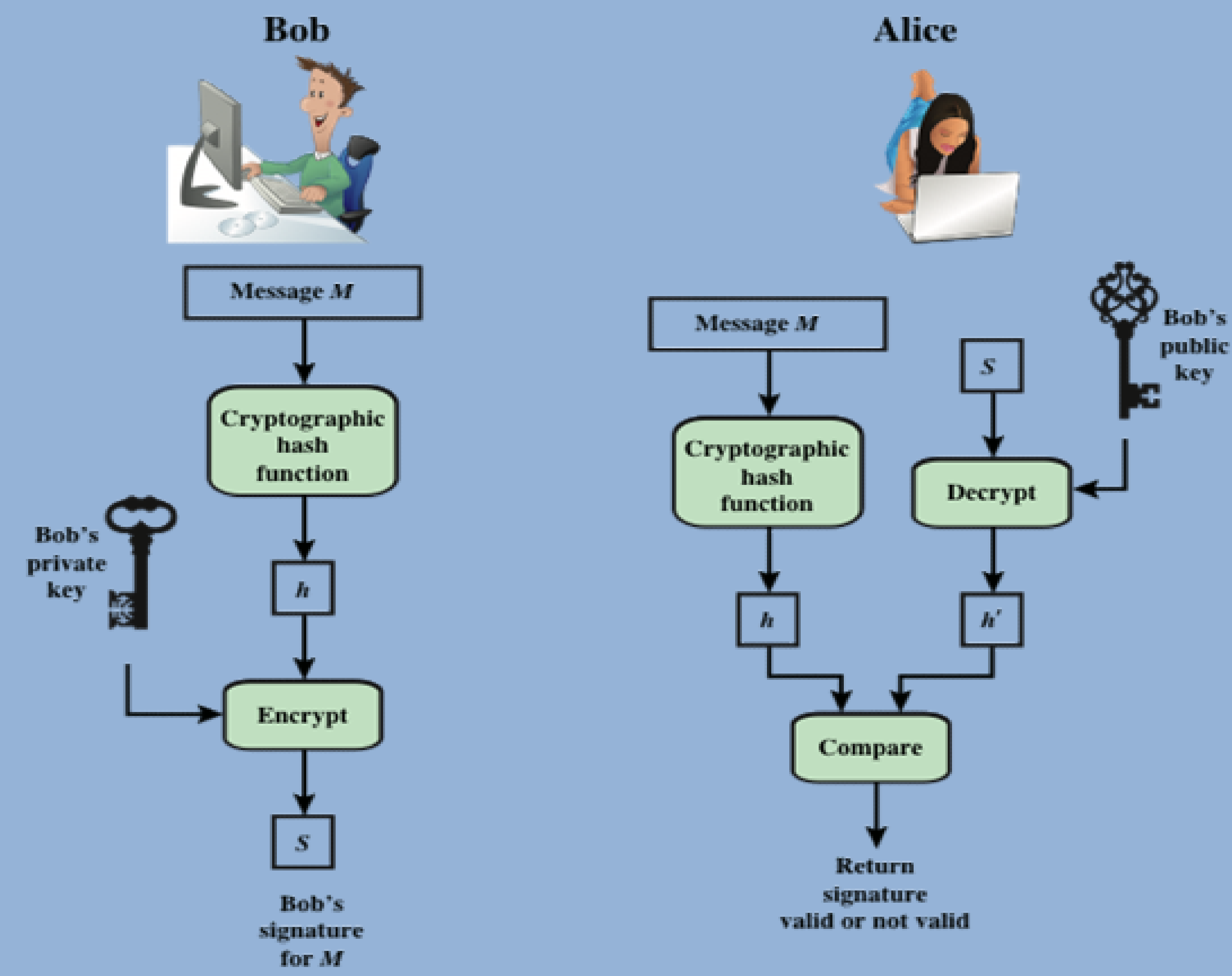


Figure 13.2 Simplified Depiction of Essential Elements of Digital Signature Process

Digital Signature Properties

- 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

Forgeries

Total break

- C determines A’s private key

Universal forgery

- C finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages

Selective forgery

- C forges a signature for a particular message chosen by C

Existential forgery

- C forges a signature for at least one message; C has no control over the message

Digital Signature Requirements

- 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.

Direct Digital Signature Conflicts

- Refers to a digital signature scheme that involves only the communicating parties.
  - It is assumed that the destination knows the public key of the source.

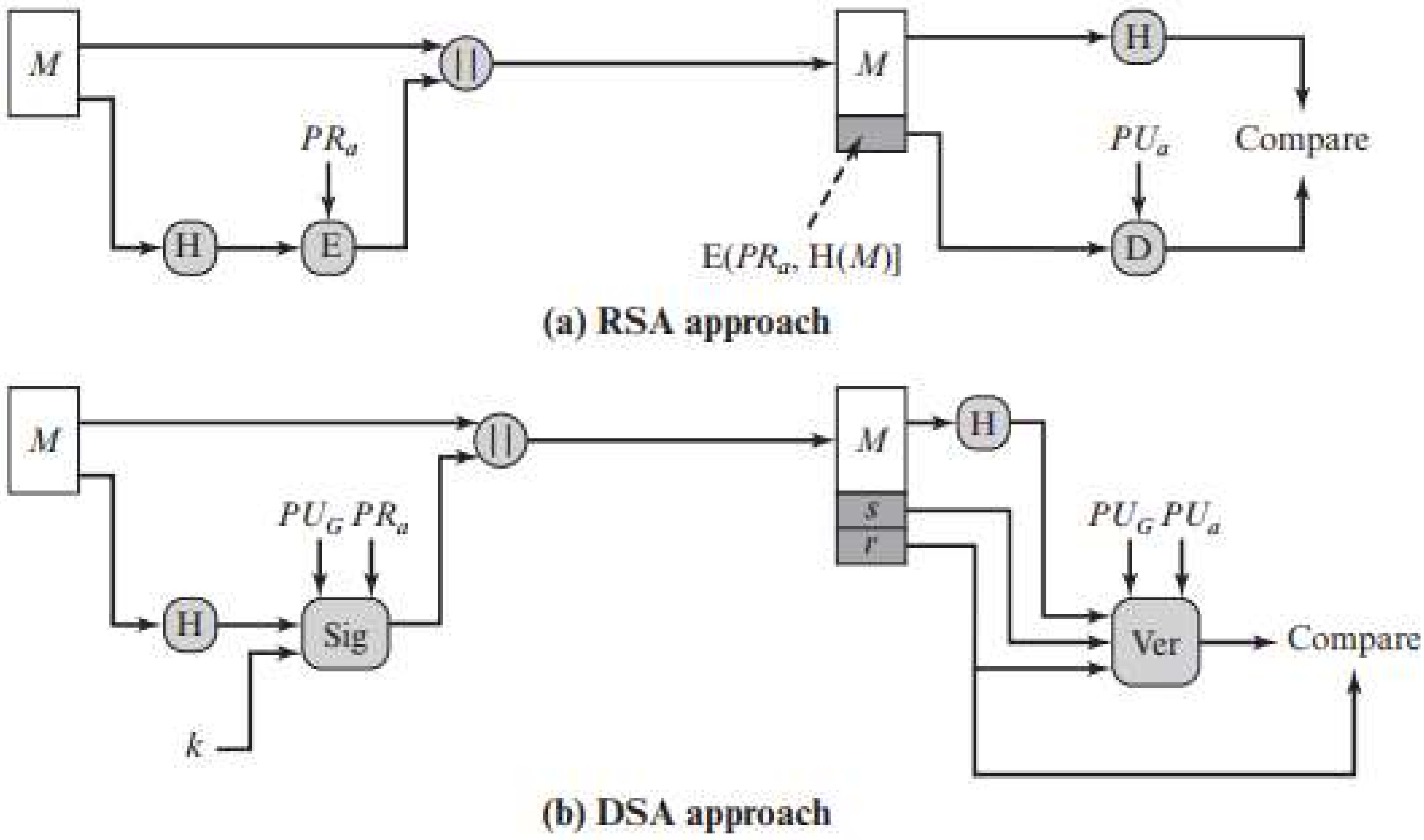
- Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key.
  - It is important to perform the signature function first and then an outer confidentiality function.
  - In case of dispute some third party must view the message and its signature.

- The validity of the scheme depends on the security of the sender's private key
  - If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.
  - One way to thwart or at least weaken this ploy is to require every signed message to include a timestamp and to require prompt reporting of compromised keys to a central authority.

NIST Digital Signature Algorithm

- Published by NIST as Federal Information Processing Standard FIPS 186.
- Makes use of the Secure Hash Algorithm (SHA).
- The latest version, FIPS 186-3, also incorporates digital signature algorithms based on RSA and on elliptic curve cryptography.

Digital Signature Algorithm (DSA/DSS)



Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$
for $512 \leq L \leq 1024$ and L a multiple of 64;
i.e., bit length L between 512 and 1024 bits
in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{N-1} < q < 2^N$
i.e., bit length of N bits

g $= h$(p − 1)/q is an exponent mod p,
where h is any integer with $1 < h < (p - 1)$
such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k random or pseudorandom integer with $0 < k < q$

Signing

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

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

Signature $= (r, s)$

Verifying

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

$u_1 = [H(M')w] \bmod q$

$u_2 = (r')w \bmod q$

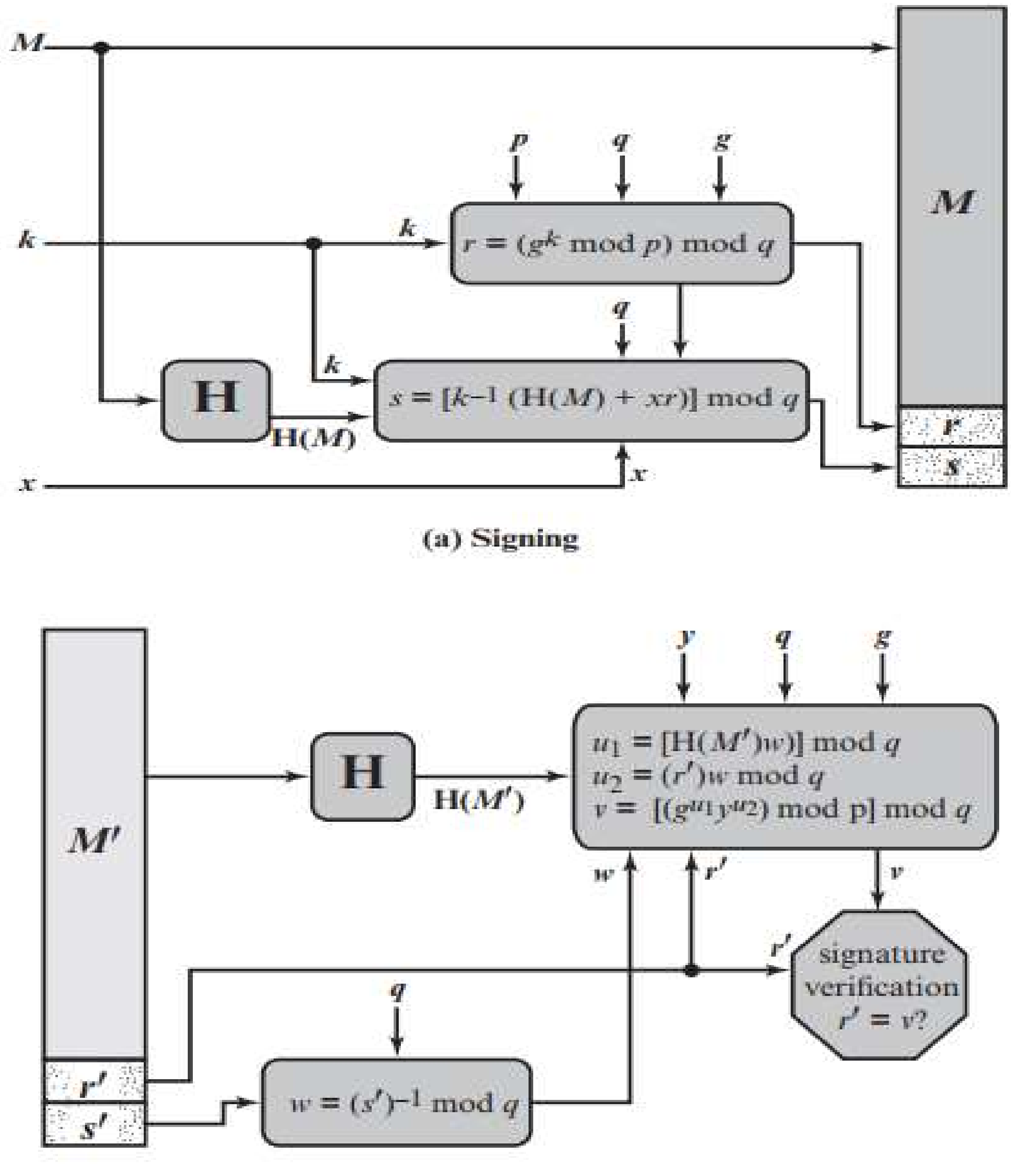
$v = [(g^{u1}y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

M = message to be signed
H(M) = hash of M using SHA-1
M', r', s' = received versions of M, r, s

Figure 13.3 The Digital Signature Algorithm (DSA)

DSA Signing and Verifying



(a) Signing

(b) Verifying