SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-3 HASH FUNCTION AND DIGITAL SIGNATURE

Digital Signature

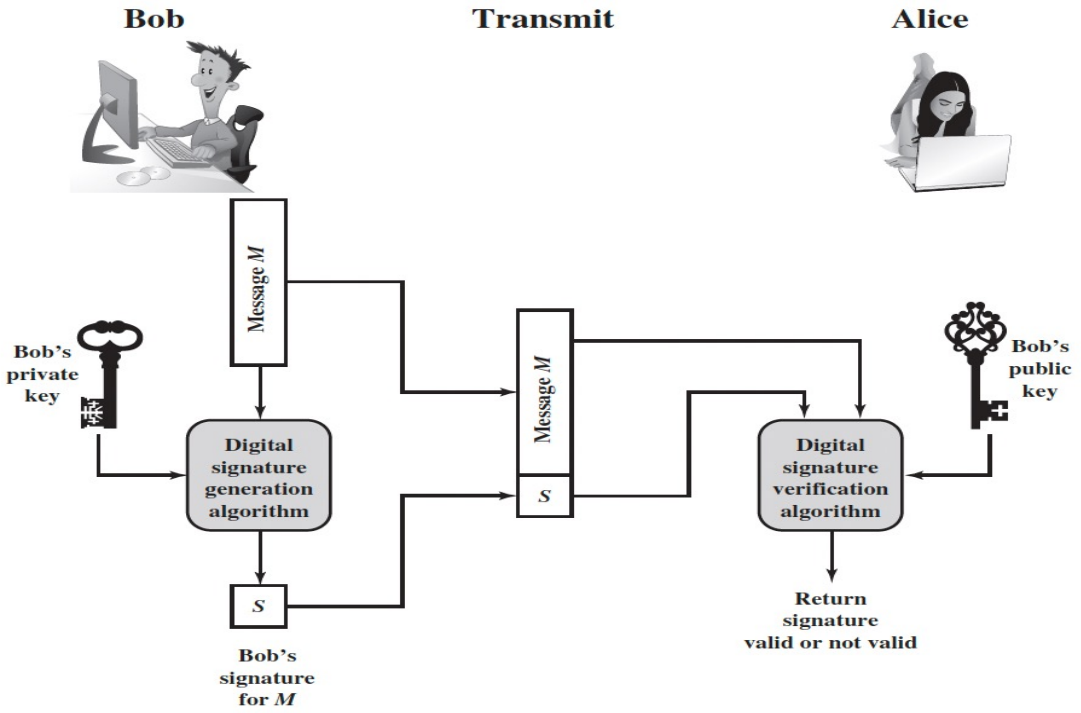


Figure 13.1 Generic Model of Digital Signature Process

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

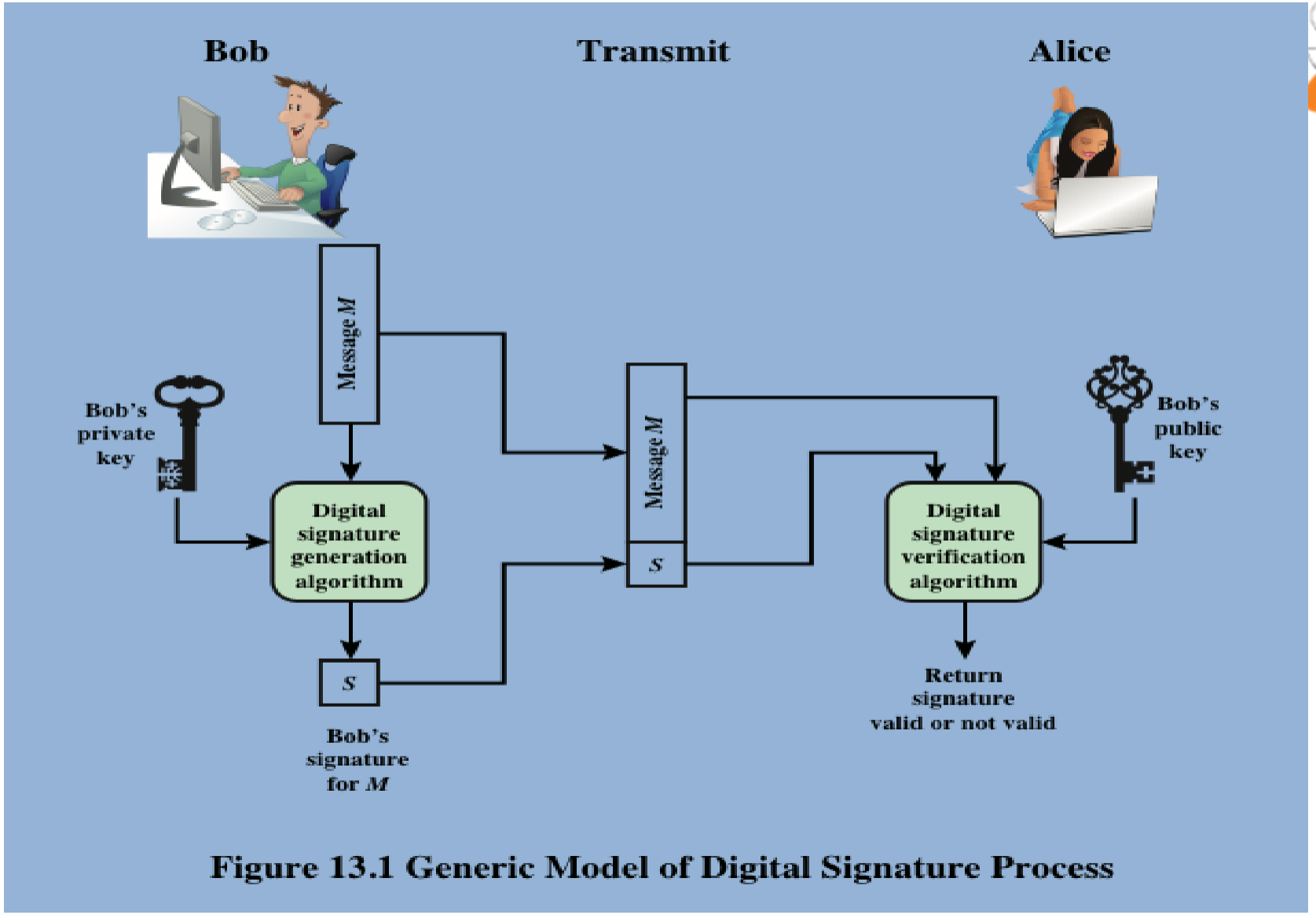


Figure 13.1 Generic Model of Digital Signature Process

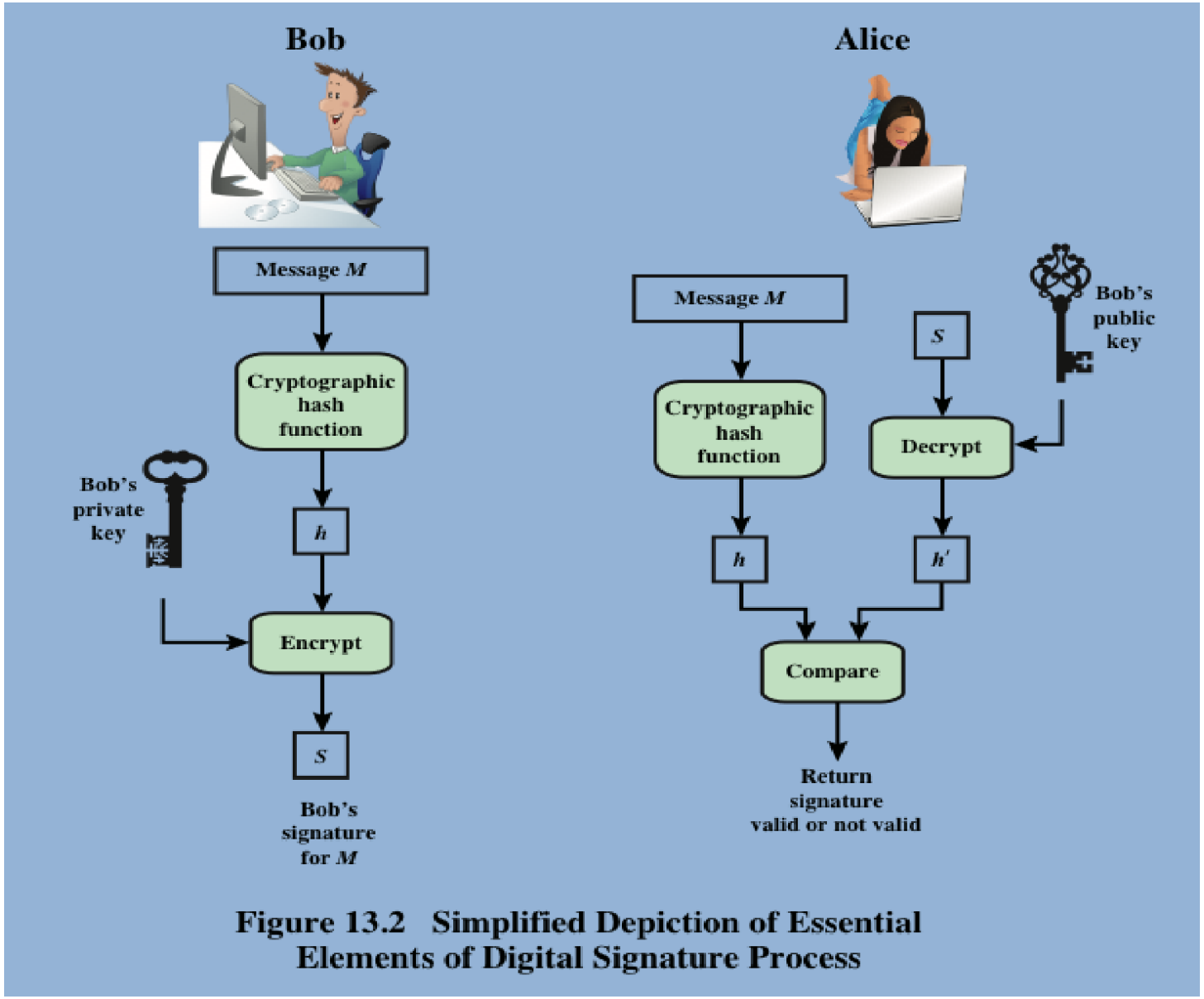
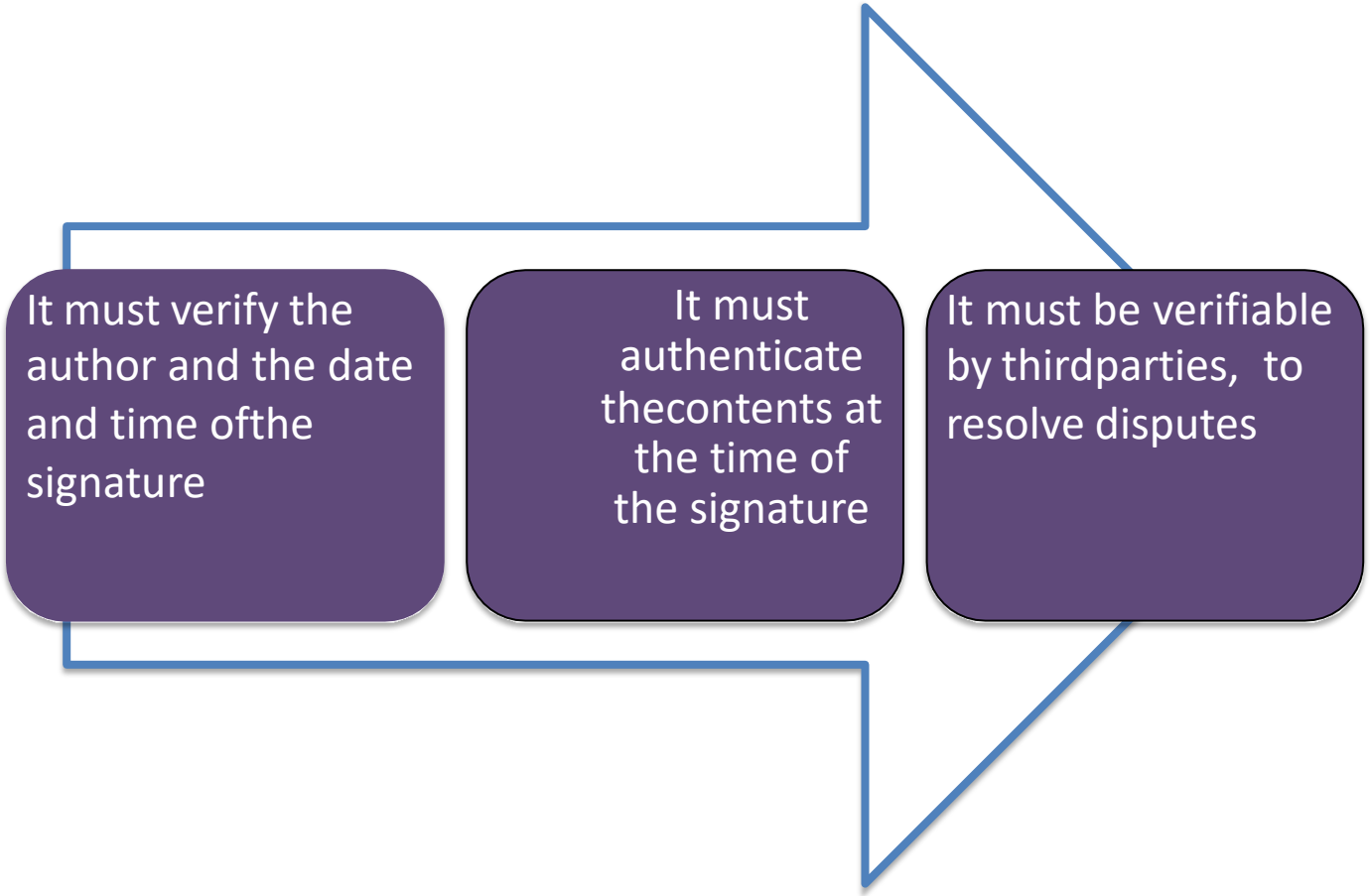
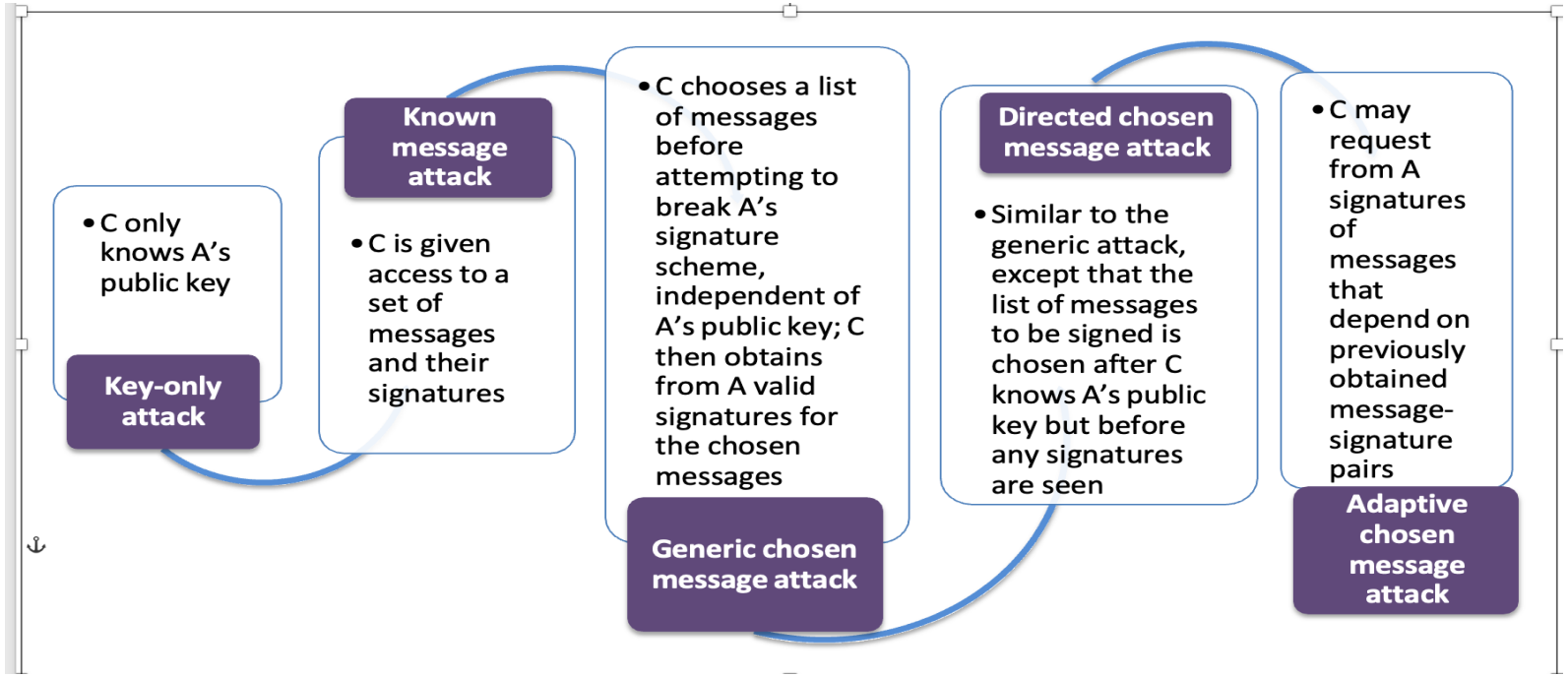


Figure 13.2 Simplified Depiction of Essential Elements of Digital Signature Process

Digital Signature properties



Attacks


• C only knows A's public key
Key-only attack
Known message attack
• C is given access to a set of messages and their signatures
• C chooses a list of messages before attempting to break A's signature scheme, independent of A's public key; C then obtains from A valid signatures for the chosen messages
Generic chosen message attack
Directed chosen message attack
• Similar to the generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any signatures are seen
• C may request from A signatures of messages that depend on previously obtained message-signature pairs
Adaptive chosen message attack