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

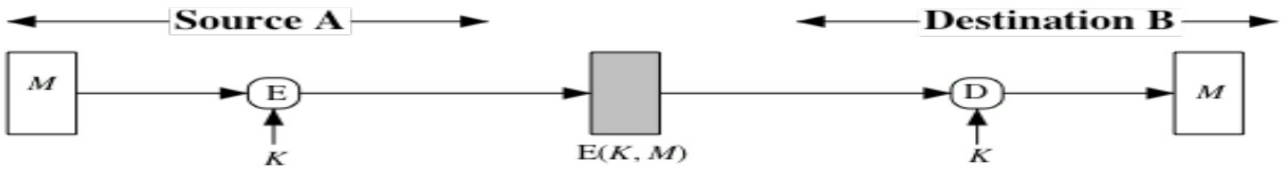
19ITB302-Cryptography and Network Security

UNIT-3 HASH FUNCTION AND DIGITAL SIGNATURE

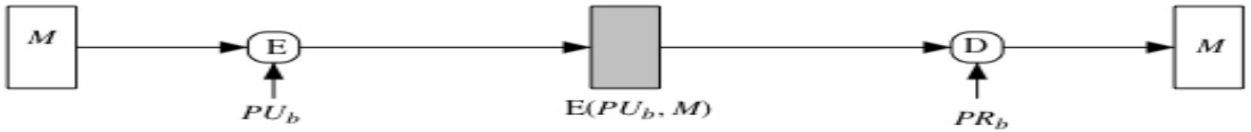
Classes of Message Authentication Function

1. **Hash function** - A function that maps a message of any length into a fixed length hash value, which serves as the authenticator
2. **Message encryption** - The ciphertext of the entire message serves as its authenticator
3. **Message Authentication Code (MAC)** - A function of the message and a secretkey that produces a fixed-length value that serves as the authenticator.

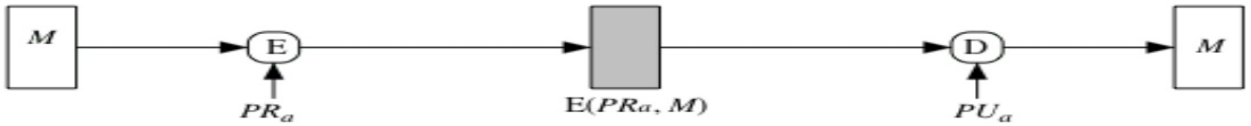
Message Encryption



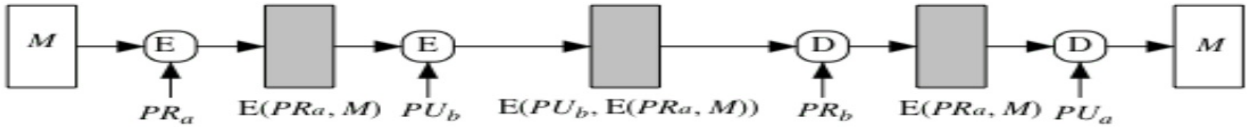
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality

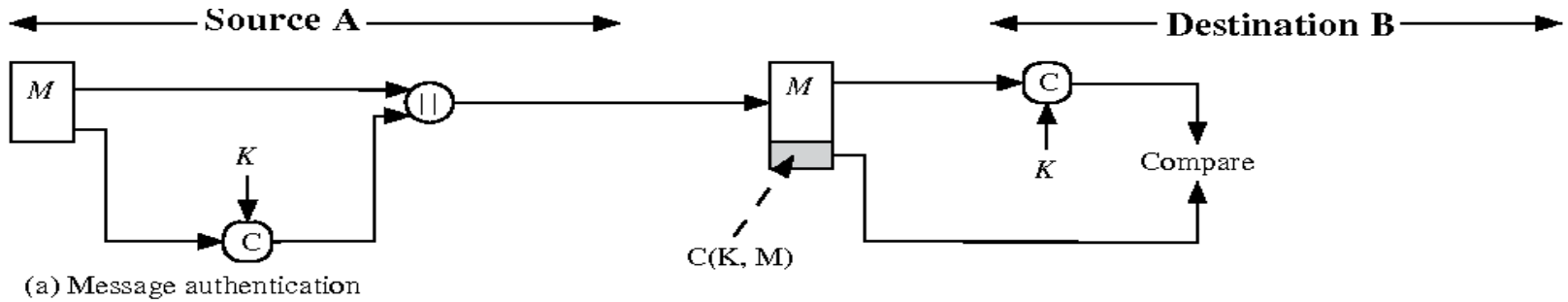


(c) Public-key encryption: authentication and signature

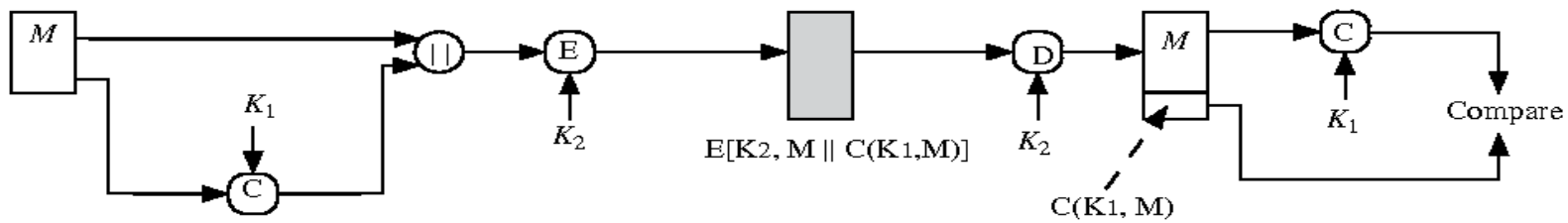


(d) Public-key encryption: confidentiality, authentication, and signature

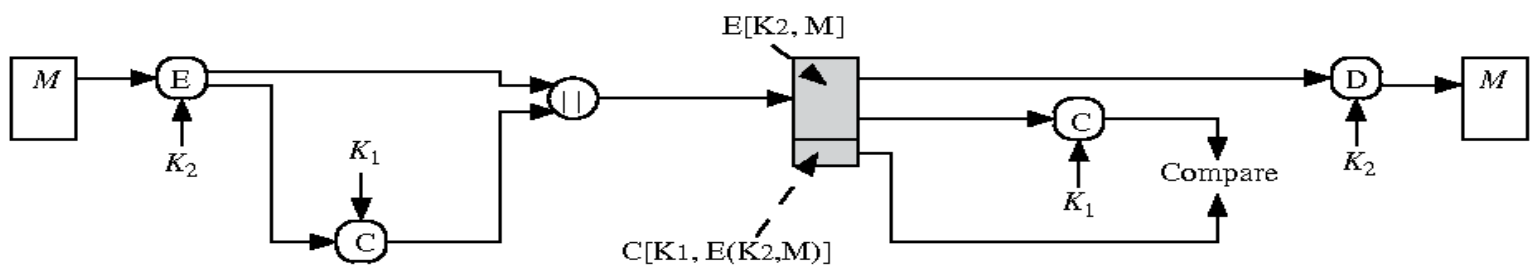
Message Authentication Code



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

REQUIREMENTS FOR MESSAGE AUTHENTICATION CODES

- The MAC is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by recomputing the MAC.
- If an opponent observes and, it should be computationally infeasible for the opponent to construct a message M' such that MAC (K, M') = MAC (K, M)
- MAC(K, M) should be uniformly distributed in the sense that for randomly chosen messages, M and M' , the probability that is MAC(K, M) = MAC(K, M') is 2^n, where n is the number of bits in the MAC