Message Authentication Codes

Outline

- Message Authentication Codes
- MAC requirements and security

Message Authentication

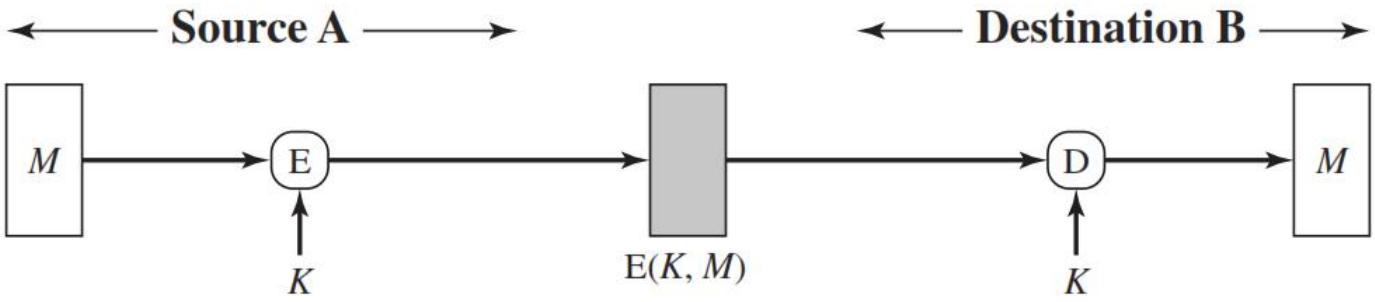
- **Message authentication** is a procedure to verify that received messages come from the genuine source and have not been altered.
- Message authentication may also verify sequencing and timeliness.
- Message authentication is a mechanism or service used to verify the **integrity of a message**.
- Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay).

Message Authentication Requirements

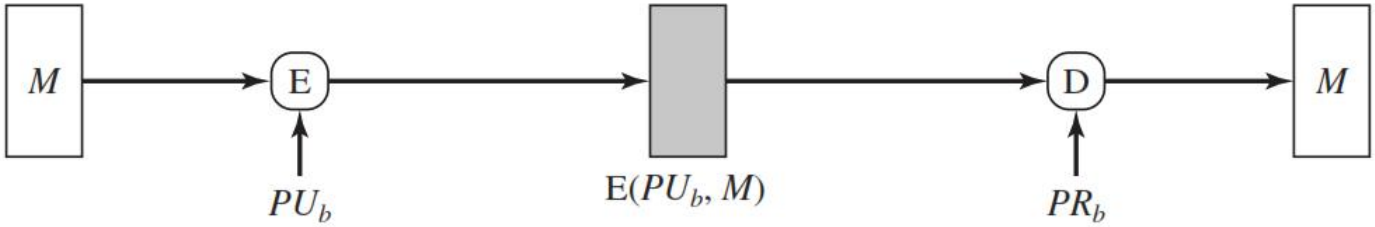
1. **Disclosure:** Disclosure of message contents
2. **Traffic analysis:** Discovery of the pattern of traffic between parties
3. **Masquerade:** Insertion of messages into the network from a fraudulent source
4. **Content modification:** Changes to the contents of a message
5. **Sequence modification:** Any modification to a sequence of messages between parties
6. **Timing modification:** Delay or replay of messages
7. **Source repudiation:** Denial of transmission of message by source
8. **Destination repudiation:** Denial of receipt of message by destination

Message Authentication Requirements

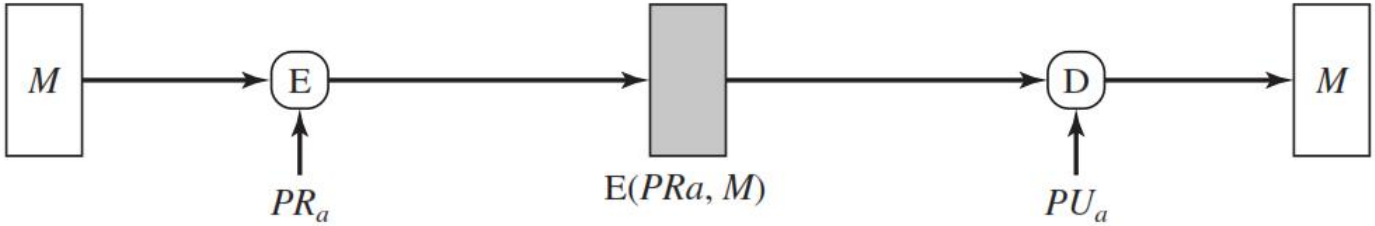
1. Disclosure
2. Traffic analysis
3. Masquerade
4. Content modification
5. Sequence modification
6. Timing modification
7. Source repudiation
8. Destination repudiation



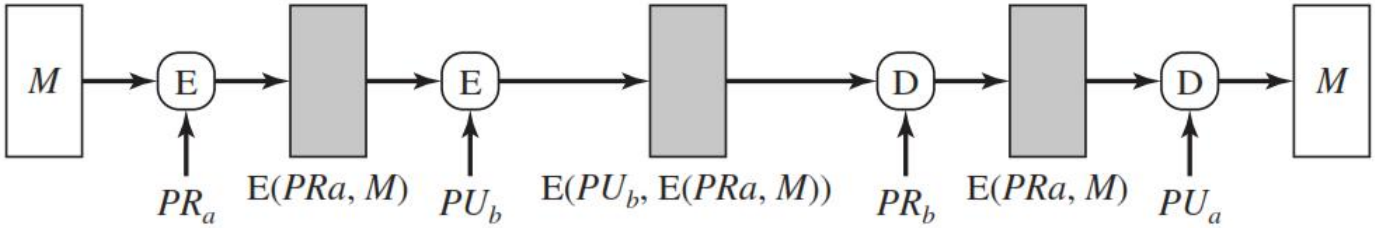
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality



(c) Public-key encryption: authentication and signature



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