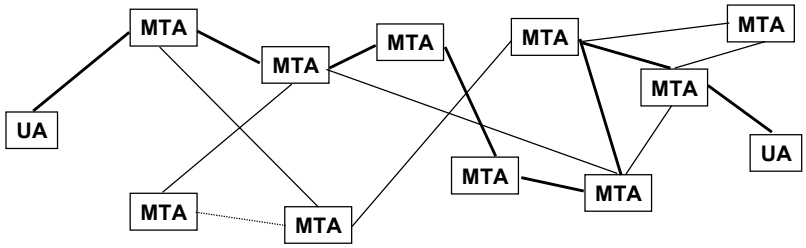
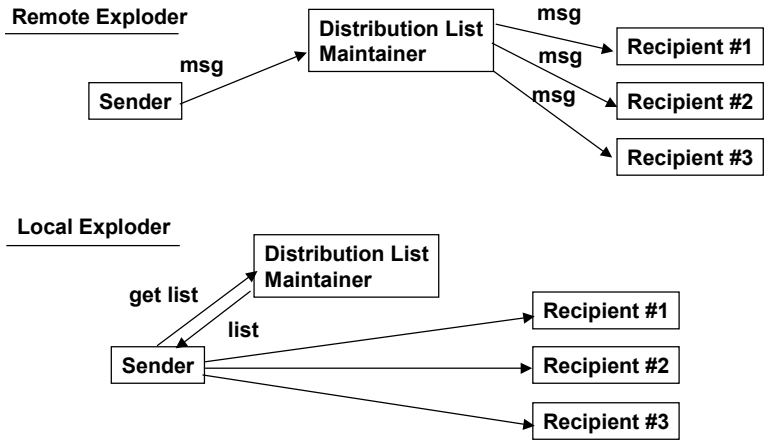
Store and Forward Processing



UA : User Agent
MTA : Message Transfer Agent

Distribution Lists



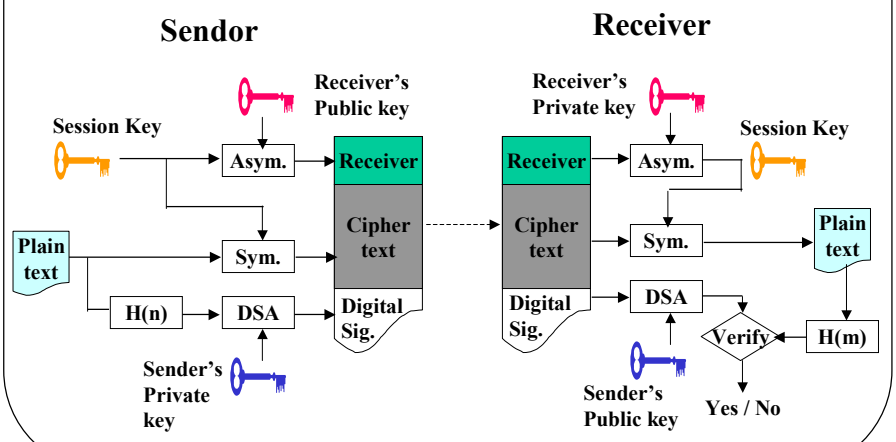
Real World

- Private e-mail to friends
- Private e-mail to business associates
- Private and authenticated e-mail to business partners
- Electronic Commerce
- etc.

Security Req't of E-mail

- Privacy
- Authentication
- Integrity
- Non-repudiation : third-party authentication
- Proof-of-submission : certified mail
- Proof-of-delivery
- Message flow confidentiality : C can't know the fact A and B communicates each other.
- Anonymity : not revealing sender's ID information
- Containment : security labeling
- Audit : logging specific day's mailing facts
- Accounting : extract statistics
- Self destruct : self destruct after receiving
- Message sequence integrity : sequential delivery of messages

Implementation Example



Non-repudiation

- (Definition in OSI)
  - security service that counters repudiation where repudiation is defined as "denial by one of the entities involved in a communication of having participated in all or part of the communication"
  - anti-repudiation is better choice
- (Definition in ABA)
  - Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission of delivery of the message and the integrity of its contents.

Non-repudiation

- Non-repudiation of Origin (NRO)
  - prevents or resolves disagreements as to whether a particular party originated a particular item.
- Non-repudiation of Receipt (NRR)
  - prevents or resolves disagreements whether a particular party received a particular data item, the time the delivery occurred.

Implementing Non-repudiation

- Direct Method
  - Secret exchange protocol
  - Oblivious Transfer protocol
  - Fairness Problem
- Indirect Method
  - TTP(Ex : Post Office)
  - DA(Delivery Agent)
- TimeStamping

How NRO happens

- A recipient claims to have received
  - a message, but the party identified as sender claims not to have sent any message.
  - a message different from that which the sender claims to have sent.
  - a particular message originated on a specific date and time, but the party identified as sender claims not to have sent that particular message at that specific time and date.

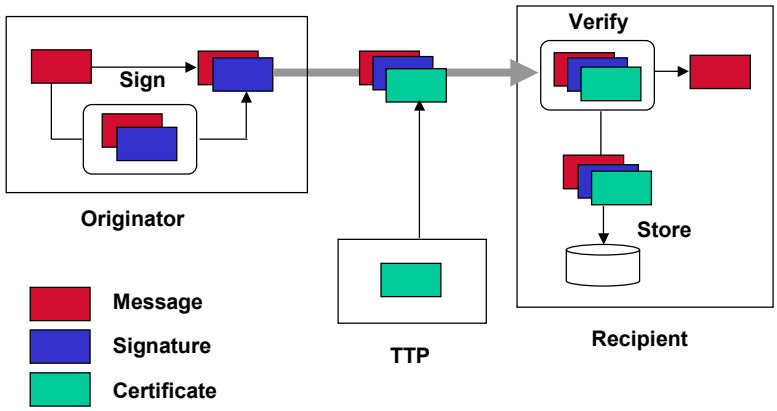
Measures against NRO

- Adequately associate, or link together, various pieces of information including at least
  - The identity of the originator and
  - The content of the message,

  optionally
  - The date and time at which origination occurred.
  - The identity of the intended recipients and
  - The identity of any TTP involved in generating evidence

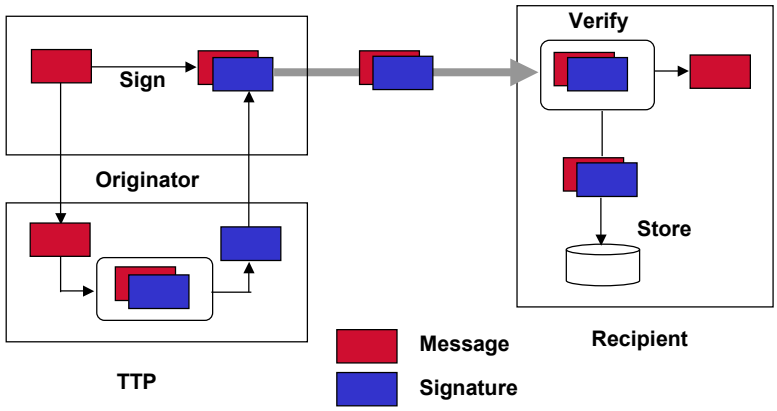
Way of NRO

(1) Originator's Digital Signature



Way of NRO(II)

(2) Digital Signature of TTP



Why NRR happens

- **A sender claims to have sent**
  - **a message, but the party identified as recipient claims not to have sent any message.**
  - **a message different from that which the recipient claims to have received.**
  - **a particular message originated on a specific date and time, but the party identified as recipient claims not to have received that particular message at a time and on a date consistent with the claimed time and date of sending.**

Measure against NRR

- **Adequately associate, or link together, various pieces of information including at least**
  - **The identity of the recipient and**
  - **The content of the message,**

  optionally
  - **The date and time at which delivery of the message occurred.**
  - **The identity of the originator and**
  - **The identity of any TTP involved in generating evidence**

Way of NRR

(1) Recipient's Signature