Secure Mail
Complexities of email

• text-based
• distribution lists
  – local vs remote explosion
• store-and-forward
Possible features. How with secret vs public keys, dist lists?

- Privacy
- authentication
- integrity
- non-repudiation
- plausible deniability
- proof of submission
- proof of delivery
Integrity/Authentication

- Public key, straightforward
- Secret key: various possibilities
  - CBC residue computed with shared key.
  - Keyed hash with per-user shared secret
  - MD encrypted with the shared secret
  - What about taking a per-message secret S, and doing any of the above using S?
Non-repudiation/Plausible Deniability

• Public keys: nonrepudiation easy, PD hard
• Secret keys: vice versa
• How to do PD with public keys?
• Secret key NR: with notary
  – Alice negotiates with notary to add “seal” to msg, $f(S_N, \text{msg, “Alice”}; S_N$ is secret local to notary
  – Bob can’t tell if seal OK, but could ask
  – Or Notary can add second seal for Bob: Note: Bob’s seal better cover Alice’s. Why?
Proof of submission/delivery

• post office signs MD of message
• proves it received it, not that it was delivered
• proof of delivery
  – signed by recipient
  – requires cooperation of recipient
  – can’t be sure. false negative, false positive, depending on order
More possible features

- message flow confidentiality
- anonymity
- containment; mark msgs, filter
- self-destruct
- message sequence integrity
- preventing post or back dating
PEM

- Could do integrity protection with DES-CBC or MD
- Could use public or secret interchange keys
- Note PEM uses an IV even though there’s a per-message secret. Any ideas as to why?
PEM, secret keys, CBC

- Encrypted: Alice to Ted using CBC:
  - \{S\}_{Alice-Ted}
  - \{CBC \text{ using } S \text{ as key} \}_{Alice-Ted}
  - \{msg\}_S

- Unencrypted: same except send msg, not \{msg\}
Alice to Bob and Ted, using CBC

- \( \{S\}_{\text{Alice-Bob}} \)
- \( \{\text{CBC using } S \text{ as key}\}_{\text{Alice-Bob}} \)
- \( \{S\}_{\text{Alice-Ted}} \)
- \( \{\text{CBC using } S \text{ as key}\}_{\text{Alice-Ted}} \)
- msg or \( \{\text{msg}\}S \)
- How can Bob forge msg from Alice to Ted?
- Can eavesdropper?
PEM with secret keys/MD

• unencrypted: Alice to Ted using MD:
  – \{1st 64 bits of MD\}_{Alice-Ted}
  – \{2nd 64 bits of MD\}_{Alice-Ted}
  – msg
• If Ted accepts CBC from Alice, what can eavesdropper forge?
• What if msg from Alice was encrypted?
PEM with public keys/CBC

• encrypted: Alice to Bob using CBC:
  – \{S\}_\text{Bob}
  – \{[\text{CBC using } S']_\text{Alice}\}_S
  – \{\text{msg}\}_S
PEM with public keys/CBC

• unencrypted: Alice to Bob using CBC:
  – $\{S\}_\text{Bob}$
  – $[\text{CBC}]_\text{Alice}$
  – msg
PEM/Public keys

- Show how Bob can forge Alice’s signature. Does it matter if the message was encrypted?
- What can an eavesdropper do if the message was unencrypted?
PEM with secret keys

- Alice to Ted using DES-CBC
  - \{S\}_\text{Alice-Ted}
  - \{CBC residue(msg using S)\}_\text{Alice-Ted}
  - msg

- Alice to Ted using MD
  - \{(1st 64 bits of MD)\}_\text{Alice-Ted}
  - \{(2nd 64 bits of MD)\}_\text{Alice-Ted}
  - msg