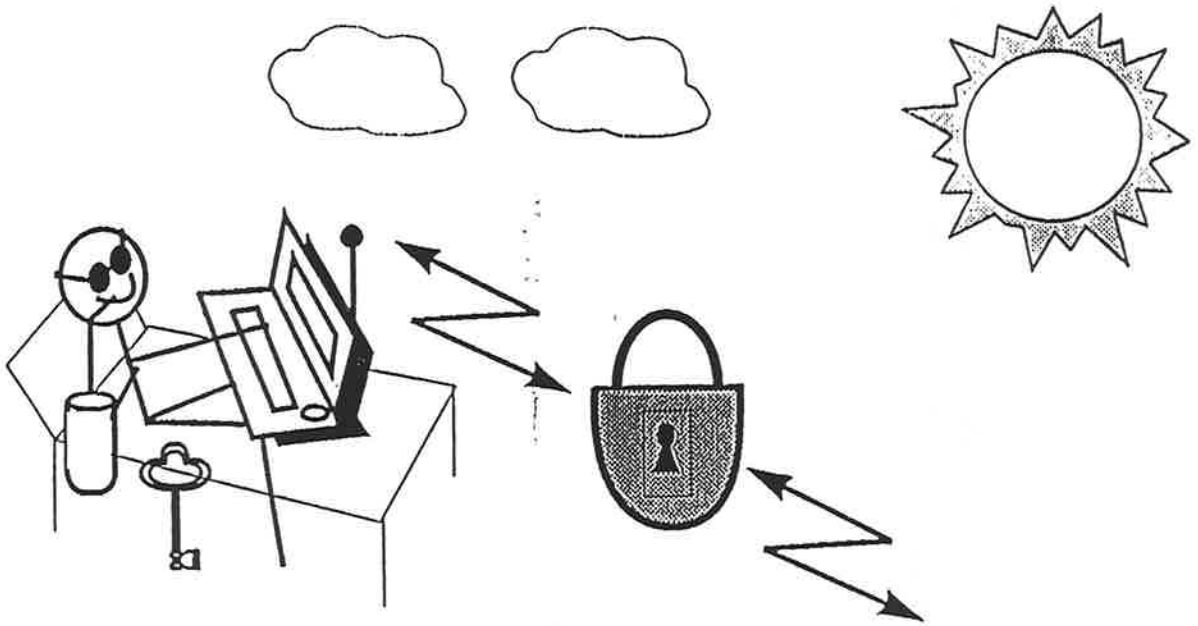
WIRELESS NETWORK SECURITY

Ashar Aziz

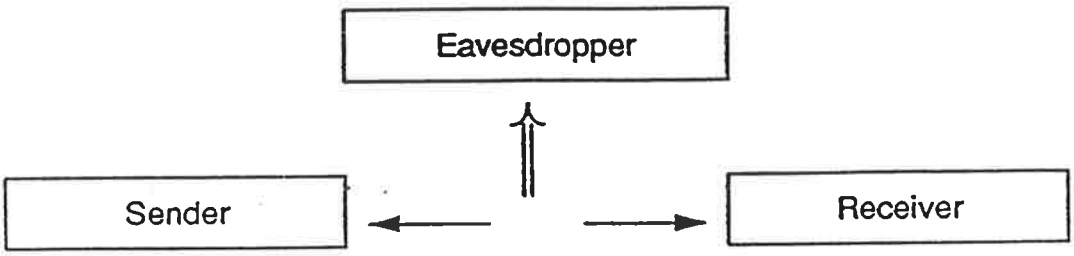
Whitfield Diffie



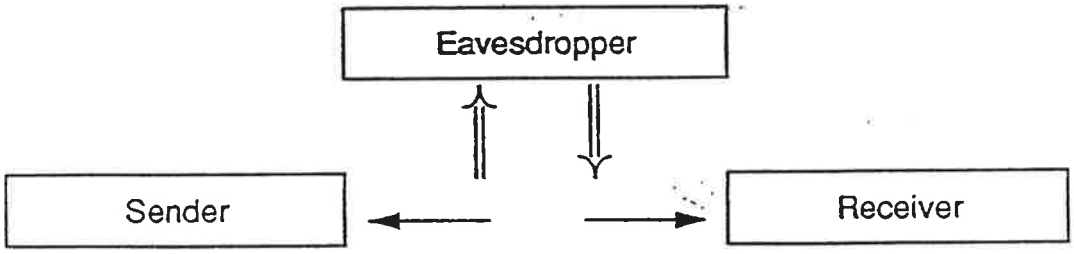
The Need For Security

- Ethernet security has largely depended upon physical security in network environments.
- This method is inapplicable to radio-based wireless networks.
- Unauthorized users can potentially listen, as well as connect into the wired network.
- In industrial parks, where competitors are close-by, one competitor's network can masquerade as the other's.
- This motivates the need for network security that is independent of physical security.

Privacy and Authentication



- **Privacy** — assurance to the sender of a message that its contents will be revealed only to the intended receiver.



- **Authentication** — assurance to the receiver that he knows the identity of the sender, and that the received message has not been modified during transmission.

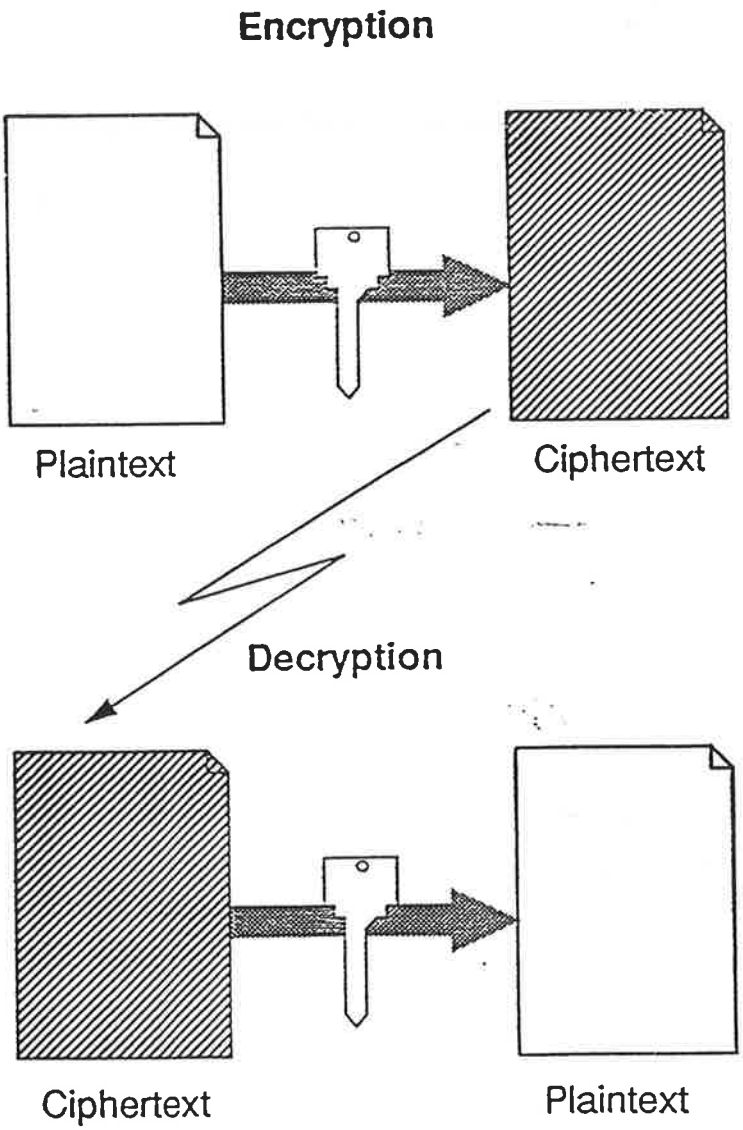
Approaches to Protection

A. 'Physical' Protection of the communication media.

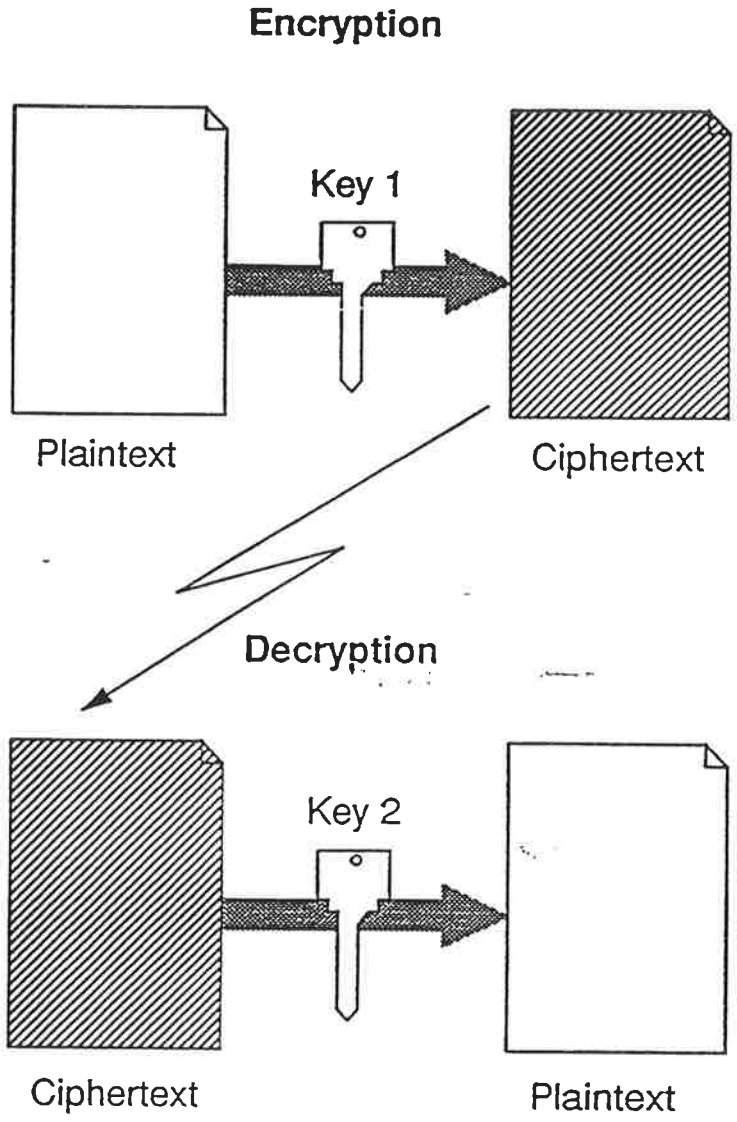
B. Cryptography

Cryptography

- Secret keys transform useful and comprehensible plaintext into scrambled and meaningless ciphertext, thus protecting the data.

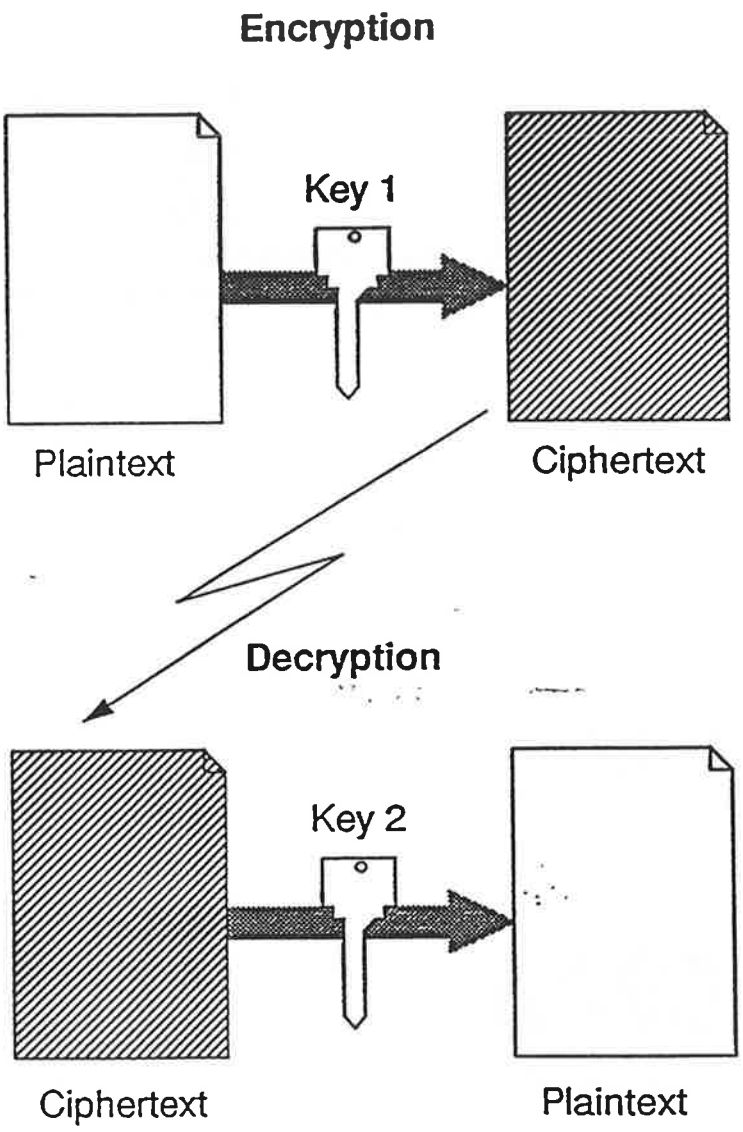


Conventional or Shared-Key Cryptography



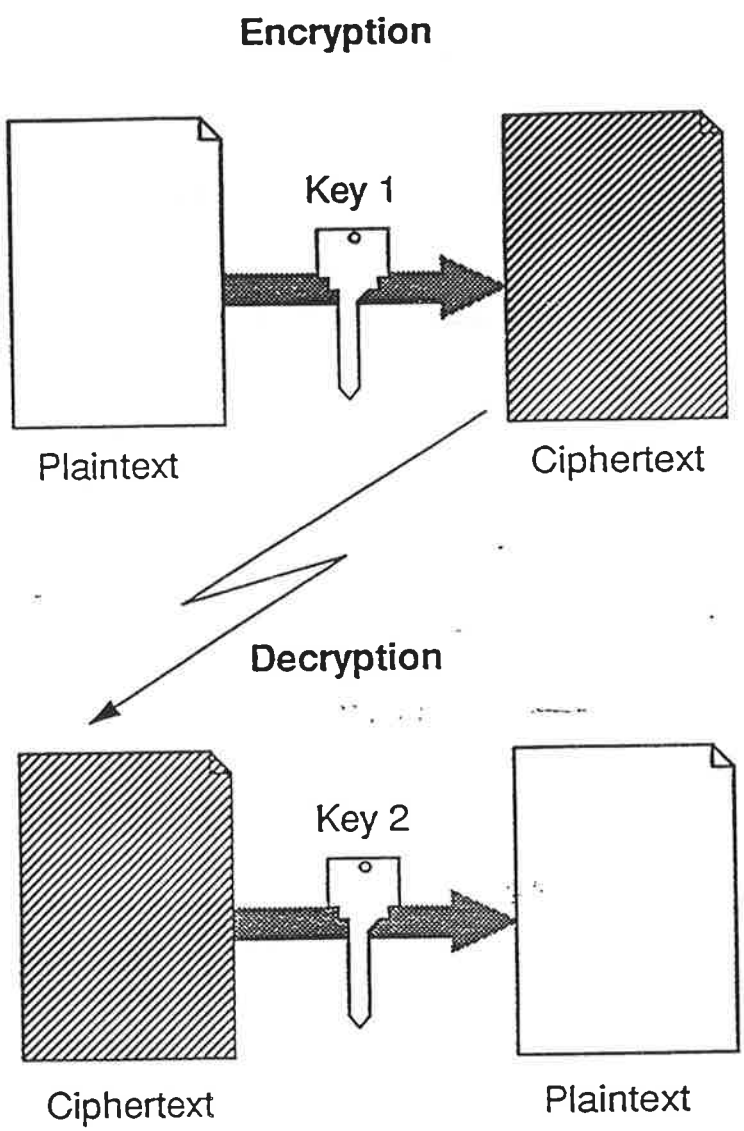
Key 1 = Key 2

Public-Key Cryptography



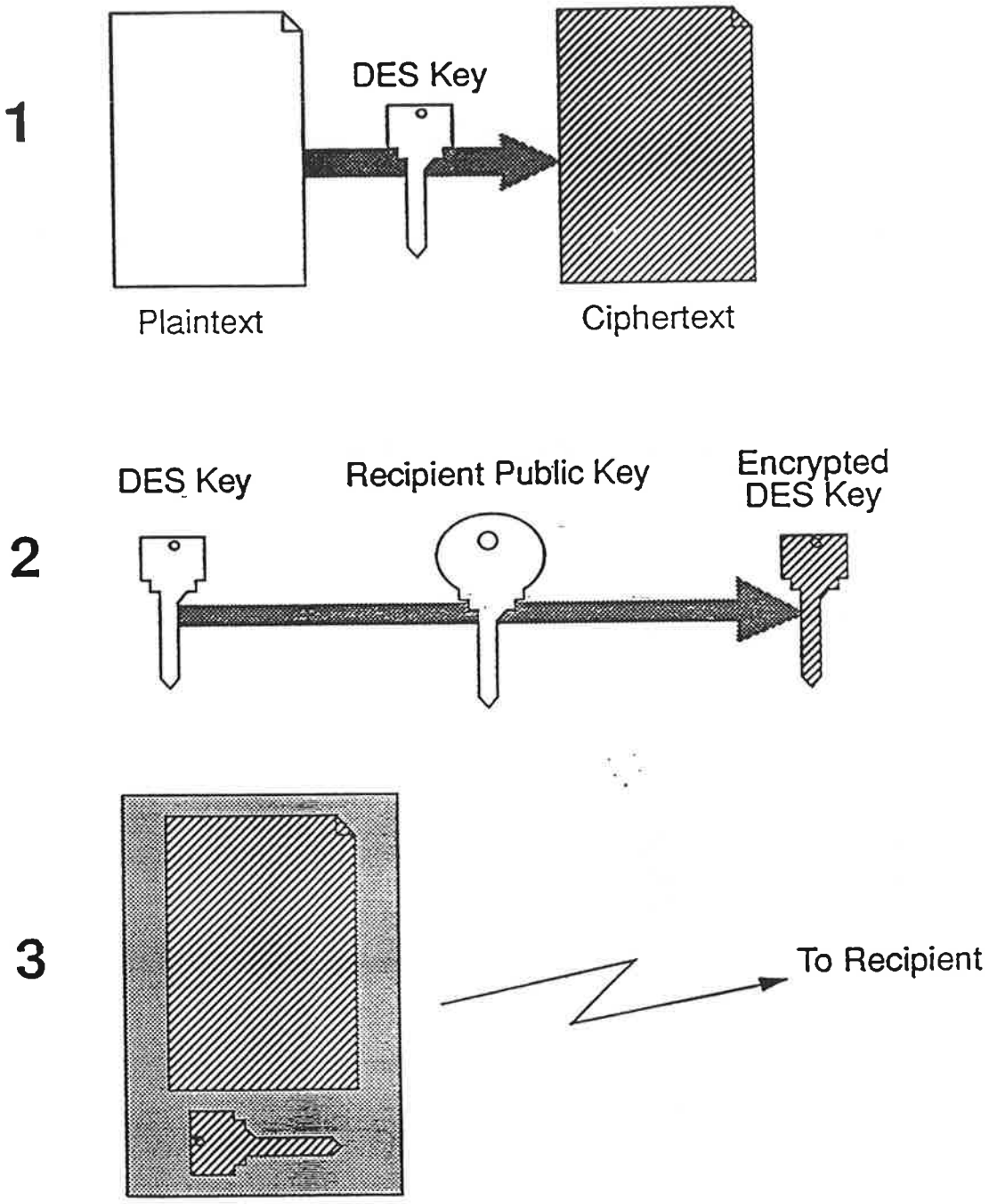
- Privacy
  - — Key 1 = Recipient's Public Key
  - — Key 2 = Recipient's Private Key

Public-Key Cryptography

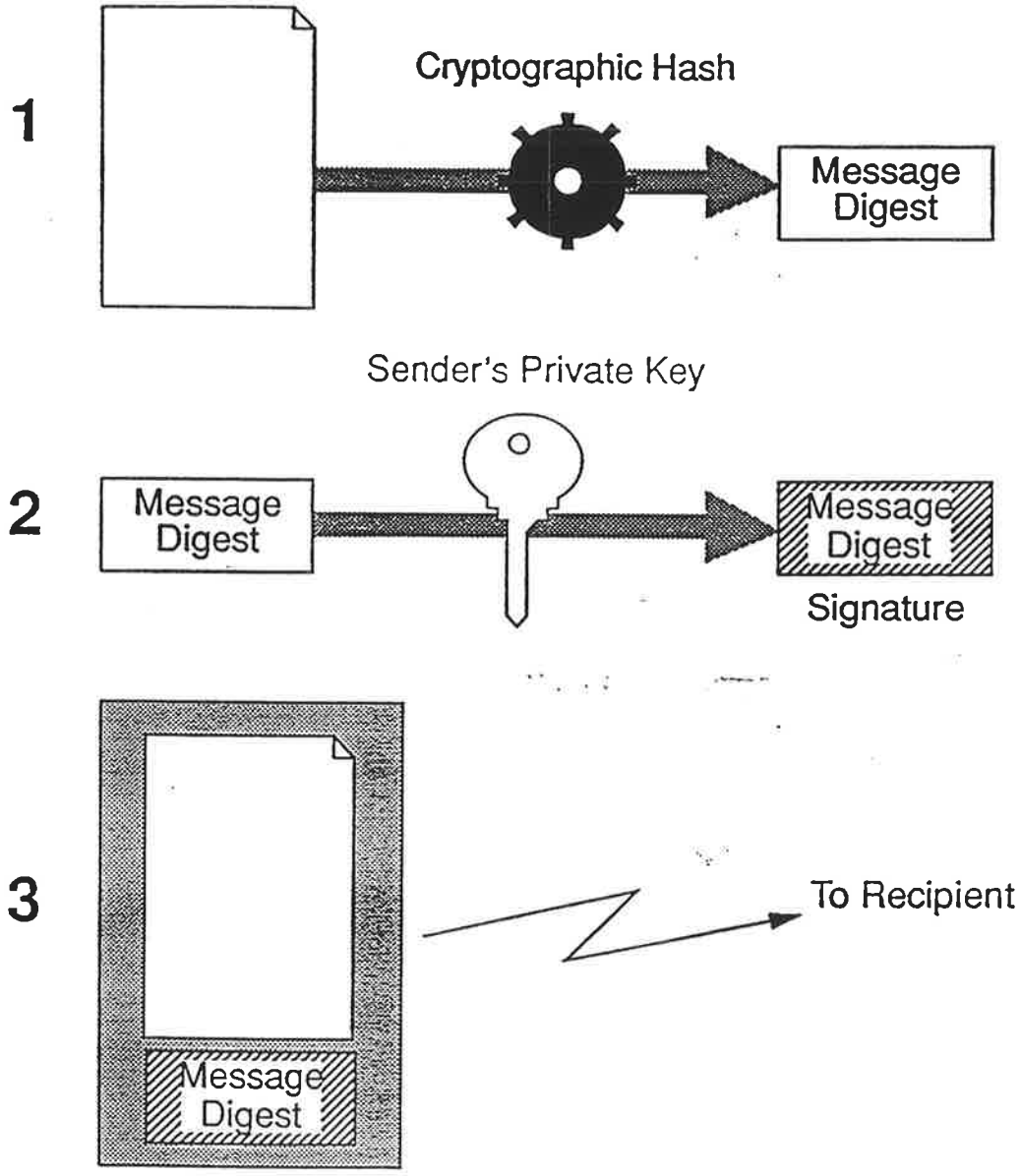


- Authentication
  - — Key 1 = Sender's Private Key
  - — Key 2 = Sender's Public Key

Practical Privacy Using Public-Key

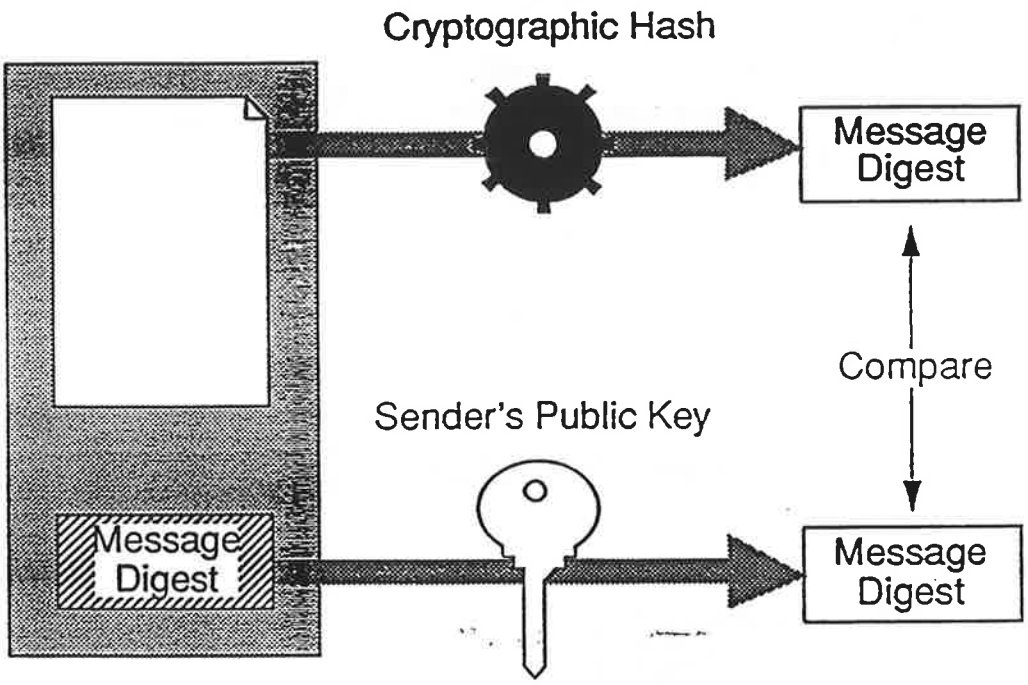


Practical Authentication Using Public-Key



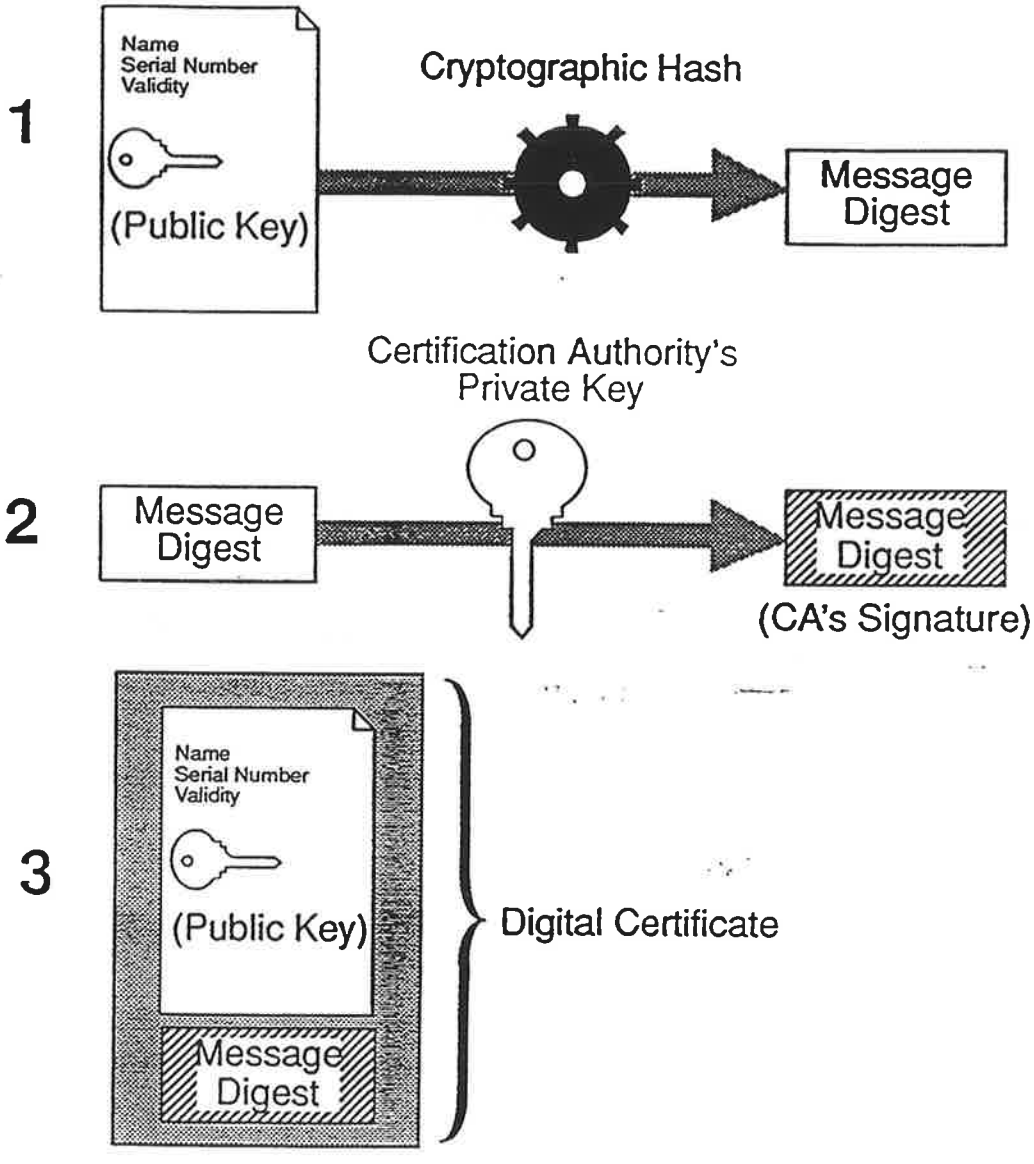
(Digital Signature Creation)

Practical Authentication Using Public-Key



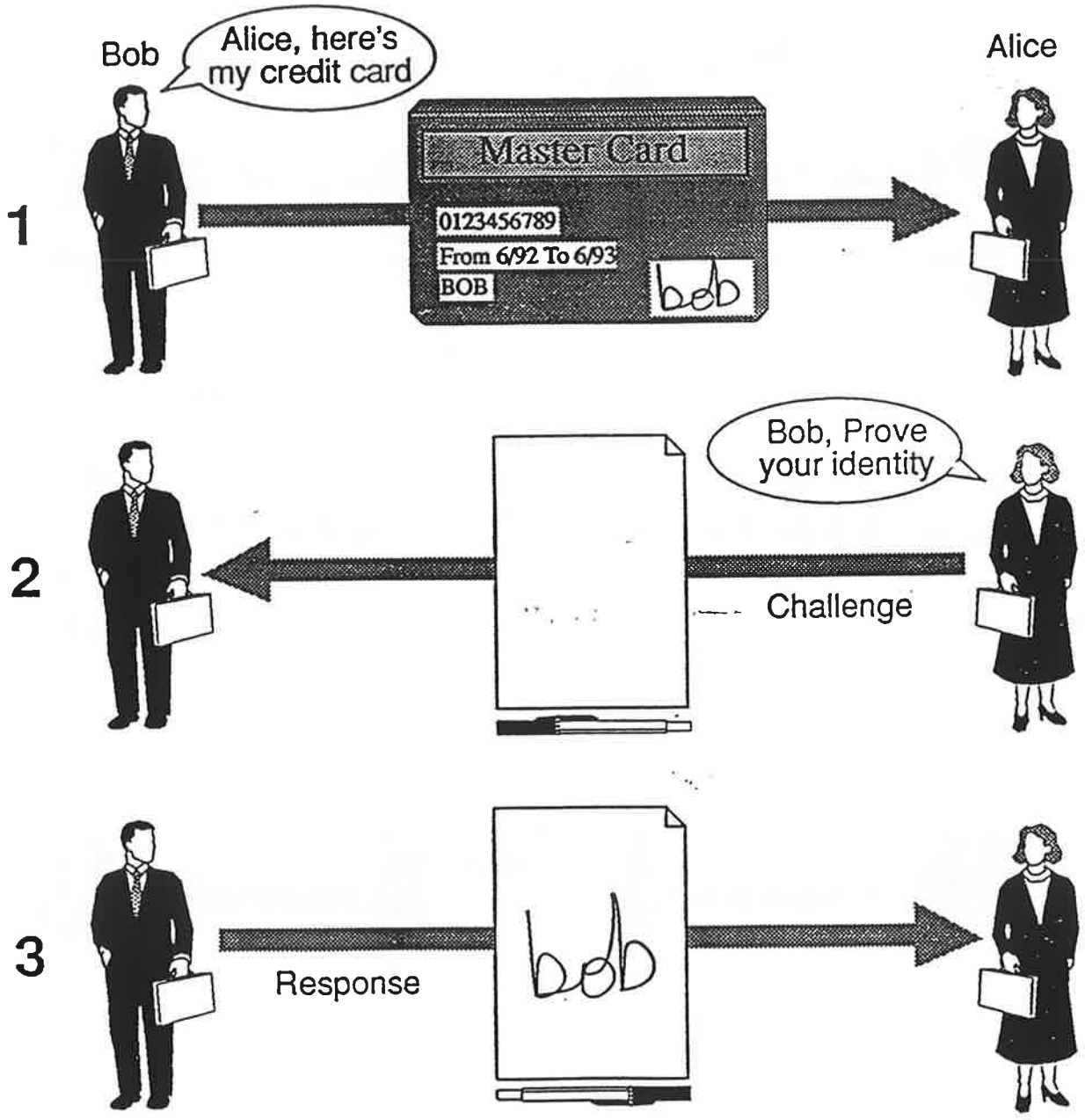
(Digital Signature Verification)

Secure Public-Key Distribution

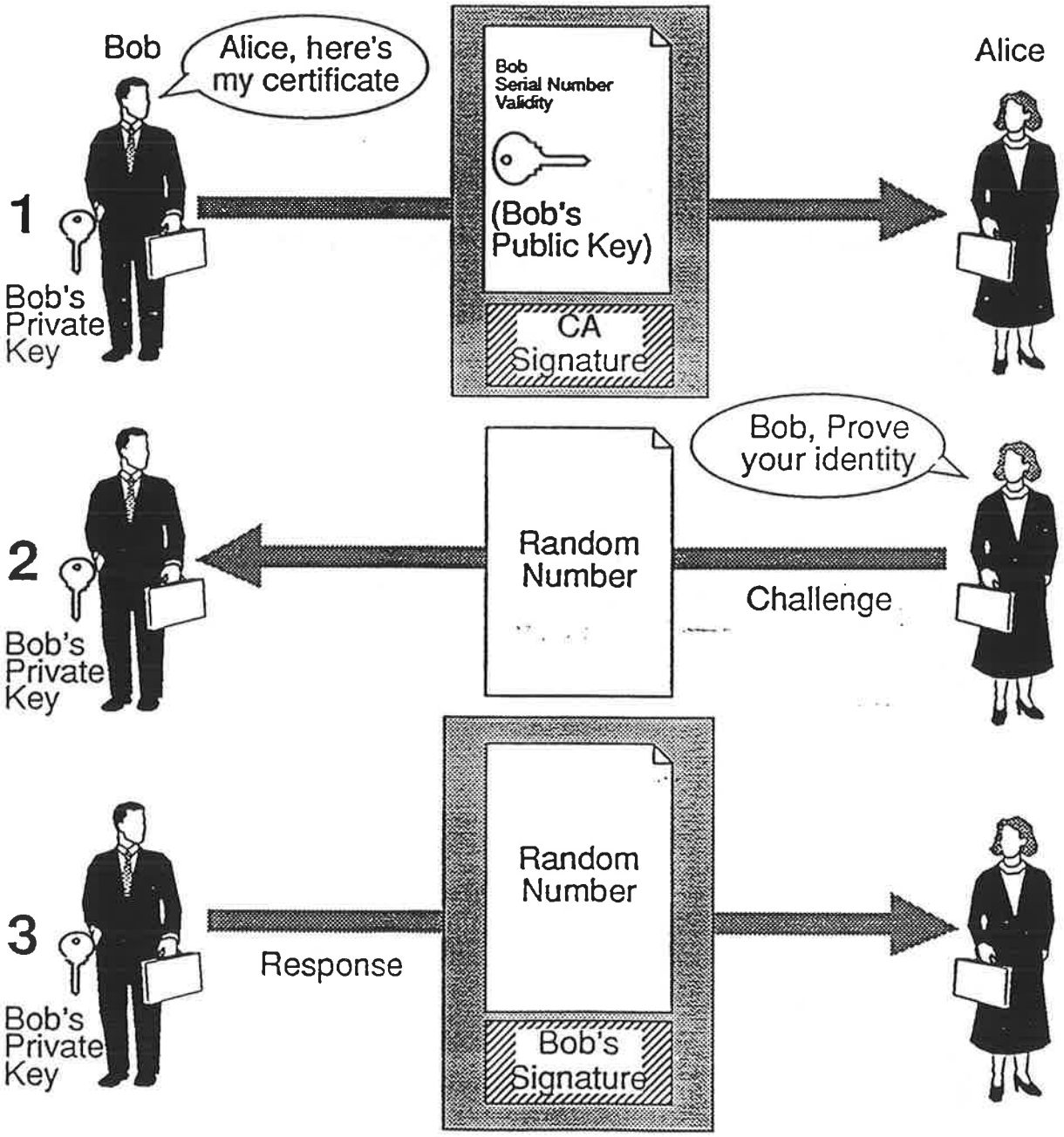


(CA Public-Key Universally Known)

Human Challenge-Response Protocol



Digital Challenge-Response Protocol



Cryptography Guarantees Authenticity

- Message sent by Intruder will decrypt to nonsense.
- Intruder may inject messages, but cannot 'get them accepted.'

Cryptography Guarantees Privacy

- Only authorized receivers who know secret keys can decrypt
- Eavesdropper may intercept message, but cannot understand it.

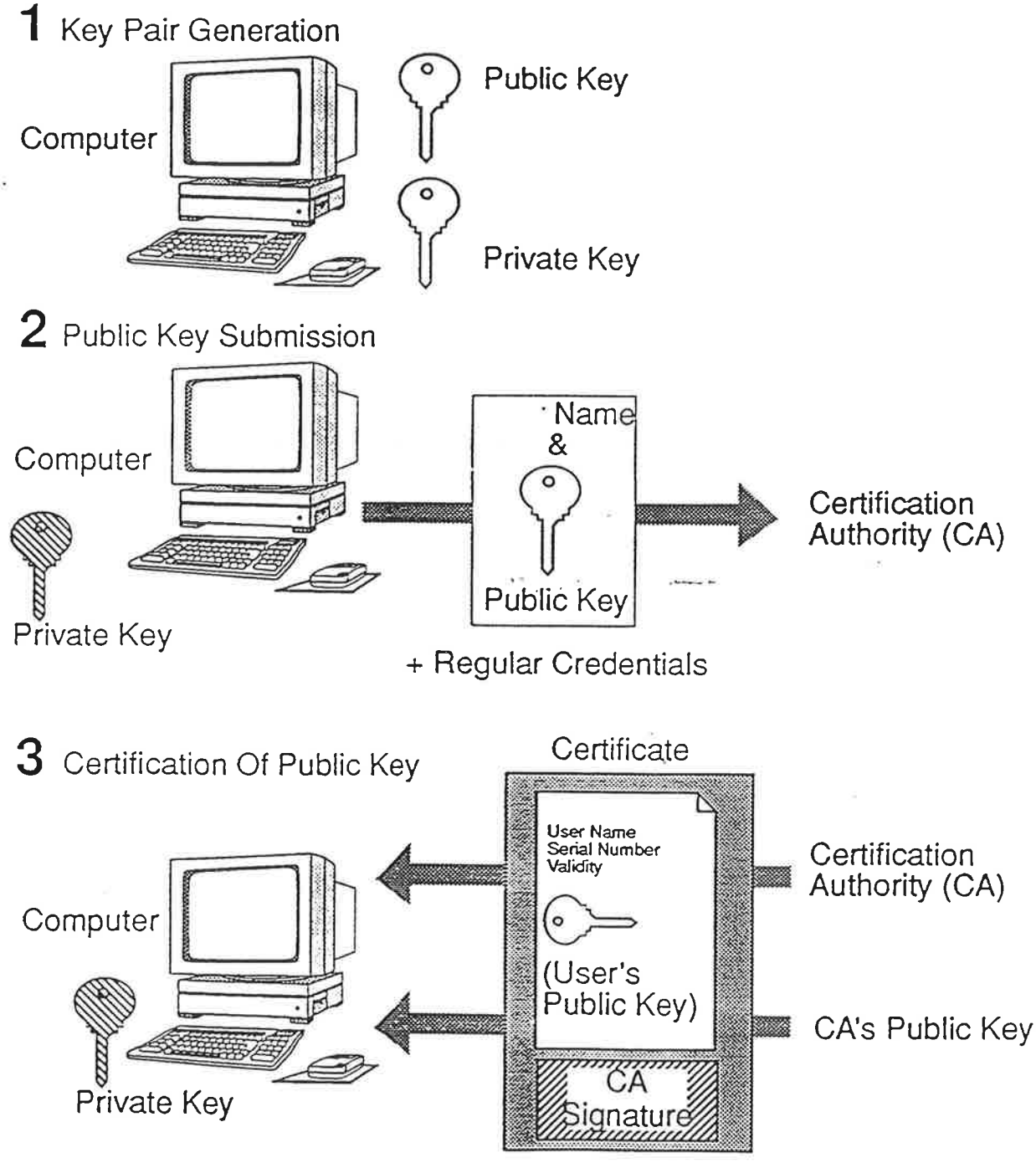
Security Protocol Goals

- Provide for privacy and authentication over wireless link.
- Authentication must be mutual authentication, i.e both the Base and the Mobile should be able to authenticate each other.
- Data sent over wireless link must be confidential (private).

- This protocol is a replacement for the physical security of ethernet. Host to Host authentication considered adequate for this purpose.

  Host-to-host authentication conceptually correct for a link layer protocol.

Initial Configuration Process



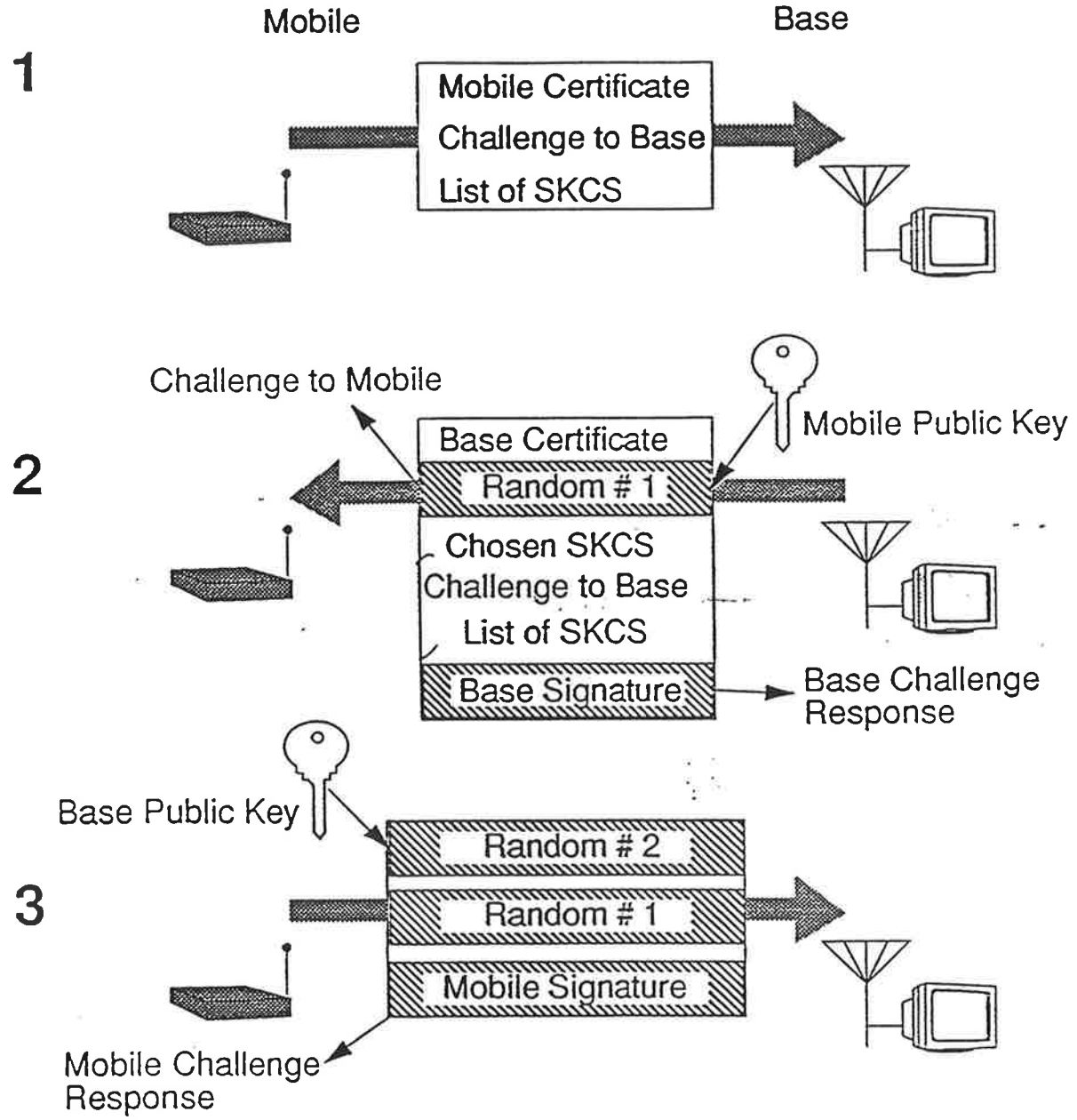
Mobile Configuration Information

- Public key(s) of CA(s)
- Certificate Issued to Mobile
- Private Key of Mobile saved in encrypted form
- Latest copy of Certificate Revocation List

Base Configuration Information

- Access to Base certificate (may be locally stored)
- Access to public keys of all the CAs
- Access to up-to-date version of Certificate Revocation List
- Private key of Base station saved in a protected manner

Wireless Security Protocol



Session Key = (Random # 1 ⊕ Random #2)