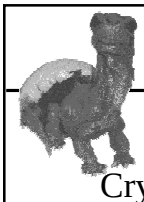
This Week

- Last week of classes
- Lot's of surveys
- Exam, 17 June, 9:30am, EA006
- Watch mail for demo signup.



Cryptography and Security

Comp 305 Lecture 12

Quote of the Week

"… about 25% of the computer keyboards used by people in most companies have the password written underneath."

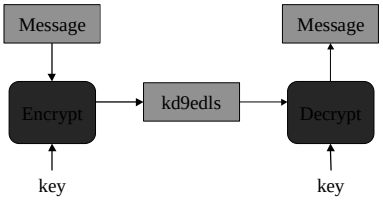
Simon Naylor
Security Dynamics
in InfoTech Weekly

Security in Distributed Systems

- Policy required to address:
  - Preventing unauthorised access
  - Avoiding denial of service
  - Communication between trusted sites
  - Information access by unknown parties
  - Access to active objects
  - Communication with unknown parties
  - Authenticated transaction

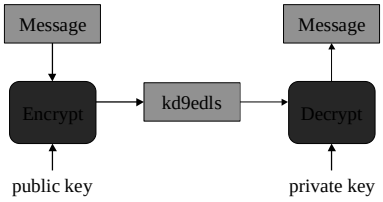
Cryptography

- Standard private key encryption



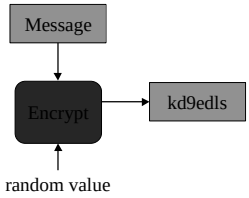
Cryptography

- Standard public key encryption



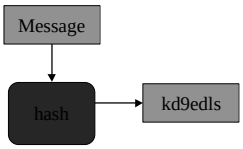
Cryptography

- One way encryption

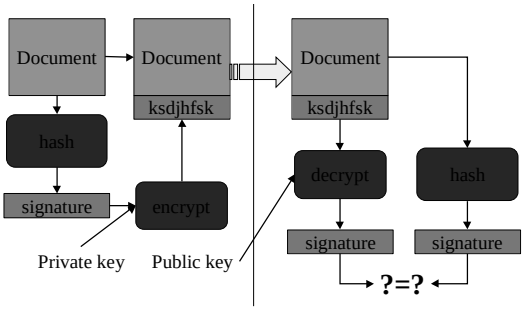


Cryptography

- Signature =
  compression + one way hash

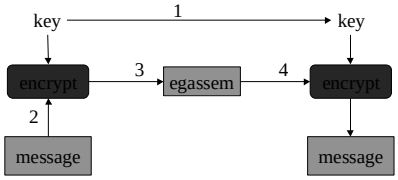


Signing a Document



Private Key Cryptography

- Key exchanged “off-line”
- Requires previous arrangement by parties

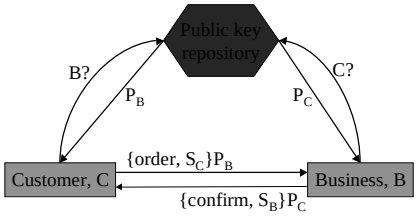


Cryptographic Algorithms

- Private key
  - DES, IDEA, Blowfish
- Public key
  - RSA, Diffie-Hellman
  - Expensive
- Hash
  - MD5

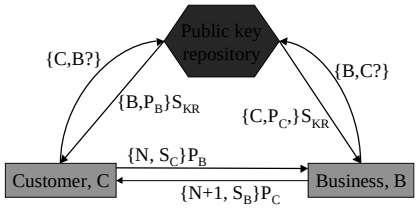
Secure Communication with Strangers

- Key repository



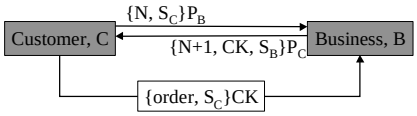
Secure Communication with Strangers

- Key repository



Conversation Keys

- Public key encryption is inefficient
- Switch to private conversation key



Private Transactions