Introduction to Network Security

Appendix A

Cryptology

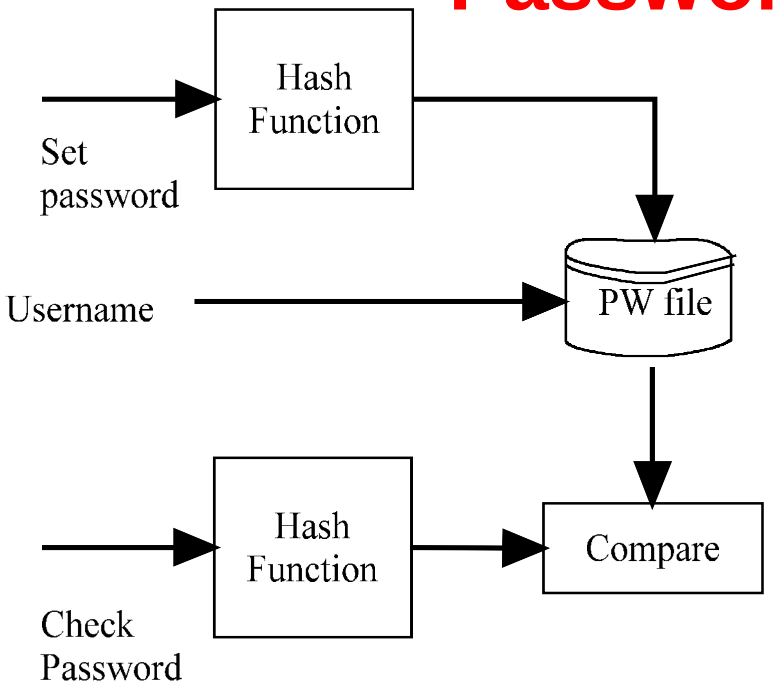
Topics

- Hash Functions
- Symmetric Key Encryption
- Asymmetric Encryption
- Digital Signatures
- Symmetric Key Distribution

Hash Functions

- One way encryption
- Takes n bytes of data and computes a fixed size hash
- Many to one mapping
- Used to ensure data has not been modified
- Used for passwords (see next slide)
- Collisions occur when different data have same hash value

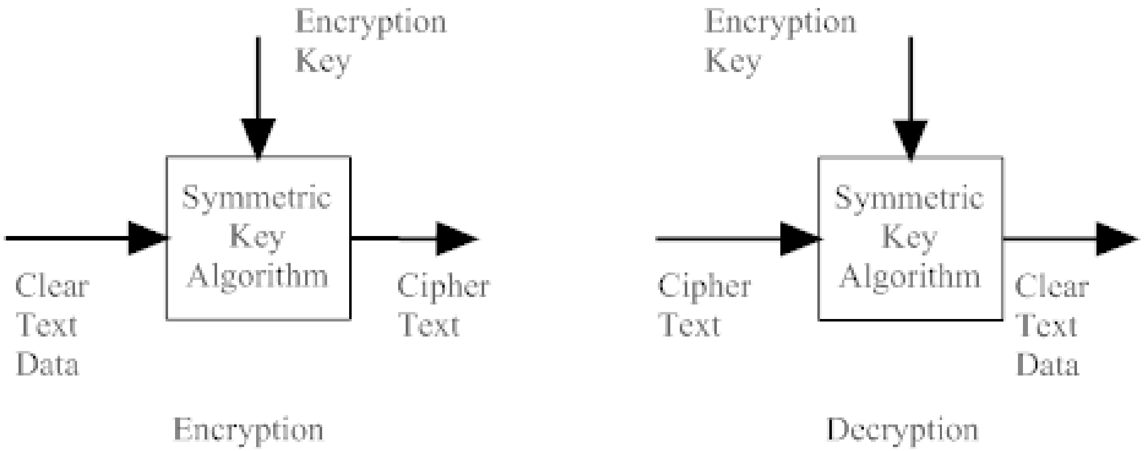
Hash Functions for Passwords



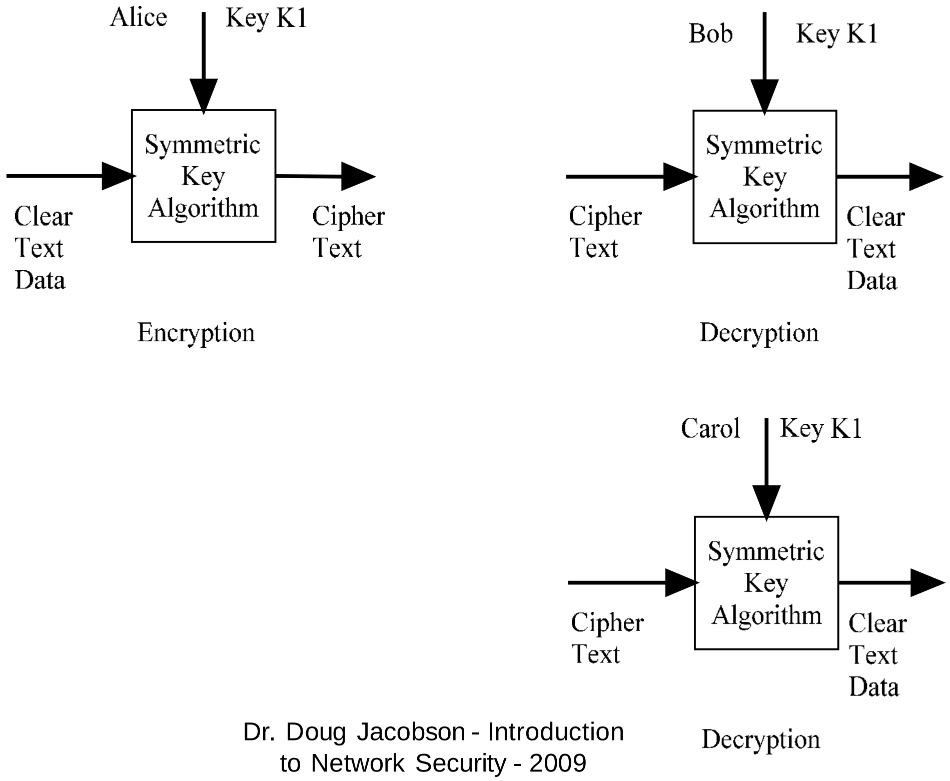
Symmetric Key Encryption

- One key to encrypt and decrypt
  - – Idea
  - – DES
  - – AES

Symmetric Key Encryption



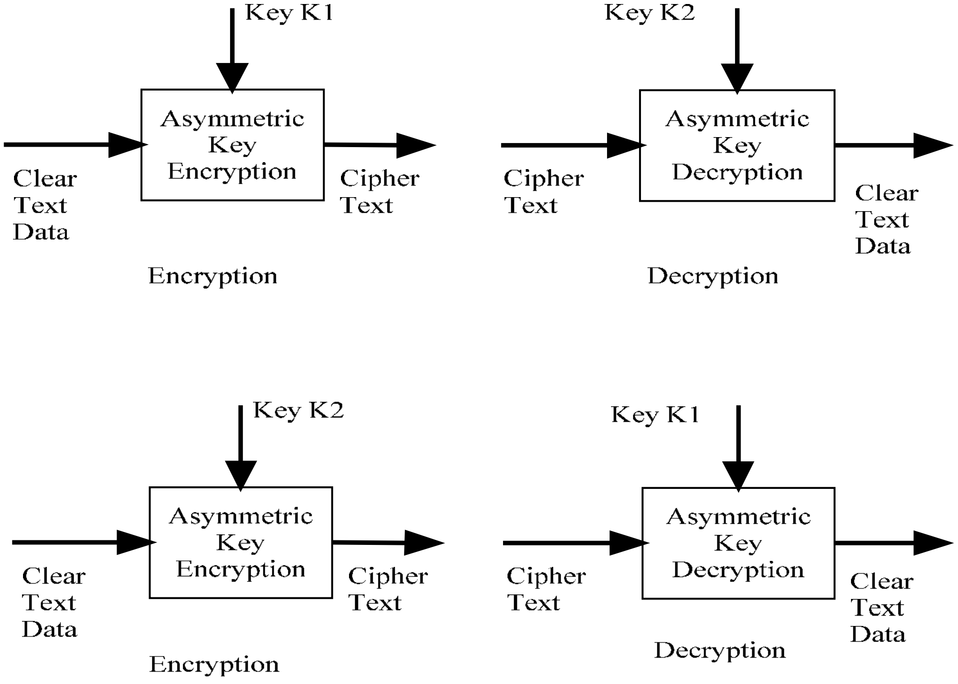
Multiple Key Encryption



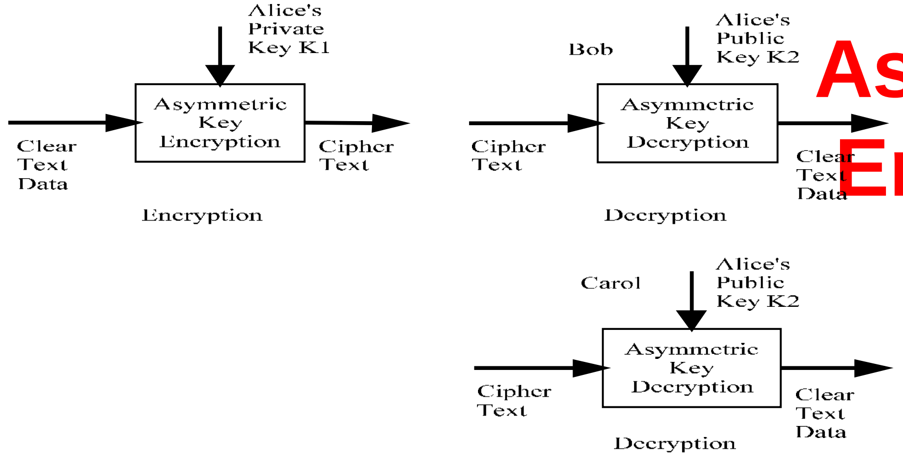
Asymmetric Encryption

- Matched set of keys
- One public, one private
- Either key can encrypt but other key must be used to decrypt
- Publish public key

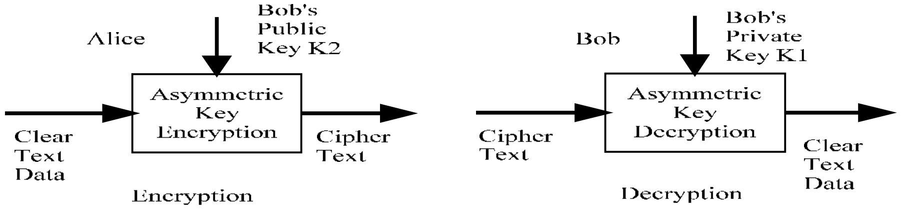
Asymmetric Encryption



Using Asymmetric Encryption

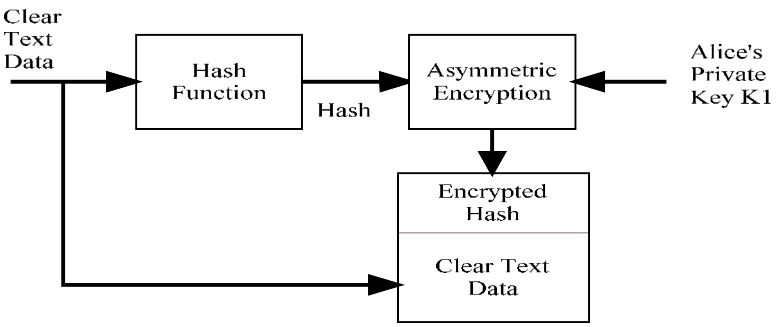


Verifying Alice as a sender



Verifying Bob as a receiver

Digital Signature



Clear Text Data

Hash Function

Hash

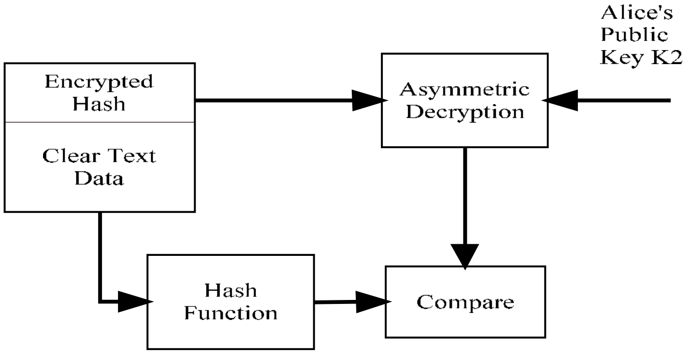
Asymmetric Encryption

Alice's Private Key K1

Encrypted Hash

Clear Text Data

Creating a digital signature



Alice's Public Key K2

Encrypted Hash

Clear Text Data

Asymmetric Decryption

Hash Function

Compare

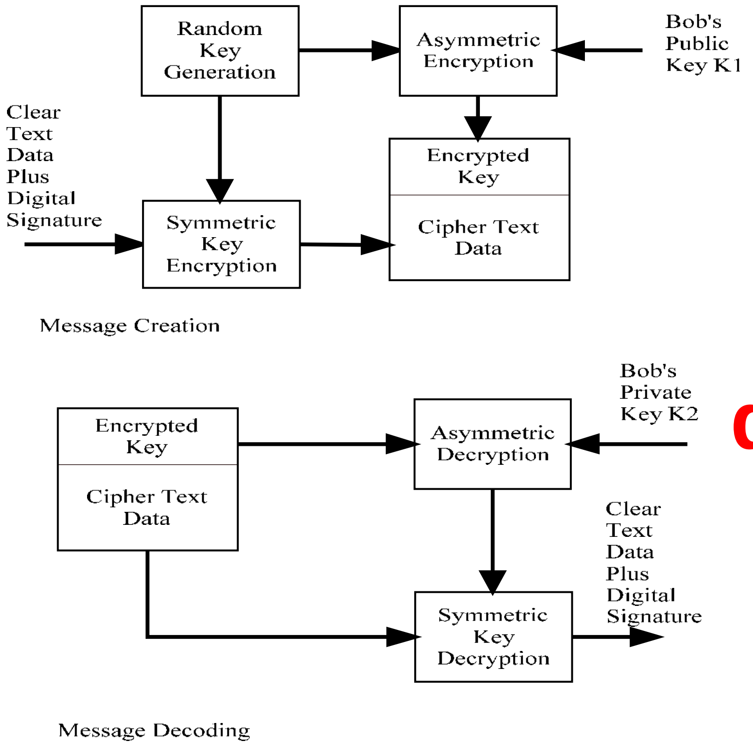
Problems with Asymmetric Key Encryption

- Time to compute
- Key revocation

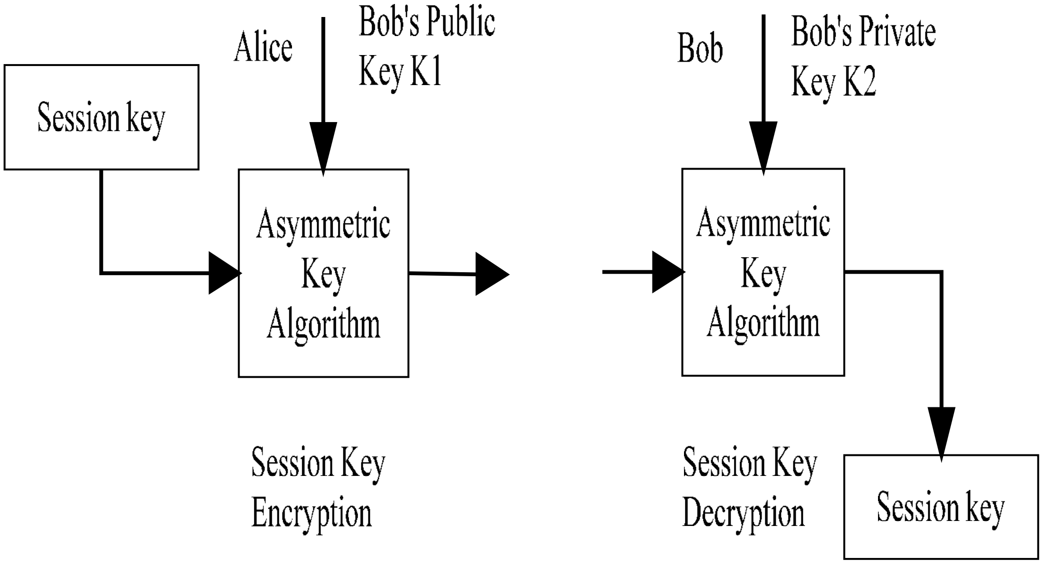
Key Distribution

- Symmetric
  - Physical distribution
  - Use old key to deliver new key
    - Doesn’t scale well
  - Trusted third party
    - Kerberos
- Asymmetric
  - Common knowledge
  - PKI

Message-based symmetric key distribution



Network-Based Symmetric key exchange



Dr. Doug Jacobson - Introduction to Network Security - 2009