CSE 543 - Computer Security

Lecture 4 - Cryptography
September 14, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/

Review: secret vs. public key crypto.

- Secret key cryptography
  - Symmetric keys, where A single key (k) is used is used for E and D
  - D(E(p, k), k) = p
- All (intended) receivers have access to key
- Note: Management of keys determines who has access to encrypted data
  - E.g., password encrypted email
- Also known as symmetric key cryptography

- Public key cryptography
  - Each key pair consists of a public and private component:

    k+ (public key), k- (private key)

    D(E(p, k+), k-) = p

    D(E(p, k-), k+) = p
- Public keys are distributed (typically) through public key certificates
  - Anyone can communicate secretly with you if they have your certificate
  - E.g., SSL-base web commerce

The symmetric/asymmetric key tradeoff

PENNSTATE

- Symmetric (shared) key systems
  - Efficient (Many MB/sec throughput)
  - Difficult key management
    - Kerberos
    - Key agreement protocols
- Asymmetric (public) key systems
  - Slow algorithms (so far …)
  - Easy (easier) key management
    - PKI - public key infrastructures
    - Webs of trust (PGP)