Security

Note Title 12/10/2008

- Secrecy
- Authentication
- Non-repudiation
- Integrity

Threat Model
Who is trying to do what to the communications and what tools and techniques do they have available

---

Cryptography – "secret writing"

Notation

P : plaintext
C : cyphertext
K : Key
E : $E_K(P)$ encryption w/ key K
D : $D_K(C)$ decryption w/ key K

Sender of msg computes $C = E_{K_1}(P)$
sends C
Receiver computes $P = D_{K_2}(C)$

Symmetric Key Crypto : $K_1 = = K_2$

Public Key Crypto : $K_1 \neq K_2$

Kerckhoff's principle:
all Crypto algorithms must be considered public — only keys are secrets.

Public Key Crypto: (K_1, K_2) : A key pair

$D_{K_2}(E_{K_1}(P)) = P$: K_1 is made public.

How to use PKC:

Requirement for a key pair to be useful for crypto:
given D, E, K_1 : it is very hard to figure out K_2; given $E_{K_1}(P)$ very hard to figure out P.