Nov-25-2014

Note Title 8/28/2014

Security

- Encryption m K

ciphertext = K(m)

+ One time pad
+ sub alg

- Symetric Key $K_{A-B}(m)$

$K_{A-B}(K_{A-B}(m)) = m$

- Public key K_B^+ K_B^-

$K_B^+(m)$ ⟷ B $K_B^-(m) \rightarrow m$

$K_B^-(K_B^+(m)) = m = K^+(K^-(m)) = m$

Note Title 8/28/2014

- Problems
  + Symtric Key → Key Distribution
  + Public Key → K_B^+ really is Bob's
- Solution Symtric key → KDC ↴ Kerberos
- Digital Signatures & Hashes -