CSE 543 - Computer Security

Lecture 5 - Public Key Cryptosystems
September 11, 2007
URL: http://www.cse.psu.edu/~tjaeger/cse543-f07/

Key Distribution/Agreement

- Key Distribution is the process where we assign and transfer keys to a participant
  - Out of band (e.g., passwords, simple)
  - During authentication (e.g., Kerberos)
  - As part of communication (e.g., skip-encryption)
- Key Agreement is the process whereby two parties negotiate a key
  - 2 or more participants

- Typically, key distribution/agreement this occurs in conjunction with or after authentication.
  - However, many applications can pre-load keys

Diffie-Hellman Key Agreement

PENNSTATE

- The DH paper really started the modern age of cryptography, and indirectly the security community
  - Negotiate a secret over an insecure media
  - E.g., "in the clear" (seems impossible)
  - Idea: participants exchange intractable puzzles that can be solved easily with additional information.

- Mathematics are very deep
  - Working in multiplicative group G
  - Use the hardness of computing discrete logarithms in finite field to make secure
  - Things like RSA are variants that exploit similar properties