Shared/Symmetric vs. Public/Private

- Shared keys reveal too much information
  - Hard to *revoke* permissions from principals
  - E.g., group of principals shares one key

    → want to remove one principal from group

      → need everyone in group to change key
- Public/private keys involve costly encryption or decryption
  - At least one of these 2 operations is costly
- Many systems use public/private key system to generate shared key, and use latter on messages