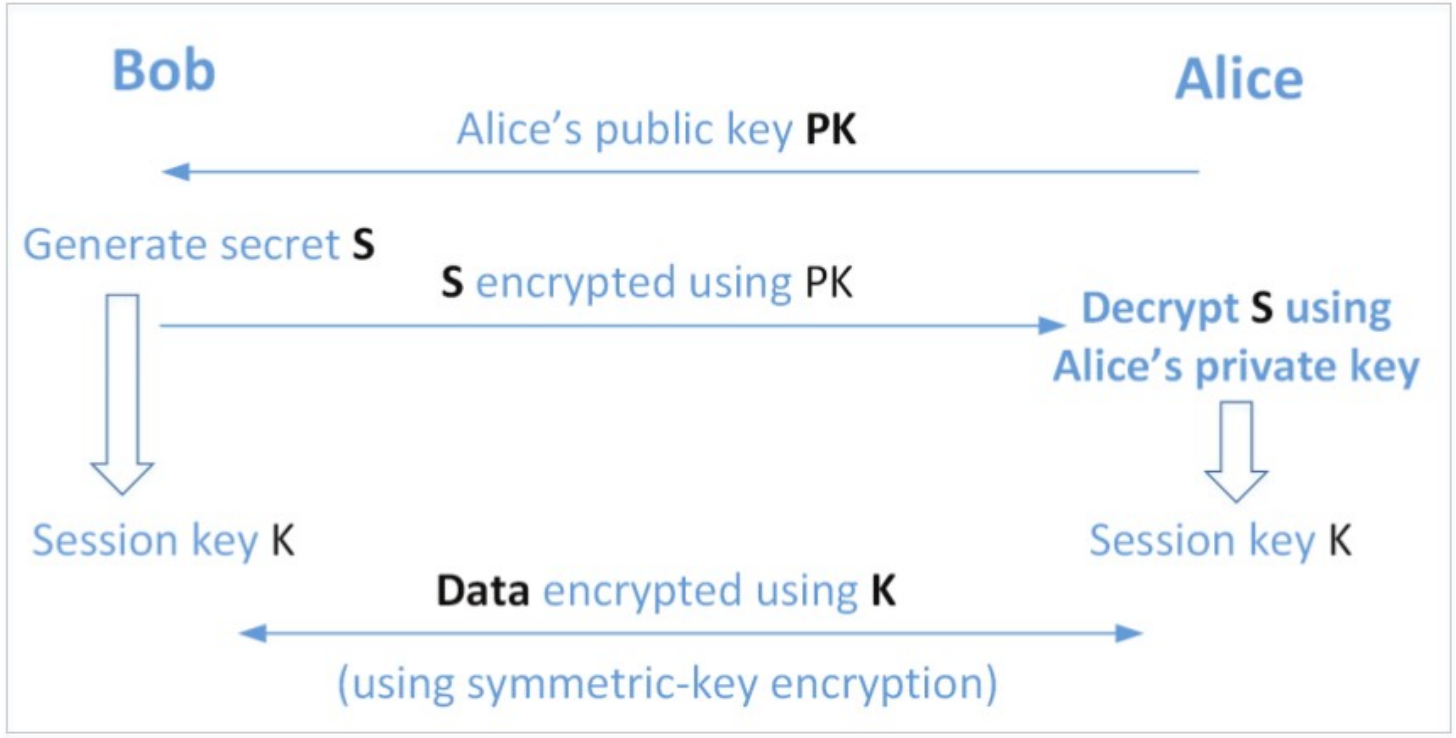
Public Key Cryptography

Applications of Public Key Criptography: HTTPS and TLS/SSL

- HTTPS protocol is used to secure web services
- HTTPS is based on the TLS/SSL protocol (uses both public key encryption and signature)
  - encryption using secret-key encryption algorithms
  - public key algorithms are mainly used for key exchange

Applications of Public Key Criptography: HTTPS and TLS/SSL (Contd.)



Use of public key algorithms for (symmetric) key exchange

- Problems?
  - If RSA is used, the pre-master secret is ciphered with server's public key
  - Scenario:
    - Ciphered stream is recorded for one year
    - Server is recycled and its private key is stolen
    - Attacker can now decrypt pre-master secret and rebuild master secret and session keys and hence decrypt stored communications
  - Perfect Forward Secrecy property must be guaranteed

Diffie-Hellman Key Exchange

- Allows communicating parties with no prior knowledge to exchange shared secret keys over an insecure channel
- Alice and Bob want to communicate
- Alice and Bob agree on:
  - Number p: big prime number (such as a 2048-bit number)
  - Generator g: small prime number (such as 2 and 3)
- Alice picks a random positive integer $x < p$
- Bob picks a random positive integer $y < p$

Diffie-Hellman Key Exchange (Contd.)