Public-Private Key Cryptography

- If Alice wants to send a secret message M that can be read only by Bob
  - Alice encrypts it with Bob's public key
  - $K_{Bpub}(M)$
  - Bob only one able to decrypt it
  - $K_{Bpriv}(K_{Bpub}(M)) = M$
  - Symmetric too, i.e., $K_{Apub}(K_{Apriv}(M)) = M$