Public Key Cryptography

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 21 Dec 2021,
public.tex, r1944

Contents

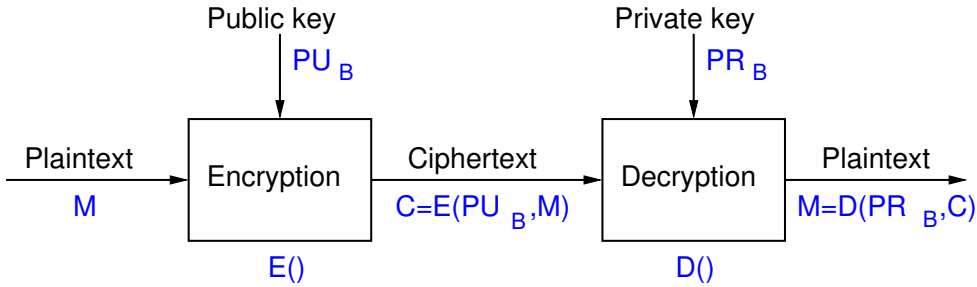
Public Key vs Symmetric Key

- Symmetric Key Encryption
  - Same key used for encryption and decryption
  - Key is randomly generated (e.g. by sender)
  - Problem: How does receiver securely obtain secret key?
- Public (or asymmetric) key encryption
  - Two different, but mathematically related keys
  - One key (public) for encryption, another key (private) for decryption
  - Since encrypt key is public, key exchange is not a problem
  - Ciphers designed around math problems
  - Problem: Performance: much, much slower than symmetric

Public and Private Keys

- Every user has their own key pair: (PU, PR)
  - Keys are generated using known algorithm (they are not chosen randomly like symmetric keys)
- Public key, PU
  - Available to everyone, e.g. in email signature, on website, in newspaper
- Private key, PR
  - Secret, known only by owner, e.g. access restricted file on computer
- Ciphers: if encrypt with one key in the pair, can only successfully decrypt with the other key in the pair

Confidentiality with Public Key Crypto



- User A is sender, user B is receiver
- Encrypt using receivers public key, PU_B
- Decrypt using receivers private key, PR_B
- Only B has PR_B, therefore only B can successfully decrypt $\rightarrow$ confidentiality

Why Does Public Key Crypto Work?

- Public key ciphers consist of:
  - Key generation algorithm
  - Encryption algorithm
  - Decryption algorithm
- Designed around computationally hard mathematical problems
- Very hard to solve without key, i.e. trapdoor functions
  - Finding prime factors of large integers
  - Solving logarithms in modulo arithmetic
  - Solving logarithms on elliptic curves

Public Key Crypto Examples

- RSA (Rivest Shamir Adleman)
  - Security depends on difficult to factor large integers
  - Widely used for digital signatures
- Diffie-Hellman
  - Security depends on difficult to solve logarithms in modulo arithmetic
  - Widely used for secret key exchange
- Elliptic Curve
  - Security depends on difficulty to solve logarithms on elliptic curve
  - Newer, used in signatures and key exchange
  - Smaller keys is benefit