Public Key encryption / Two key encryption

- 2 keys created, 1 chosen to be public, the other chosen to be private
- Have
  - Plain-text
  - Encryption algorithm
  - Public/Private keys
  - Decryption algorithm
- Requirements
  - Easy for receiver to generate keys
  - Easy for receiver to generate plain-text from keys
  - Unfeasible for attacker to know private key from public key
- RSA
  - Most widely used
  - Larger keys = worse performance
- Asymmetric encryption algorithms
  - RSA
  - Diffie-Hellman
  - DSS
  - ECC

Digital Envelopes

- Protects message without sender/receiver having same secret key
- Same as sealed envelope with unsigned letter

Random Numbers

- Sessions keys
- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Handshaking to prevent replay attacks
- Requirements
  - Uniform distribution
  - Independence (should not be able to derive one value from another)
- Pseudo-randomness
  - Likely to be predictable
  - Satisfy randomness tests
- Practical Applications
  - Encryption of stored data