Asymmetric key cryptography

- Also called Public Key Cryptography. A pair of keys are used
- Public key: used for encryption
- Private key: used for decryption. Only known to the owner. Only the corresponding private key can decrypt
- Requirements:
  - It's computationally infeasible to find the private key given only the algorithm and public key
  - It's computationally easy to en/decrypt a message using the relevant key