# Digital signatures

- When A sends to B, A uses B's public key to encrypt, so the message is confidential

- In many situations we need "signatures" to verify the identity of someone

- We can use a different scheme
  - A uses his private key to encrypt a message
  - Anyone can check the message is signed by A by using A's public key
  - Only A can sign the message