Counter replay attacks

Several solutions:

- **use a nonce (random number)**
- use sequence numbers
- use timestamps
- have fresh key for every transaction
  (key exchange problem)

Defeat replay attack with a nonce (not fully secured)