Passwords

problem: store human password m
issue: m short / low entropy

- the worst: store m (even if encrypted)
- still bad: store H(m) instead of m
  one-way hash
- better: generate random s for each m, store s, H(m,s)
  salt
- good: use a slow (!) hash function H
  [SHA 2/3: very fast]

EG PBKDF2, bcrypt, scrypt
- PBKDF2: WPA2: based on SHA-1 (4096 iterations)
- scrypt: also increases memory consumption

conclusion: store salted hashes + use slow hash