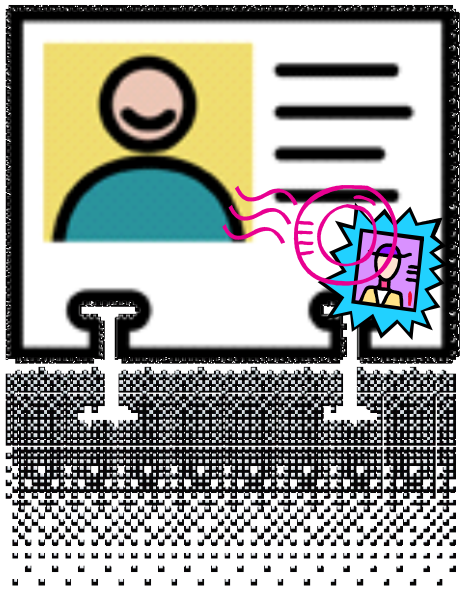
Digital Certificates, Trust

(Digital) Certificates

- A certificate binds a public key to a specific user. It consists of three things
  - Public key
  - User info: name, etc
  - Digital signature of attester



Public-Key Infrastructure

- Public-Key Infrastructure (PKI)
  - Certificate storage
  - Certificate server
  - Public-key management
- CA = certificate authority (certification)
  The CA creates certificates & signs them
- RA = registration authority
  Supports the registration of users w/in the PKI

Establishing Trust

- Direct trust
- Hierarchical trust (PKI, CA)
- Web of trust – PGP
  → key signing parties

- Revocation of keys are not trivial
  (if you lose the key or it gets stolen)

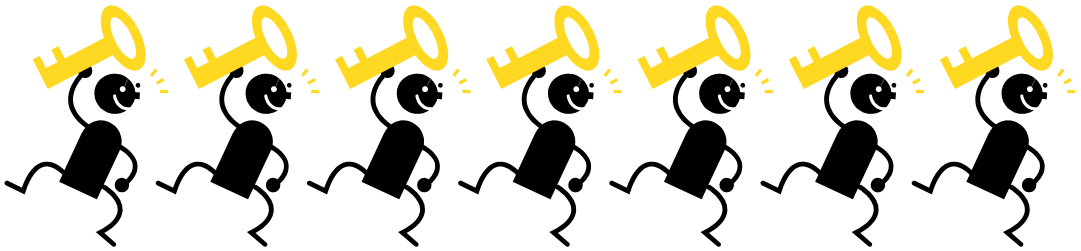
Key management problems
The key length is not the full truth

- Many factors influence the security of the cryptographic scheme
  - Key management
  - Key storage
  - Key generation
  - Badly selected keys / parameters / picture
  - Backdoors, social engineering

➔ Go after lowest-hanging fruit – weakest part

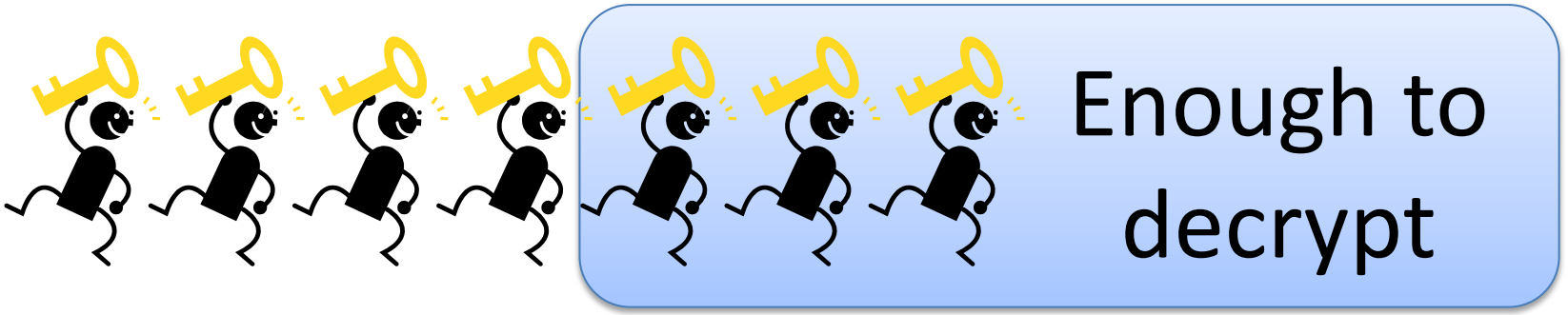
Next steps …

- Threshold cryptography



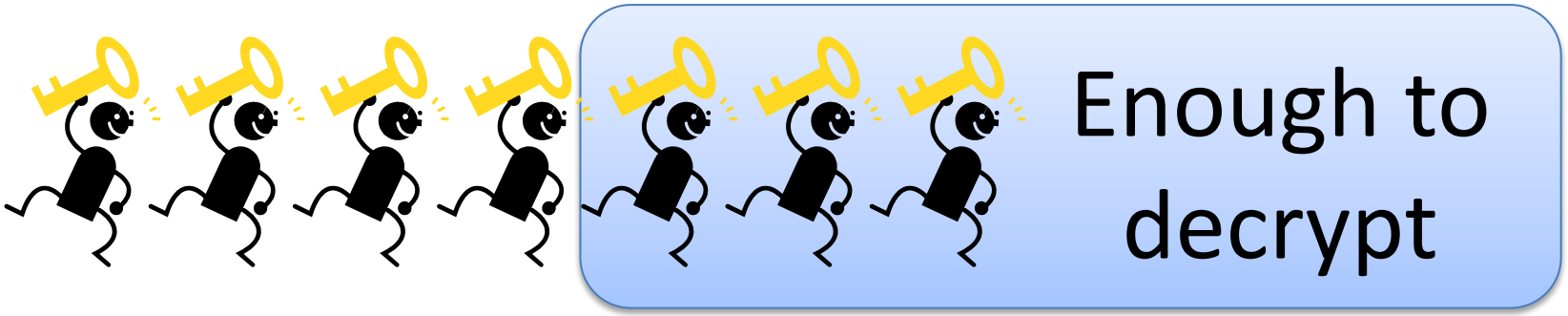
Next steps …

- Threshold cryptography



Next steps …

- Threshold cryptography



- Zero-knowledge proofs
  - Prove that you know something without telling the secret.
  - Convince one person but in such a way that he cannot in turn convince another that he has the secret.