# Quick Review: primitives

**To protect non-secret data**: (data integrity)

- using small read-only storage: use collision resistant hash
- no read-only space: use MAC … requires secret key

**To protect sensitive data**: only use authenticated encryption

(eavesdropping security by itself is insufficient)

**Session setup**:

- Interactive settings: use authenticated key-exchange protocol
- When no-interaction allowed: use public-key encryption