4 密码学
4.1 加密技术 2种：概念+优劣
4.2 密码长度作用
4.3 混合模式安全方案
4.4 哈希算法
4.4.1 完整性
4.4.2 加密vs哈希，逆向哈希
4.4.3 哈希在数字签名作用

4.1 ① symmetric : one

Asymmetric : two entryption decryption

fast✓ secure✓

S~ : ~~efficiency~~ ✓ short ✓ exchange y

A~ : exchange ✓ long x many key x

slow x less secure x

4.2 long ↑ crack time ↑

4.3 ① Adv. Disadv.

② hybird —— generate session key

share PK.

encrypt by session key

throughput ✓ key management ✓

4.4.1 one way compression function

no way to get plain text

4.4.2 encryption → ∈

hash → ∉

4.4.3 ① size ↓

② Detect change