§1.3 信息安全的发展

一、密码理论的发展

第一阶段（1949年前）：初期阶段，未形成一门独立学科

第二阶段（1949～1976）：形成学科阶段，

标志：Shannon发表的“保密通信的信息理论”

第三阶段（1976年后）：新体制形成与发展阶段，

标志：Diffie和Hellman发表的“密码学的新方向”，

公钥密码体制诞生了

第四阶段（20世纪80年代）：量子密码学的兴起。

§1.3 信息安全的发展

二、信息安全的发展趋势

1、技术创新与融合

2、量子计算倒逼密码体系升级

3、地缘政治加剧供应链与数据主权风险

4、身份与访问管理面临新挑战

5、安全范式从“成本中心”转向“业务赋能”