密码学可以实现哪些安全特性，如何实现

古典密码体制及其实现

哈希函数的定义、性质及实现

对称密码体制分类、常用算法、模式及实现

非对称密码体制常用算法、填充模式及编程实现

数字签名常用算法、填充模式及编程实现

消息认证机制的分类、常用算法及编程实现

常用的加密认证模式及编程实现

密钥的序列化和反序列化编程实现

常用密钥交换协议及编程实现。

数字证书的结构、作用，如何认证其合法性