- SM4
  - 算法核心操作
    - 异或操作
      - 异或运算原理
        - 二进制异或规则
        - 异或操作在SM4中的应用
    - 移位变换
      - 循环左移定义
        - 左移位数确定
        - 循环左移对字节的影响
      - 移位变换在SM4中的作用
    - 盒变换
      - 8bit输入输出映射
        - 固定变换表
        - 盒变换的安全性
      - 盒变换在加密解密中的应用
  - 算法模块划分
    - 密钥拓展模块
      - 密钥拓展流程
        - 初始密钥处理
        - 密钥拓展步骤
        - 拓展密钥存储
      - 密钥拓展对安全性的影响
    - 加/解密模块
      - 加密流程
        - 明文输入处理
        - 加密操作执行
        - 密文输出
      - 解密流程
        - 密文输入处理
        - 解密操作执行
        - 明文恢复
    - 模块间交互
      - 密钥拓展与加密模块的关联 —— 拓展密钥的使用
      - 加密与解密模块的相似性
        - 流程相似性
        - 操作相似性
  - 算法特点与优势
    - 高效性
      - 运算复杂度分析 —— 异或、移位、盒变换的运算效率
      - 加密解密速度对比
    - 安全性
      - 盒变换的固定性与安全性 —— 变换表设计的考量
      - 密钥拓展的安全性 —— 防止密钥泄露的措施
    - 灵活性
      - 支持多种密钥长度 —— 密钥长度的可配置性
      - 算法的可扩展性 —— 未来升级与优化的可能性