[toc]

课下测试

ch06

作业题目：商用密码应用安全性评估量化评估

1 学习视频 商用密码应用安全性评估量化评估规则

2 提交学习笔记（10分）

3 在应用和数据安全层面如何应用到实验4中（10分）

作业提交要求 (1')

0. 记录实践过程和 AI 问答过程，尽量不要截图，给出文本内容
1. (选做)推荐所有作业托管到 gitee或 github 上
2. (必做)提交作业 markdown文档，命名为"学号-姓名-作业题目.md"
3. (必做)提交作业 markdown文档转成的 PDF 文件，命名为"学号-姓名-作业题目.pdf"

- github链接

作业内容

- 通过浏览器扩展下载视频，通过WPS转文字稿。得到视频文字稿。观看视频修正文字稿内容。
- 使用AI总结视频内容(目前并无方便的在线的直接理解视频内容的AI，所以实际上是总结文字稿)

```
### 商用密码应用安全性评估量化评估视频文字稿总结

#### 一、概述
- **背景**：本次介绍旨在解释《量化评估规则》文件的内容及其在密码应用安全性评估中的作用。量化评估的核心在于对评估结果进行打分，从而提供一个客观的评价标准。
- **目的**：通过量化评估，确保密码应用的安全性达到一定的标准，同时鼓励使用合规的密码算法、技术和产品。

#### 二、设计初衷
- **密码学特点**：密码学强调高度的安全性，通常不包含普通安全中的量化指标或风险评估内容。
- **密钥安全**：密钥的安全性是评估的重点，任何密钥泄露风险将导致评估不通过。
- **系统安全**：密码应用的安全性受到多个因素的影响，从密钥管理到算法技术再到密码使用，每一环节的问题都会降低系统的安全性。
- **量化评估的目标**：将风险降低到可接受范围，让信息系统承建方或责任方能够看到系统的持续改进。

#### 三、量化评估的设计原则
- **遵循法律法规**：遵守相关的法律法规和标准指导性文件。
- **鼓励使用密码技术**：鼓励使用合规的密码算法、技术和产品。
- **优先应用领域**：优先在网络和通信安全以及数据安全领域应用密码技术。
```

四、量化评估的步骤与框架
1. **评估步骤**：
- 完成整体测评后，对每个测评项进行评分。
- 汇总每个测评项的得分，得到测评单元的得分。
- 汇总所有测评单元的得分，得到安全层面的得分。
- 最终汇总所有安全层面的得分，得到总体得分。
2. **评估框架**：
- **密钥管理安全**：评估密钥管理的全生命周期是否安全。
- **密码算法和技术安全**：评估算法和技术是否合规。
- **密码使用安全**：评估密码技术是否被正确有效地使用。

五、具体的量化评估指标
- **使用安全**：评估密码技术是否被正确有效使用。
- **算法技术合规**：评估算法和技术是否合规。
- **密钥管理安全**：评估密钥管理是否安全。
- **评分标准**：
- **1分**：使用认证合格的密码产品，且算法技术合规，密钥管理安全。
- **0.5分**：算法技术或密钥管理有不足，但产品认证合格；或产品未认证，但算法技术合规。
- **0.25分**：产品未认证且算法技术不合规。
- **0分**：密码使用不安全或算法技术、密钥管理均不符合要求。

六、管理方面的评估
- **管理评估**：管理方面的测评单元只有一分、0.5分或0分三个档次。
- **权重设置**：不同层面和指标有不同的权重，优先考虑网络层和应用层的安全性。
- **不适用情况**：不适用的指标不计入整体分值。

七、整体得分计算
- **权重分配**：
- 物理和环境安全：10分
- 网络和通信安全：15分
- 设备和计算安全：15分
- 应用和数据安全：30分
- 管理人员建设：8分
- 应急处置：6分
- **加权平均**：根据各层面的权重进行加权平均，得到最终得分。

八、最终结论
- **高风险判定**：评估过程中需结合高风险判定指引，高风险不影响最终得分，但需重点关注。
- **技术层面的评估**：技术层面的部分符合判定需谨慎，要求测评人员具备专业知识和严谨的证据。
- **鼓励使用认证产品**：鼓励使用通过认证的密码产品，确保密钥和产品的安全性。

九、未来展望
- **文件修订**：《量化评估规则》文件将根据实际应用情况进行适时修订，逐步提高评估标准。
- **推动行业发展**：通过量化评估，推动密码应用的标准化和规范化，提升整体信息安全水平。

- 学习笔记

商用密码应用安全性评估量化评估学习笔记

一、概述
- **背景**：商用密码应用安全性评估量化评估的主要目的是通过对评估结果进行打分，提供一个客观的评价标准，确保密码应用的安全性。这不仅有助于提升系统的整体安全性，还能促使企业和组织采用更合规的密码技术和产品。
- **目的**：量化评估旨在将密码应用的安全性量化，帮助信息系统承建方或责任方看到系统的持续改进，确保风险降低到可接受的范围内。

二、设计初衷
- **密码学特点**：
- 密码学强调高度的安全性，通常不包含普通安全中的量化指标或风险评估内容。
- 例如，传统密码学中，密钥长度和算法复杂度是衡量安全性的关键指标。如2048位RSA密钥的安全强度约为2^112，而1024位RSA密钥的安全强度仅为2^80。
- **密钥安全**：
- 密钥的安全性是评估的重点，任何密钥泄露风险将导致评估不通过。
- 例如，如果在密钥生成、存储、传输或销毁的任何一个环节出现问题，都将被视为重大安全隐患。
- **系统安全**：
- 密码应用的安全性受到多个因素的影响，从密钥管理到算法技术再到密码使用，每一环节的问题都会降低系统的安全性。
- 例如，即使密钥管理得当，但如果算法选择不当或使用方式错误，仍可能导致系统安全漏洞。

三、量化评估的设计原则
- **遵循法律法规**：
- 遵守相关的法律法规和标准指导性文件，确保评估的合法性和规范性。
- **鼓励使用密码技术**：
- 鼓励使用合规的密码算法、技术和产品，提升系统的整体安全性。
- 例如，使用国家密码管理局认证的SM2、SM3、SM4等算法。
- **优先应用领域**：
- 优先在网络和通信安全以及数据安全领域应用密码技术，因为这些领域的密码应用较为成熟。
- 例如，在网络通信中使用TLS协议进行数据加密，确保数据传输的安全性。

四、量化评估的步骤与框架
1. **评估步骤**：
- 完成整体测评后，对每个测评项进行评分。
- 汇总每个测评项的得分，得到测评单元的得分。
- 汇总所有测评单元的得分，得到安全层面的得分。
- 最终汇总所有安全层面的得分，得到总体得分。
2. **评估框架**：
- **密钥管理安全**：评估密钥管理的全生命周期是否安全。
  - 例如，检查密钥的生成、存储、传输、使用和销毁是否符合安全标准。
- **密码算法和技术安全**：评估算法和技术是否合规。
  - 例如，检查使用的密码算法是否经过国家密码管理局认证。
- **密码使用安全**：评估密码技术是否被正确有效地使用。
  - 例如，检查密码技术在实际应用中的配置和使用是否正确。

五、具体的量化评估指标
- **使用安全**：
- 评估密码技术是否被正确有效使用。
- 例如，检查SSL/TLS协议的配置是否正确，证书是否有效。
- **算法技术合规**：
- 评估算法和技术是否合规。

- 例如，检查使用的加密算法是否符合国家标准。
- **密钥管理安全**：
- 评估密钥管理是否安全。
- 例如，检查密钥是否定期更换，存储是否安全。
- **评分标准**：
- **1分**：使用认证合格的密码产品，且算法技术合规，密钥管理安全。
  - 例如，使用通过国家密码管理局认证的硬件加密模块，且算法选择和密钥管理均符合标准。
- **0.5分**：算法技术或密钥管理有不足，但产品认证合格；或产品未认证，但算法技术合规。
  - 例如，使用认证合格的产品，但算法选择不完全符合标准。
- **0.25分**：产品未认证且算法技术不合规。
  - 例如，使用未经认证的产品，且算法选择存在明显问题。
- **0分**：密码使用不安全或算法技术、密钥管理均不符合要求。
  - 例如，使用了不安全的算法，且密钥管理存在严重漏洞。

六、管理方面的评估
- **管理评估**：
- 管理方面的测评单元只有一分、0.5分或0分三个档次。
- 例如，检查是否有完整的密码管理制度和操作流程。
- **权重设置**：
- 不同层面和指标有不同的权重，优先考虑网络层和应用层的安全性。
- **不适用情况**：
- 不适用的指标不计入整体分值。
- 例如，某些特定的系统可能不需要进行物理安全评估，这部分指标不计入总分。

七、整体得分计算
- **权重分配**：
- 物理和环境安全：10分
- 网络和通信安全：15分
- 设备和计算安全：15分
- 应用和数据安全：30分
- 管理人员建设：8分
- 应急处置：6分
- **加权平均**：
- 根据各层面的权重进行加权平均，得到最终得分。

八、最终结论
- **高风险判定**：
- 评估过程中需结合高风险判定指引，高风险不影响最终得分，但需重点关注。
- 例如，即使某些指标得分较高，但如果存在高风险问题，仍需进行详细分析和整改。
- **技术层面的评估**：
- 技术层面的部分符合判定需谨慎，要求测评人员具备专业知识和严谨的证据。
- 例如，评估一个未认证的产品是否实现了合规的算法，需要详细的测试和验证。
- **鼓励使用认证产品**：
- 鼓励使用通过认证的密码产品，确保密钥和产品的安全性。
- 例如，推荐使用国家密码管理局认证的硬件加密模块，以确保密钥的安全性。

九、未来展望
- **文件修订**：
- 《量化评估规则》文件将根据实际应用情况进行适时修订，逐步提高评估标准。
- 随着密码技术的发展，评估标准可能会变得更加严格。
- **推动行业发展**：
- 通过量化评估，推动密码应用的标准化和规范化，提升整体信息安全水平。

- 通过评估结果，帮助企业发现并解决潜在的安全问题，提高系统的安全性。

- 在应用和数据安全层面如何应用到实验4中
  - 在应用和数据安全层面，量化评估信息可以让系统承建方或责任方看到系统进步，看到系统改进的方向。
  - 对照量化评估的标准给自己的实验项目评分
    - 可以在每完成一个功能模块就找到量化评估标准中相关的指标进行评分，然后迭代改进项目
  - 下面是AI提供的一个参考示例

```
### 将量化评估应用于电子公文系统设计中的应用和数据安全层面

#### 一、背景
电子公文系统是政府机关和企事业单位常用的信息管理系统，用于处理和管理各类公文。为了确保电子公文系统的安全性，特别是在应用和数据安全层面，需要引入量化评估的方法，确保系统的安全性和合规性。

#### 二、量化评估在应用和数据安全层面的关键点
1. **数据传输安全**
2. **数据存储安全**
3. **身份认证和访问控制**
4. **审计和日志管理**
5. **密钥管理**

#### 三、具体应用

##### 1. 数据传输安全
- **评估指标**:
- 使用加密协议（如TLS/SSL）保护数据传输。
- 确保传输过程中数据的完整性和机密性。
- 定期更新和维护加密协议。
- **量化评分**:
- **1分**：使用最新版本的TLS/SSL协议，配置正确，无已知漏洞。
- **0.5分**：使用较旧版本的TLS/SSL协议，存在已知漏洞但已采取临时措施。
- **0分**：未使用加密协议，数据传输存在安全隐患。

##### 2. 数据存储安全
- **评估指标**:
- 使用加密技术保护存储的数据。
- 确保数据备份的安全性。
- 定期进行数据恢复测试。
- **量化评分**:
- **1分**：使用国家认证的加密算法（如SM4），数据备份安全，定期进行恢复测试。
- **0.5分**：使用非国家认证的加密算法，数据备份存在安全隐患。
- **0分**：未使用加密技术，数据存储存在安全隐患。

##### 3. 身份认证和访问控制
- **评估指标**:
- 实现多因素身份认证（如用户名密码+短信验证码）。
- 实施细粒度的访问控制策略。
```

- 定期审核和更新用户权限。
- **量化评分**：
- **1分**：实现多因素身份认证，访问控制策略完善，定期审核用户权限。
- **0.5分**：仅使用单一因素身份认证，访问控制策略存在漏洞。
- **0分**：未实现身份认证，访问控制策略缺失。

4. 审计和日志管理
- **评估指标**：
- 记录所有关键操作的日志。
- 定期审查日志，发现并处理异常行为。
- 保护日志文件的完整性和机密性。
- **量化评分**：
- **1分**：记录所有关键操作日志，定期审查，日志文件保护良好。
- **0.5分**：记录部分关键操作日志，审查不及时，日志文件保护存在隐患。
- **0分**：未记录关键操作日志，缺乏审查机制。

5. 密钥管理
- **评估指标**：
- 密钥的生成、存储、传输、使用和销毁符合安全标准。
- 定期更换密钥。
- 保护密钥的访问权限。
- **量化评分**：
- **1分**：密钥管理符合国家密码管理局标准，定期更换，访问权限严格控制。
- **0.5分**：密钥管理存在部分漏洞，更换不及时，访问权限控制不严。
- **0分**：密钥管理存在严重漏洞，未定期更换，访问权限失控。

四、评估示例

假设某电子公文系统正在进行应用和数据安全层面的量化评估，以下是一个具体的评估示例：

1. **数据传输安全**：
- **评估结果**：使用TLS 1.2协议，配置正确，无已知漏洞。
- **评分**：1分

2. **数据存储安全**：
- **评估结果**：使用SM4加密算法，数据备份安全，定期进行恢复测试。
- **评分**：1分

3. **身份认证和访问控制**：
- **评估结果**：实现用户名密码+短信验证码的多因素身份认证，访问控制策略完善，定期审核用户权限。
- **评分**：1分

4. **审计和日志管理**：
- **评估结果**：记录所有关键操作日志，定期审查，日志文件保护良好。
- **评分**：1分

5. **密钥管理**：
- **评估结果**：密钥管理符合国家密码管理局标准，定期更换，访问权限严格控制。
- **评分**：1分

6. **总分**：
- **应用和数据安全层面总分**：5分（满分5分）

五、结论
通过上述量化评估，可以全面评估电子公文系统在应用和数据安全层面的安全性。评估结果可以帮助系统管理员发现潜在的安全隐患，并采取相应的改进措施，提升系统的整体安全性。例如，如果某项评估得分为0.5分或0分，应立即采取措施进行整改，确保系统的安全性和合规性。