[toc]

课下测试

ch06

作业题目：信息系统密码应用高风险判定指引

1 学习视频《信息系统密码应用高风险判定指引》解读 https://www.bilibili.com/video/BV1q24y1W7j1

2 提交学习笔记（10分）

3 在应用与数据安全层面分析实验4哪些方面会存在高风险，你实验中如何规避。（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

完成过程

- 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。
- AI辅助
    - 使用AI总结文稿内容

> 该文档是关于信息系统密码应用高风险判定指引标准的介绍，主要内容包括标准的背景、目的、历程、思路、条款解读、应用等方面。
>
> ### 一、标准编制背景和目的
> 信息系统密码应用专业性强，密评机构对高风险问题判定差异大，影响测评结论准确性，因此出台该标准对风险评价环节进行规划，为密评人员提供参考尺度，促进密评工作标准化和规范化，同时也可供信息系统使用单位在建设时规避高风险问题。
>
> ### 二、编制历程和思路
> 1. **历程**：从去年3月下旬立项，经过多次专家审查会和反馈意见修改，最终形成发布稿。
> 2. **思路**：研究国家对密码的相关要求，关注密码发展技术，针对密码应用场景提出高风险判定规则，结合密评经验形成标准。
>
> ### 三、标准条款解读
> 1. **总体结构**：10个章节1个附录，包括安全问题和缓解措施两个重要定义，判例结构结合安全问题和缓解措施综合考虑风险评价。
> 2. **通用部分**：密码算法适用于所有信息系统，安全问题明确且任意一条满足即可判定为高风险，采用存在安全问题的算法、安全性未知的算法以及对重要数据保护不当等均

属于高风险问题，通用部分无缓解措施。
3. **密码产品和服务**：在网络和应用层面考虑产品检测认证要求，重点关注密钥管理。
4. **物理和环境安全**：以身份鉴别为例，适用范围为二级以上，安全问题设置指向通用要求，缓解措施尽量避免使用非密码技术。
5. **网络和通信安全**：以通信过程中数据机密性为例，安全问题第一条指向通用要求，网络和应用层面提产品认证证书要求，注意等效措施的条件。
6. **应用和数据安全**：增加数据重要数据存储完整性要求，鼓励使用密码技术实现完整性保护，缓解措施给出非密码技术弥补情况。
7. **密码应用管理**：针对新建系统制定密码应用方案，强调方案的重要性。
8. **密钥管理**：附录A针对密钥产生、分发、存储、使用等环节给出可能的安全隐患问题。

四、标准应用
1. **指标选取**：选取基本要求中的核心条款，其他条款需参考通用要求。
2. **实际测评**：对于未涵盖的安全问题，若分析确实会造成严重安全隐患，可作为高风险判定；同时要根据用户场景进行合理判断。
3. **应用时机**：主要在整体测评期间和风险分析期间使用，整体测评时需考虑标准中的弥补措施，风险分析时根据标准判定问题是否为高风险。

- 自己观看视频和阅读文稿后的补充：
  - 应用与数据安全层面包括：数据存储完整性、数据机密性保护、密钥管理、密码应用方案四个方面
  - 高风险问题总结：
    - **采用存在安全问题的密码算法**：如MD5、DES等，以及IC不足2048位（如IC1024位）的情况。
    - **采用安全性未知的算法**：包括自行设计且未经检测认证的算法，以及密码产品中未经安全性认证的密码算法。
    - **对重要数据保护不当**：未对重要数据进行有效保护，或者使用不安全的算法对重要数据进行处理。
    - **密钥产生不合规**：未通过认证的设备产生密钥，可能导致密钥的随机性不足。
    - **密钥分发不安全**：如使用普通U盘分发密钥且不加密，明文传输密钥等情况。
    - **新建系统缺乏密码应用方案或方案未经评审**：可能导致系统建设完成后存在各种密码应用问题。
  - 如何选取信息系统密码应用高风险判定指引标准的指标：
    - 核心条款：选取基本要求中的核心条款作为高风险判定的指标。这些核心条款是对信息系统密码应用的关键要求，必须严格遵守，若不符合则视为高风险。
    - 通用要求：对于其他条款，尤其是技术条款，要参考高风险判定指引的第五章通用要求。在核查时，不能触碰通用要求中所涉及的问题，否则可能被判定为高风险。
    - 实际情况判断：考虑到密码应用场景的复杂性，标准无法涵盖所有安全问题。在实际测评中，如果发现的安全问题经分析确实会造成严重安全隐患，即使未在标准中明确列出，也可作为高风险来判定。但同时要注意，对于一些在标准中列出但在特定用户场景下威胁不存在或概率极小的情况，需要进行合理判断，避免误判为高风险。

- 学习笔记

信息系统密码应用高风险判定指引标准学习笔记

一、标准编制背景与目的
信息系统密码应用专业性强，不同密评机构对高风险问题判定差异大，影响测评结论准确性。为解决此问题，该标准应运而生，旨在规范和指导密码应用高风险判定，为密评人员提供参考尺度，促进密评工作标准化和规范化，同时帮助信息系统使用单位在建设时规避高风险问题。

二、编制历程与思路
1. **历程**：2023年3月下旬立项，历经5月、7月、8月三次专家审查会，10月根据反馈意见修改形成发布稿。
2. **思路**：研究国家对密码相关的发展和管理要求，关注密码发展技术，针对密码应用场景提出高风险判定规则，结合密评经验形成标准。

三、标准条款解读
1. **总体结构**：包含10个章节和1个附录，其中安全问题和缓解措施是两个重要定义。判例结构结合安全问题和缓解措施综合考虑风险评价。
2. **通用部分**：密码算法适用于所有信息系统，安全问题明确且任意一条满足即可判定为高风险。如采用存在安全问题的算法（如MD5、DES等）、安全性未知的算法（自行设计且未经检测认证或密码产品中未经安全性认证的算法）、对重要数据保护不当等情况。通用部分无缓解措施。
3. **密码产品和服务**：在网络和应用层面考虑产品检测认证要求，重点关注密钥管理。
4. **物理和环境安全**：以身份鉴别为例，适用范围为二级以上。安全问题设置指向通用要求，缓解措施尽量避免使用非密码技术。
5. **网络和通信安全**：以通信过程中数据机密性为例，安全问题第一条指向通用要求，网络和应用层面提产品认证证书要求，注意等效措施的条件。
6. **应用和数据安全**：增加数据重要数据存储完整性要求，鼓励使用密码技术实现完整性保护，缓解措施给出非密码技术弥补情况。
7. **密码应用管理**：针对新建系统制定密码应用方案，强调方案的重要性。
8. **密钥管理**：附录A针对密钥产生、分发、存储、使用等环节给出可能的安全隐患问题。

四、标准应用
1. **指标选取**：选取基本要求中的核心条款作为高风险判定指标，其他条款需参考通用要求。
2. **实际测评**：对于标准未涵盖的安全问题，若经分析会造成严重安全隐患，可作为高风险判定。同时，要根据用户场景进行合理判断，避免误判。
3. **应用时机**：主要在整体测评期间和风险分析期间使用。整体测评时需考虑标准中的弥补措施，风险分析时根据标准判定问题是否为高风险。

五、应用与数据安全层面要点
包括数据存储完整性、数据机密性保护、密钥管理、密码应用方案四个方面。

六、高风险问题总结
1. **算法方面**：采用存在安全问题或安全性未知的算法。
2. **数据保护方面**：对重要数据保护不当。
3. **密钥管理方面**：密钥产生不合规、分发不安全。
4. **方案方面**：新建系统缺乏密码应用方案或方案未经评审。

在应用与数据安全层面，实验4可能存在以下高风险及相应规避措施：

高风险方面：

1. **数据存储安全**：重要数据若未进行加密存储或采用不安全的加密算法，可能导致数据泄露风险。例如，实验中对电子公文等重要数据的存储，如果没有遵循相关密码应用要求，使用如MD5等存在安全问题的算法，数据易被窃取或篡改。

2. **数据传输安全**：在公文发送等数据传输过程中，若未采用安全的通信协议或加密方式保障数据机密性，可能被拦截窃听。比如，未使用符合标准的加密算法对传输中的公文进行加密保护，数据在网络传输时存在安全隐患。
3. **权限管理风险**：三员（系统管理员、安全保密管理员、安全审计员）权限设置不合理，可能出现越权操作。如权限分配不当，操作员可能获得审核员甚至更高权限，从而对数据进行非法操作。
4. **密钥管理风险**：私钥和对称算法密钥管理不善，如未妥善存储或传输，可能导致密钥泄露，进而危及数据安全。若密钥以明文形式存储或在不安全的网络环境中传输，很容易被攻击者获取。

规避措施：

1. **数据存储安全**：按照标准要求，对重要数据采用安全的加密算法（如SM4等）进行加密存储，确保数据的保密性和完整性。
2. **数据传输安全**：在数据传输过程中，使用安全的通信协议（如SSL/TLS等），并结合加密算法（如SM2、SM4等）对数据进行加密，防止数据被窃取或篡改。
3. **权限管理**：严格依据三员职责进行权限设置，确保各角色权限合理、相互制约。同时，建立权限变更审批流程，及时调整人员变动后的权限。
4. **密钥管理**：采用安全的密钥管理系统（如硬件安全模块）存储密钥，在传输过程中进行加密处理，并对密钥操作进行详细记录和审计，确保密钥的安全性。