**会议记录1**

**会议主题**: 信息加密系统需求性分析讨论

**会议时间**: 2024年12月22日

**参与人员**:

* 谢焕豪
* 许洛熙
* 彭锦锋
* 关超华
* 邓佳诚
* 李佳伦
* 展浩铭

**会议内容**:

1. **功能性需求讨论**
   * **加密算法支持**:
     + 确定支持的加密算法，包括Caesar、Transposition、Vigenere和RSA加密。
     + 讨论每种算法的实现要求和性能考量，确保系统能高效处理不同规模的文本数据。
   * **数据一致性**:
     + 强调加密解密验证的重要性，以及需要实现的错误检测和异常处理机制。
   * **多平台支持**:
     + 确保系统在主流操作系统上兼容运行，保持用户界面的一致性和性能优化。
2. **安全性需求讨论**
   * **算法安全性**:
     + 确保所用加密算法的强度，并讨论如何支持算法的更新与替换。
   * **密钥管理**:
     + 强调生成、存储和分发密钥的安全性，特别是RSA密钥的管理。
   * **数据传输安全**:
     + 讨论数据在传输过程中加密的必要性，以及实施身份验证机制。
   * **抗攻击能力**:
     + 确保系统设计能抵御各种攻击，包括暴力破解和侧信道攻击。
3. **性能需求讨论**
   * **加密和解密速度**:
     + 强调实时性能和大数据量处理的能力，确保系统快速响应用户请求。
   * **系统资源消耗**:
     + 讨论如何优化资源使用，确保在高负载下系统稳定运行。
   * **并发处理能力**:
     + 确保系统支持多用户同时操作，并具备负载均衡机制。
4. **用户体验需求讨论**
   * 强调系统界面的友好性与操作的简便性，确保用户能够轻松使用。
   * 讨论如何提供有效的错误信息反馈和帮助系统，提升用户体验。
5. **发展方向需求讨论**
   * 讨论系统应具备添加新加密方式的能力，并规避版权问题。
   * 提出需要开发服务器和管理员功能，以支持更广泛的应用场景，并考虑增加通信功能。
6. **测试和维护需求讨论**
   * 强调测试覆盖的重要性，包括功能性、安全性和性能测试。
   * 讨论系统的持续维护与更新策略，以确保系统的稳定性和可靠性。

**会议结论**:

* 形成一致意见，逐步推进信息加密系统的开发工作，确保各项需求在后续实施中得到落实。
* 确定各成员负责的具体任务，以便于后续的跟进和进展汇报。