要求：

以DES、AES、SM4或者祖冲之算法为数据加密算法；以RSA或者ElGamal算法为对称密钥传输的公钥加密算法；以数据认证算法MAC或SHA-256等Hash算法为消息认证算法；以DSA或者SM2算法为数字签字方法；选择适当的公钥管理方案和密钥协商方案，实现一套简单的保密通信系统。

设计一个简单的保密通信系统，并**模拟**一次该系统下的信息传输过程，发送消息的内容为：由学号、姓名、班级构成的字符串。系统配置从以下表格中选择。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 对称加密算法 | 对称密钥协商 | | | 消息认证算法 |
| 公钥加密算法 | 数字签名算法 | 公钥证书 |
| AES | RSA | RSA | 简单公钥证书系统 | HMAC |
| DES | ElGamal | DSA | openssl | CBC-MAC |
| SM4 | SM2 | SM2 |  | SHA256 |
| 祖冲之算法 |  |  |  |  |

需求分析的写作可以按照以下结构展开：

1. 引言：

- 对系统的简要介绍和背景说明。

- 提及设计目标和要求。

2. 功能需求：

- 列出系统所需实现的功能需求，包括算法选择和加密/解密操作。

- 对每个功能需求进行详细描述，包括输入、输出和操作步骤。

3. 数据需求：

- 定义系统中涉及的数据元素和数据格式。

- 描述消息内容的结构和要求。

- 讨论密钥的生成、存储和管理。

4. 安全性需求：

- 确定系统的安全性要求，包括机密性、完整性和真实性。

- 讨论如何保证密钥的安全性和防范攻击。

5. 性能需求：

- 讨论系统的性能要求，包括加密效率和认证效率。

- 定义性能指标和限制。

6. 其他需求：

- 讨论与系统相关的其他需求，如易用性、可扩展性、可维护性等。

7. 系统约束：

- 讨论可能对系统设计和实现产生影响的约束条件，如硬件、软件、网络环境等。

8. 附录：

- 提供相关支持材料，如系统流程图、数据结构定义等。

在需求分析的过程中，要确保清晰、具体、可衡量的需求，以便后续的系统设计和开发工作能够基于这些需求进行。同时，需求应该能够满足系统的目标和用户的期望，同时考虑到安全性和性能方面的要求。

1. 引言：

本文将要设计的是一套基于加密算法、公钥加密算法、消息认证算法、数字签名算法、公钥证书和密钥协商方案的简单保密通信系统。该系统旨在提供保密性、完整性和真实性保障，以保护用户传输的敏感数据不受攻击者篡改或窃取。

2. 功能需求：

系统需要实现以下功能需求：

1. 使用AES、RSA、SM4或者祖冲之算法作为对称加密算法，对消息内容进行加密和解密操作。

2. 使用RSA或者ElGamal算法作为公钥加密算法，进行对称密钥协商。

3. 使用MAC或SHA-256等Hash算法作为消息认证算法，验证消息的真实性。

4. 使用DSA或者SM2算法作为数字签名算法，对消息进行数字签名。

5. 使用适当的公钥管理方案和密钥协商方案，保证密钥的安全性。

6. 提供简单的公钥证书系统，以验证对方公钥的真实性。

具体的操作流程为：

- 生成公钥和私钥，并将公钥传给通信对方；

- 通信对方使用公钥加密消息并发送给本方；

- 本方使用私钥解密消息，同时使用MAC或者Hash算法验证消息的真实性；

- 本方对消息进行签名并传回给通信对方；

- 通信对方使用本方的公钥对签名进行验证并使用本地私钥解密收到的消息。

3. 数据需求：

在本系统中，消息内容由学号、姓名、班级构成的字符串组成。对称加密算法和公钥加密算法所需的密钥将采用随机生成的方式进行。对称加密算法和消息认证算法所使用的密钥需要保存在本地，而公钥最好通过公钥证书的方式进行验证。用户的公钥和私钥需要保存在本地，并需要采取相应的措施保证其安全性。

4. 安全性需求：

本系统需要满足机密性、完整性和真实性需求。对称加密算法和公钥加密算法的密钥需要保证其随机性和唯一性，以防止攻击者进行字典攻击或重放攻击。消息认证算法需要使用MAC或Hash算法进行认证，以防止攻击者对消息进行篡改。数字签名算法要求使用DSA或SM2算法，并确保签名的唯一性和正确性。公钥证书系统需要对公钥进行验证，以防止中间人攻击或伪造证书带来的安全风险。

5. 性能需求：

本系统需要满足高效、低延迟的需求。对称加密算法和消息认证算法所需的密钥需要在本地保存，以提高加解密的效率。同时，需要对算法进行优化，选择适当的算法和参数，以提高加解密和数字签名的速度。

6. 其他需求：

本系统需要满足易用性、可扩展性、可维护性等需求，采用友好的用户界面，以方便用户进行操作。同时，系统应该便于扩展和维护，以适应未来的需求变化。

7. 系统约束：

本系统需要满足硬件、软件、网络等方面的约束条件。硬件方面需要满足加解密算法的计算资源要求，软件方面需要满足库文件的支持和兼容性，网络方面需要满足通信的可靠性和稳定性。

8. 附录：

本文档提供了详细的技术支持，包括系统流程图、数据结构定义等，以帮助用户更好地理解系统的实现。同时，提供了代码实现和操作说明，以方便用户进行测试和运行。