**实验内容**

Part 1：

每个人的电子病历，都是一个文件（可以是数据库文件，也可以是二进制文件），存储在一个U盘中。

这个电子病历文件，必须是加密的，只有拥有人（病人）解密，才能查看和增加。

电子病历文件中，包含个人的基本信息（身份证号、姓名、性别、出生年月、药物过敏情况、血型），还包含了**每次**看病医生输入的信息，如

病人姓名：

病情：

诊断：

处理（处方和医嘱等）：

日期：

此外，医生要对所输入信息，做数字签名，附加于后。

Part 2：

但还存在一个问题，请大家思考：

看病时，往往是医生操作计算机，大多数情况下，病人基于对医生的信任，都会直接把密码告诉给医生，让医生代为输入。

这就造成一个安全漏洞。医生掌握了病人的密码，一旦出现医疗事故，比如处方有误等，医生在得到电子病历文件的情况下，是可以重新修改处方和重新签名的。这一方面阻碍了日后电子病历的网络化；另一方面使得本安全体系失去意义，电子病历的安全弱化为依赖U盘的物理安全。

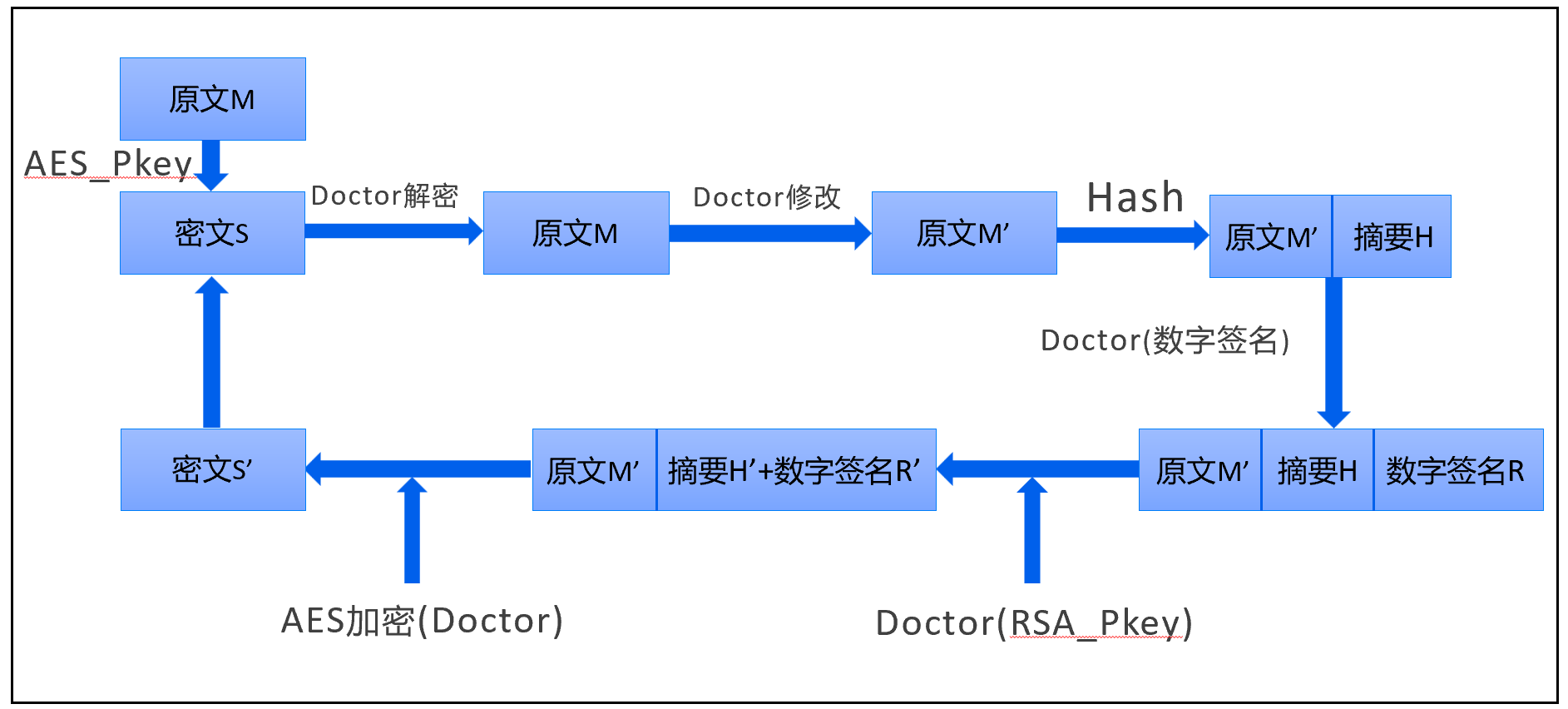
请大家开动脑筋，再补充完善本安全机制，以填上这个漏洞。

**实验工具**

**算法实现工具：python**

**辅助工具：visio**

**主要算法描述**

**在我们设计的电子病历系统中，患者的原始电子病历数据首先通过对称加密算法（如AES）进行加密，使用患者专属的密钥（Patient(AES)）生成密文。医生接收到密文后，使用患者的密钥（Patient(AES)）对密文进行解密，以获取原始的电子病历数据。医生在对电子病历进行修改后，利用哈希算法（Hash Algorithm）对修改后的原文生成一个数据摘要（Digest），以确保数据的完整性和一致性。为了验证修改者的身份并确保数据的不可否认性，医生需要在数据摘要后附加自己的数字签名。这通常通过医生的私钥（Doctor(RSA\_PrivKey)）对数据摘要进行加密来实现。医生使用患者的公钥（Doctor(RSA\_PKey)）对数字摘要和数字签名进行加密，由于医生不知道患者的私钥，故使用患者公钥进行加密后无法解密，达到无法修改的目的。最后，医生将修改后的原文、数据摘要和数字签名封装在一起，再次使用先前使用的对称加密算法（如DES）对整个信息包进行加密，生成最终的密文。患者接收到加密后的密文，可以安全地将其传输给下一次就诊的医生，确保在传输过程中数据的机密性和完整性。**

**这样的加密算法是如何解决诸多电子病历的安全问题呢？首先，患者的原始电子病历数据首先使用对称加密算法进行加密，加密使用的是患者专属的密钥（Patient(AES)）。这样，只有拥有相应解密密钥的人才能阅读病历内容，确保了数据的机密性。医生接收到密文后，使用相应的解密密钥（Doctor(AES\_Key)）对密文进行解密，获取原始的电子病历数据。医生在对电子病历进行修改后，利用哈希算法对修改后的原文生成一个数据摘要（Digest）。这个摘要是原文的固定长度的指纹，任何对原文的微小改动都会导致摘要发生显著变化，从而确保数据的完整性和一致性。为了验证修改者的身份并确保数据的不可否认性，医生需要在数据摘要后附加自己的数字签名。这通常是通过医生的私钥（Doctor(RSA\_PrivKey)）对数据摘要进行加密来实现的。数字签名确保了只有医生本人才能生成这个签名，其他人无法伪造。医生使用患者的公钥（Doctor(RSA\_PubKey)）对数字摘要和数字签名进行加密，由于医生不知道患者的私钥，故使用患者公钥进行加密后无法解密，达到无法修改的目的。最后，医生将修改后的原文、数据摘要和数字签名封装在一起，再次使用对称加密算法和医生的密钥（Doctor(AES)）对整个信息包进行加密，生成最终的密文。这样，即使在传输过程中，数据的机密性和完整性也得到了保障。**

**由于每次修改都会生成一个新的数据摘要，并且医生的数字签名与之关联，任何未经授权的修改都会被检测出来，因为修改会导致数据摘要变化，而没有相应私钥的人无法生成匹配的新签名。又因为每次修改后的数据都通过医生的私钥进行了数字签名，下一个医生即使能够解密查看病历内容，也无法伪造前一个医生的签名，因此无法否认前一个医生的修改记录。每个医生的修改都会生成新的数据摘要和数字签名，确保了病历的连续性和责任追溯。**

**我们通过采用了数字签名与摘要相结合的加密方式来增强安全性。即使医生掌握了病人的密码，也无法在没有患者RSA私钥的情况下篡改电子病历内容，因为任何篡改都会导致摘要值不匹配，从而被病人或审计系统检测到。同时，数字证书确保了公钥的真实性，防止了中间人攻击。这样，我们就能有效解决提到的安全漏洞，增强电子病历的安全性。**

**实验体会**

**黄静坡：**

通过这次实践，我深刻体会到了算法在软件安全中的重要性。设计一个既高效又安全的算法，不仅需要扎实的理论基础，还需要对实际应用场景有深刻的理解。在设计过程中，我不断与团队成员沟通，确保算法的可行性和实用性。同时，我也学习到了如何将复杂的技术内容以简洁明了的方式呈现在PPT中，这对于提高团队的工作效率和对外展示项目成果都至关重要。这次实验不仅提升了我的技术能力，也锻炼了我的沟通和表达能力。

**杨猛：**

作为负责算法实现和软件开发的一员，我在这次实验中深刻感受到了将理论转化为实践的挑战。我需要将黄静坡设计的算法转化为实际的代码，并确保软件的稳定性和安全性。在这个过程中，我学习到了如何优化代码，提高软件的性能，并且确保软件能够抵御潜在的安全威胁。我也意识到了团队合作的重要性，与何奕逊在软件测试方面的紧密合作，帮助我及时发现并修复了多个潜在的漏洞。这次实验不仅让我的技术能力得到了提升，也让我更加理解了软件开发的复杂性和安全性的重要性。

**何奕逊：**

通过这次实验，我深刻认识到了软件测试在整个软件开发过程中的关键作用。我需要确保软件的每一个功能都能正常工作，并且没有安全漏洞。这不仅需要我具备细致的观察力，还需要我能够理解软件的工作原理和潜在的风险点。在测试过程中，我与杨猛紧密合作，及时反馈测试结果，帮助他优化软件。同时，我也学习到了如何撰写清晰、准确的实验报告，这对于记录实验过程和总结实验成果非常重要。这次实验让我更加明白了软件测试的重要性，并且提升了我的分析和写作能力。

**总结：**

这次实验是一次宝贵的学习经历，它不仅让我们在技术上有所成长，也让我们在团队合作和沟通方面获得了宝贵的经验。我们相信，通过这次实验，我们能够将所学应用到未来的工作中，为电子病历安全领域做出更多的贡献。