第 5 章实验报告

|  |  |  |
| --- | --- | --- |
| 学号：1120223455 | 姓名： 杜恩俊 | 班级： 12012202 |
| 实验题目：基于Paillier 算法的匿名电子投票流程实现 | | |
| 实验日期：2024年3月26日 | | |
| 实验目的：  1.编写Paillier算法（密钥生成、加密和解密算法）并验证其加法同态性质  2.模拟实现基于Paillier 算法的匿名电子投票流程，了解该算法的应用，加深对同态加密算法的认识 | | |
| 硬件环境：  磁盘驱动器：NVMe KIOXIA- EXCERIA G2 SSD  NVMe Micron 3400 MTFDKBA1TOTFH  显示器：NVIDIA GeForce RTX 3070 Ti Laptop GPU  系统型号 ROG Strix G533ZW\_G533ZW  系统类型 基于 x64 的电脑  处理器 12th Gen Intel(R) Core(TM) i9-12900H，2500 Mhz，14 个内核，20 个逻辑处理器  BIOS 版本/日期 American Megatrends International, LLC. G533ZW.324, 2023/2/21  BIOS 模式 UEFI  主板产品 G533ZW  操作系统名称 Microsoft Windows 11 家庭中文版 | | |
| 软件环境： PyCharm 2023.2 专业版  python 3.11  无另外pip的第三方库 | | |
| 实验步骤与分析：  一：首先理解实验原理   * 1. 在密钥生成阶段，我们选择两个大素数p 和 q，这两个素数的选择要足够随机且相互独立。然后计算N=pq 和 λ=lcm(p−1,q−1)，其中lcm 是最小公倍数函数。这些值构成了公钥和私钥的一部分。   2. 我们还需要选择一个随机数 g，确保 g 与 N²互素。这样做的目的是为了确保在加密和解密过程中存在一个特定的模逆 μ，使得解密过程能够正确地还原明文。   3. 加密过程涉及将明文 m 加密为密文 c。为了确保加密的安全性，我们首先选择一个随机数 r∈ZN​，然后应用加密公式，将明文映射到密文空间中。   4. 解密过程是加密过程的逆过程，即从密文中还原出原始的明文。在解密过程中，我们首先将密文的 λ 次幂取模 N²，然后将其乘以预先计算的模逆 μ，最后将结果取模 N，得到原始的明文。   二：安全性分析  Paillier加密算法的安全性基于两个数论难题：大素数分解问题和离散对数问题。攻击者需要能够分解 N 为其素因子 p 和 q，以获得 λ 的值。但是，由于 N 是两个大素数的乘积，目前尚未找到高效的算法来解决这个问题。离散对数问题：攻击者需要能够从 gm 中还原出 m，即求解离散对数问题。但是，由于 g 是随机选择的，没有已知的有效算法可以在合理的时间内解决这个问题。因此，Paillier加密算法被认为是安全的，并且在广泛的应用场景中得到了验证。 三：代码编写  首先我们尝试编写Paillier.py：  首先我们编写keygen函数，用于生成密钥。我采用Miller-Rabin素性检测来检验，根据计算得知，运行k次后判断一个数是素数的正确率大于(1-1/2^k),经验证，当k=14时，判断的准确率大于99.99%。根据公式来计算p，q，λ，μ和N。然后根据公司和得到的私钥、公钥、明文来进行encrypt和decrypt函数的编写。然后编写main函数测试输入明文333和444后程序的输出结果。  然后我们编写ElectronicVoting.py  我将p和q的长度设置为1024比特，然后根据题目要求编写代码，引用了time库使得程序运行更流程，引用Paillier里的三个函数完成密钥生成、加密和解密的过程。  最终将两个代码进行测试，代码完美完成预计任务 | | |
| 结论与体会：  在本次实验中，通过编写和测试Paillier算法及其在匿名电子投票系统中的应用，我深刻理解了同态加密算法的原理和实际应用价值。通过实践，我掌握了Paillier算法的核心机制，包括密钥生成、加密、解密过程以及如何利用算法的加法同态性质。  首先，在密钥生成阶段，我学习到了选择合适的大素数p和q，以及如何计算N和λ，这些都是保证加密算法安全性的基础。选择随机数g的过程也让我认识到了在加密算法中引入随机性的重要性，这有助于提高算法的安全性。在编写加密和解密函数时，我通过实践深入理解了Paillier算法的数学原理，以及如何将理论应用到实际编程中。  通过将Paillier算法应用于模拟的匿名电子投票系统中，我体会到了同态加密算法在保护隐私信息方面的巨大潜力。在这个系统中，选民的投票选择得到了加密保护，同时还能够在不解密的情况下进行票数统计，这充分展示了Paillier算法加法同态性质的强大用途。  此外，我还学习到了算法的安全性分析，包括大素数分解问题和离散对数问题，这些都是算法安全性的理论基础。通过对这些数论难题的了解，我认识到了为什么Paillier算法被认为是安全的，并且可以在实际应用中提供强有力的数据保护。  总的来说，这次实验不仅让我对同态加密算法有了深入的了解，而且还让我体会到了将理论知识应用到实践中的重要性。我意识到，理论和实践相结合是理解和掌握复杂概念的关键。通过这次实验，我对加密算法的原理、实现以及在现实世界中的应用有了更加全面的认识，这将对我的未来学习和研究产生积极影响。 | | |
|  | | |