信息安全数学基础探究报告

张昌源　　2313177

一、探究目的

1、巩固已学习的信息安全数学基础知识。

2、加深对信息安全数学基础知识在实际应用层面的了解。

3、拓展对信息安全领域的认知。

二、探究题目

1、RSA 问题

2、二次剩余

3、同态加密算法

三、探究内容

1、RSA 问题

①包含的数学问题

1）大整数分解

RSA 涉及大整数分解问题。给定两个大质数 p 和 q，计算它们的乘积 n=p×q 很容易，但从 n 反推 p 和 q 很困难。例如，对于 n=1009×1013=1022117，若仅知道 n，要找出和这两个质数因子 1009 和 1013，是相当困难的，随着的位数增加，分解复杂度呈指数级增长。

2）欧拉函数

计算 $\phi(n)=(p-1)\times(q-1)$，这里运用了欧拉函数的性质。

3）同余理论

在加密和解密过程中，基于同余定理，如加密时 $c=m^e \pmod n$，解密时 $m=c^d \pmod n$，其中 m 为明文，c 为密文，e 为公钥指数，d 为私钥指数，且 $ed\equiv 1 \pmod{\phi(n)}$，通过同余运算实现了信息的加密变换与还原。

②算法思想

1）生成密钥

选择两个大质数 p 和 q，计算它们的乘积 $n=p\times q$。

计算欧拉函数 $\phi(n)=(p-1)\times(q-1)$。

选择一个整数 e，使得 $1<e<\phi(n)$ 且 $\gcd(e,\phi(n))=1$。

计算 d，使得 $d\times e\equiv 1 \pmod{\phi(n)}$。

(e,n)是公钥，(d,n)是私钥。

2）加密

将明文 m（m<n）加密成密文 c，加密算法为 $c=m^e \pmod n$。

3）解密

将密文 c 解密为明文 m，解密算法为 $m=c^d \pmod n$。

③算法特点

1）用数学难题实现安全

RSA 的安全性主要基于大整数分解问题。将一个巨大的合数 n 分解为两个大质数是及其耗时的，从而维护了安全。

2）公钥和私钥不同

公钥用于加密，私钥用于解密，使得它在很多应用场景中非常方便。比如在网络通信中，服务器可以公开公钥，客户端使用公钥加密信息发送给服务器，只有服务器用私钥才能解密，

保证了信息不被泄露。

3）可数字签名

RSA 还可以用于数字签名。发送方用自己的私钥对消息进行签名，接收方用发送方的公钥来验证签名的有效性。

④在密码学中的应用

1）网络通信安全

在互联网通信中，如 SSL/TLS 协议就大量使用 RSA 算法。当浏览器连接到一个安全网站时，网站会发送其公钥给浏览器，浏览器用这个公钥加密数据发送给网站，网站再用私钥解密。

2）电子邮件安全

在 PGP（Pretty Good Privacy）和 S/MIME（Secure/Multipurpose Internet Mail Extensions）等电子邮件加密和签名系统中，RSA 算法被用来加密邮件内容和验证发件人的身份。用户可以用收件人的公钥加密邮件发送，收件人用自己的私钥解密。

3）数字证书

数字证书用于验证网站或其他实体的身份。证书颁发机构（CA）使用自己的私钥对包含网站公钥等信息的数字证书进行签名，用户的浏览器等客户端可以用 CA 的公钥来验证证书的签名。

2、二次剩余

①包含的数学问题

1）二次剩余定义

对于给定的整数 p，如果存在整数 x 使得 $x^2 \equiv a \pmod p$成立，则称 a 是模 p 的二次剩余。如果没有这样的 x 存在，则 a 是模 p 的二次非剩余。

2）Euler 判别法

Euler 判别法提供了一个判断数是否为模 p 的二次剩余的方法。对于奇素数 p 和整数 a，如果 a 是模 p 的二次剩余，则 $a^{(p-1)/2} \equiv 1 \pmod p$；如果是二次非剩余，则 $a^{(p-1)/2} \equiv -1 \pmod p$。

3）勒让德符号和雅可比符号

勒让德符号是一个用于判断二次剩余的工具，定义为 (a/p)，其中 p 是奇素数，a 是不被 p 整除的整数。勒让德符号的值可以是 1 或 -1，分别表示 a 是模 p 二次剩余或二次非剩余。雅可比符号是勒让德符号的推广。对于任意奇正整数 n 和整数 a，如果 n 的素因数分解为 $n=p_1^{a1}p_2^{a2\cdots}p_k^{ak}$，那么雅可比符号定义为：$(a/n)=(a/p_1)^{a1}(a/p_2)^{a2\cdots}(a/p_k)^{ak}$。其中，$(a/p_i)$是勒让德符号。当 n 是奇素数时，雅可比符号就是勒让德符号。

②算法思想

以 Goldwasser-Micali 加密算法为例。

密钥生成：选择两个大质数 p 和 q，计算 $n=p\times q$。同时计算 y，使得 y 是模 n 的二次非剩余，并且雅可比符号$(y/p)=(y/q)=-1$。公钥是(n,y)，私钥是(p,q)。

加密过程:对于明文 $m=(m_1,m_2\cdots\cdots m_i)$，其中 $m_i=0$ 或 1。对于每个 m_i，当 $m_i=0$ 时，选择一个随机数 r_i，使得 r_i 与 n 互质，计算密文 $c_i=r_i^2 \pmod n$；当 $m_i=1$ 时，同样选择一个随机数 r_i，使得 r_i 与 n 互质，计算密文 $c_i=yr_i^2 \pmod n$。最终密文为 $c=(c_1,c_2\cdots\cdots c_i)$。

解密过程：对于收到的密文 $c=(c_1,c_2\cdots\cdots c_i)$，利用私钥(p,q)，计算勒让德符号$(c_i/p)$和$(c_i/q)$。如果$(c_i/p)=(c_i/q)=1$，则明文 $m_i=0$；如果$(c_i/p)=(c_i/q)=-1$，则明文 $m_i=1$。这样就可以逐位恢复出明文。

③算法特点

1）用数学难题实现安全

与 RSA 算法类似，其安全性主要基于大整数分解问题和二次剩余判定问题。大整数分解问题使得攻击者难以从公钥 n 得到私钥(p,q)，而二次剩余判定问题的困难性保证了即使攻击者获取了密文，在不知道私钥的情况下，也很难判断密文所隐藏的明文信息。

2）概率加密特性

对于相同的明文，由于加密过程中随机数的选择不同，会产生不同的密文。这种特性增加了密码分析的难度，因为攻击者不能通过简单地比较密文来获取明文信息，即使对同一明文进行多次加密，密文也会呈现出随机性。

3）计算复杂度不大

二次剩余算法的加密和解密过程涉及到一定的数论运算，如模幂运算、勒让德符号计算等。虽然这些运算在计算上有一定的复杂度，但相较于一些其他复杂的密码算法，其复杂度在计算机可接受范围之内。

④在密码学中的应用

1）公钥加密体制

二次剩余被用于构造一些公钥密码体制，如 ElGamal 加密算法。利用二次剩余的特性来设计更高效、更安全的公钥加密方案，在保护敏感信息传输方面发挥了重要作用。

2）数字签名

二次剩余也被应用于数字签名领域。通过利用二次剩余的数学性质，设计出能够保证签名的真实性、完整性和不可否认性的签名算法。发送方可以利用自己的私钥（与基于二次剩余的加密私钥相关）对消息进行签名，接收方利用发送方的公钥和二次剩余的判定方法来验证签名的有效性。

3）密钥交换协议

在一些密钥交换协议中，二次剩余可以作为一种辅助手段来增加密钥交换的安全性。例如，通过在密钥交换过程中引入二次剩余的相关计算和验证步骤，使得双方能够在不安全的通信信道上安全地协商出共享的密钥，同时防止攻击者窃取或篡改密钥信息，为后续的加密通信提供安全的基础。

3、同态加密算法

①密码原语

1）基本定义

同态加密是一种加密技术，它允许在加密数据上进行计算，而无需解密数据。换句话说，同态加密能够支持对加密数据进行“同态”操作——即在密文上进行计算操作，解密结果与直接对明文进行相同操作的结果相同。

2）具体内容

如果满足 f(A)+f(B)=f(A+B)f(A)+f(B)=f(A+B)，我们将这种加密函数叫做加法同态。

如果满足 f(A)×f(B)=f(A×B)f(A)×f(B)=f(A×B)，我们将这种加密函数叫做乘法同态。

全同态加密：种同态加密算法支持对密文进行任意形式的计算（即满足加法和乘法）。

半同态加密: 支持对密文进行部分形式的计算，例如仅支持加法、仅支持乘法或支持有限次加法和乘法。

以乘法同态、加法同态为例：

乘法同态加密，如：

RSA 加密

密钥生成：RSA 加密系统基于大整数分解问题。生成两个大质数 p 和 q，计算 $n = p \times q$，并选择公钥 e（通常为小的整数）和私钥d使得$e \times d \equiv 1\ (mod(p-1)(q-1))$

加密过程：给定消息 m，其加密过程是$c = m^e\ (mod\ n)$

解密过程：接收方使用私钥 d解密密文 c：$m = c^d(mod\ n)$

乘法同态：RSA 加密支持在密文上进行乘法操作。如果有两个密文 $c_1 = m_1^e\ (mod\ n)$ 和 $c_2 = m_2^e\ (mod\ n)$，那么其乘积$c_1 \times c_2\ (mod\ n)$ 就是 $(m_1 \times m_2)^e\ (mod\ n)$，即密文的乘积等于明文的乘积的加密结果。

加法同态加密，如：

Paillier 加密

密钥生成：

选择两个大质数 p 和 q，计算 $n = p \times q$和 $\lambda = lcm(p-1, q-1)$

随机选择一个生成元 $g \in Z_{n^2}^*$。

公钥为 (n, g)，私钥为 λ 。

加密过程：给定明文 m 和随机数 r，加密过程为：$c = g^m \times r^n(\ mod\ n^2)$其中，$c$是密文，$r$ 是随机数。

解密过程：接收方使用私钥 λ解密密文 c：$m = \frac{L(c^\lambda\ mod\ n^2)}{L(g^\lambda\ mod\ n^2)}\ (mod\ n)$其中，$L(x) = \frac{x-1}{n}$ 是一个辅助函数。

加法同态：Paillier 支持在密文上执行加法操作。即如果有两个密文 $c_1 = g^{m_1} \times r_1^n\ (mod\ n^2)$ 和 $c_2 = g^{m_2} \times r_2^n\ (mod\ n^2)$，则它们的和是：$c_1 \times c_1\ (mod\ n^2) = g^{m_1+m_2} \times (r_1 \times r_2)^n\ (mod\ n^2)$这表示加密数据的乘积相当于明文的和的加密结果。

②应用场景

1）在云计算中的应用

在云计算过程中，数据的隐私性和安全性一直是一个重要的问题。因为数据是在云服务提供商的服务器上进行存储和处理，用户无法保证数据不会被服务提供商或其他未经授权的人员访问和窃取。同态加密技术可以实现数据的安全计算和处理，同时保护数据的隐私。例如，用户可以使用同态加密技术将敏感数据加密后存储在云端，然后进行安全计算，最终将结果解密得到。这样就可以避免云服务提供商访问用户数据的情况发生，保护了数据的隐私性。

2）在政府与公共部门的应用

在政府与公共部门，同态加密也有诸多用途。政府部门可以使用同态加密技术发布加密后的统计数据，第三方机构可以在不解密的情况下对这些数据进行分析，帮助制定政策或进行研究。例如，在人口统计、经济数据统计等方面，同态加密可以确保数据的安全性和隐私性。在选举投票中，通过同态加密技术，选民可以匿名投票，选举委员会可以在不解密选票的情况下统计投票结果，确保选举的公平性和透明度。

3）在人工智能领域的应用

在人工智能和机器学习中，训练和推理过程通常需要大量的敏感数据。通过同态加密，可以在加密数据上进行模型训练和预测，避免了数据泄露的风险。

③数学问题

1）离散对数问题

1.1 定义与背景

离散对数问题是在有限循环群的背景下提出的。设 G 是一个有限循环群，其阶为 n（即群中元素的个数），g 是 G 的一个生成元。对于给定的元素 h∈G，离散对数问题就是要找到一个整数 x（0≤x≤n-1），使得 g^x=h。在密码学应用中，通常考虑的是模素数 p 的乘法群 Zp*，即 G = Zp*，其中 p 是一个大素数。

1.2 计算困难性分析

当 p 较小时，通过简单的穷举法可以计算离散对数。例如，对于 Z_{17}*，若 g = 3，要计算 h = 12 的离散对数，可以依次计算 3^0,3^1,……,3^15 模 17 的值，直到找到等于 12 的结果，

发现 3^13≡12(mod17)，所以离散对数为 13。然而，当 p 是一个几百位甚至上千位的大素数时，穷举法的计算复杂度呈指数增长，在实际计算资源和时间限制下几乎不可行。目前，虽然有一些亚指数时间复杂度的算法，如指数积分法，但对于足够大的素数 p，离散对数问题仍然被认为是困难的。

1.3 在同态加密中的具体应用方式

在基于椭圆曲线的同态加密方案中，椭圆曲线群上的离散对数问题是保障安全性的关键。例如，加密操作可能是将明文 m 映射到椭圆曲线上的一个点 Pm，然后通过选择一个随机数 k（相当于离散对数问题中的 x）和椭圆曲线的基点 G，计算密文 C=(kG,Pm + kQ)，其中 Q 是与公钥相关的点。解密时则需要利用私钥（与离散对数 k 相关）来恢复出 Pm 进而得到明文 m。由于攻击者不知道私钥（即离散对数 k），在离散对数问题困难的假设下，难以从密文 C 中推导出明文 m。

2）整数分解问题

2.1 定义与背景

整数分解问题是数论中的经典难题。给定一个合数 n（即不是素数的整数），目标是找到它的非平凡因数，即除了 1 和 n 本身以外的因数。例如，对于 n = 15，可以很容易地分解为 3×5。但在密码学中，通常考虑的是非常大的合数，如 n = pq，其中 p 和 q 是两个大素数，且 p 和 q 的长度可能都在几百位甚至上千位。

2.2 计算困难性分析

目前，整数分解的经典算法包括试除法、Pollard's rho 算法、二次筛法和一般数域筛法等。试除法是最基本的方法，对于一个 n，从 2 开始依次尝试能否整除 n，但这种方法对于大整数 n 效率极低。Pollard's rho 算法在一定程度上改进了效率，但对于大规模的密码学应用中的大整数分解仍然不够。二次筛法和一般数域筛法是更先进的算法，它们的时间复杂度分别为亚指数时间 Ln[1/2,1]和 $Ln[1/3,(64/9)^{1/3}]$(其中 $Ln[a,b]=e^{(b(logn)^a(loglogn)^(1-a)))}$。尽管如此，当 n 足够大时，例如 n 是一个 2048 位的合数，即使使用一般数域筛法，分解所需的计算资源和时间也是巨大的，使得在实际中难以实现对这样大整数的分解。

2.3 在同态加密中的具体应用方式

在一些早期的同态加密方案或者与传统公钥密码学结合的混合方案中，整数分解问题起到重要作用。例如，在 RSA 加密算法基础上扩展的同态加密方案中，公钥 e 和私钥 d 与大整数 n = pq 相关联，加密过程可能涉及到对明文 m 进行幂运算 $m^e(mod\ n)$，解密则需要利用私钥 d 通过 $m^{ed}≡m(mod\ n)$ 恢复明文。由于攻击者难以分解 n 得到 p 和 q，进而难以计算出私钥 d（根据 ed≡1(mod(p-1)(q-1))），从而保证了加密的安全性。

四、探究收获

通过本次探究，掌握了 RSA、二次剩余和同态加密算法背后的数学原理，了解了它们在网络通信、数字签名等密码学领域的应用方式。但探究也有不足，部分复杂理论理解不够深入。