作业四

题目：Paillier 密码算法是 1999 年 paillier 发明的概率公钥加密算法，请认真学习 Paillier 密码算法并回答以下问题：

1. Paillier 密码算法的公私钥对如何生成的？其安全性依赖的数学问题是什么？

答:

密钥生成：

1) 随机选择两个大质数p和q满足$gcd(pq,(p-1)(q-1)) = 1$。要求选择的两个质数长度接近。
2) 计算$n = pq$和$\lambda = lcm(p-1,q-1)$
3) 定义$L(x) = \frac{x-1}{n}$
4) 选择生成元$g \in Z_{n^2}^*$，使得$\gcd\left(L(g^\lambda modn^2),n\right) = 1$
5) $\mu = L(g^\lambda modn^2)^{-1}modn$
6) 公钥为(n,g)
7) 私钥为(λ,μ)

例子:

1) 选择$p = 7, q = 11, gcd\left(pq,(p-1)(q-1)\right) = \gcd(77,60) = 1$
2) 计算$n = 7 \times 11 = 77, \lambda = lcm(p-1,q-1) = lcm(6,10) = 30$
3) 选择$g = 5652$，满足$\gcd\left(L(g^\lambda modn^2),n\right) = \gcd\left(\frac{(5652^{30}mod5929)-1}{77},77\right) = \gcd\left(\frac{3928-1}{77},77\right) = \gcd(51,77) = 1$
4) 计算$\mu = 51^{-1}mod77 = 74$
5) 公钥$(n,g) = (77,5652)$，私钥$(\lambda,\mu) = (30,74)$

困难问题：

Paillier 公钥加密基于大整数的素因子分解问题与n阶剩余类(复合剩余类)问题。

大整数的素因子分解问题：给定一个大整数$n = p * q$，其中p和q都是大素数，求出n的因子p和q在计算上是困难的。

n阶剩余类（复合剩余类）问题：假设$n = p * q$，其中p和q都是大素数，给定一个整数z，如果存在$y \in Z_{n^2}^*$，使得$z = y^n mod n^2$，那么称z为模n^2的n阶剩余类。判断z是否是模n^2的n阶剩余类是困难的。

2. 请描述 Paillier 算法的加密过程和解密过程。

答：

加密过程：

设m为明文，选择随机数$r \in Z_{n^2}^*$，满足$\gcd(r, n) = 1$，计算密文$c = g^m * r^n mod n^2$

例子 1：设$m = 42, r = 23, c \equiv 5652^{42} * 23^{77} mod 5929 \equiv 4019 * 606 mod 5929 \equiv 4624 mod 2929$

例子 2：设$m = 42, r = 13, c \equiv 5652^{42} * 13^{77} mod 5929 \equiv 4019 * 1371 mod 5929 \equiv 2008 mod 2929$

解密过程：

计算明文$m = L\left(c^\lambda mod n^2\right) * \mu mod n$

例子 1：$m \equiv L(4624^{30} mod 5929) * 74 mod 77 \equiv L(4852 mod 5929) * 74 mod 77 \equiv \frac{4852-1}{77} * 74 mod 77 \equiv 63 * 74 mod 77 \equiv 42 mod 77$

例子 2：$m \equiv L(2008^{30} mod 5929) * 74 mod 77 \equiv L(4852 mod 5929) * 74 mod 77 \equiv \frac{4852-1}{77} * 74 mod 77 \equiv 63 * 74 mod 77 \equiv 42 mod 77$

可以看出r的取值不同会导致密文不同，但并不影响解密的结果。

3.请分析 Paillier 算法的正确性。

答：

$\because (p-1)|\lambda, (q-1)|\lambda$

$\therefore \lambda = k_1(p-1) = k_2(q-1)$

由费马小定理(p是质数，g不是p的倍数，则$g^{(p-1)} \equiv 1 mod p$)可得$g^{\lambda} = g^{k_1(p-1)} \equiv 1 mod p$，$\left(g^{\lambda}-1\right)|p$

同理$g^{\lambda} = g^{k_2(q-1)} \equiv 1 mod q$，$\left(g^{\lambda}-1\right)|q$

$\therefore \left(g^{\lambda}-1\right)|pq$，$g^{\lambda} \equiv 1 mod n$

$\therefore g^{\lambda} mod n^2 \equiv 1 mod n$

即$g^{\lambda} mod n^2 = n * k_g + 1; k_g < n$

$\therefore L\left(g^{\lambda} mod n^2\right) = k_g$

而且有$1+kn \equiv 1+kn(mod n^2)$,

$(1+kn)^2 \equiv 1+2kn+(kn)^2 \equiv 1+2kn(mod n^2)$,

$(1+kn)^3 \equiv 1+3(kn)^2+3kn+(kn)^3 \equiv 1+3kn(mod n^2), \ldots$

可以观察出$(1+kn)^m \equiv kmn+1(mod n^2)$

$\therefore g^{m\lambda} = (1+k_g n)^m \equiv k_g mn+1(mod n^2)$,

$r^{n\lambda} = (1+k_r)^n \equiv k_r n^2+1(mod n^2) \equiv 1(mod n^2)$

有$L\left(c^{\lambda}(mod n^2)\right) = L\left(g^{m\lambda} r^{n\lambda}(mod n^2)\right) = L\left(k_g mn+1\right) = \frac{k_g mn+1-1}{n} = mk_g$

而且有$L\left(g^{\lambda} mod n^2\right) = k_g$

$\therefore L\left(c^{\lambda} mod n^2\right) * \mu mod n = \frac{L\left(c^{\lambda} mod n^2\right)}{L\left(g^{\lambda} mod n^2\right)} = \frac{mk_g}{k_g} \equiv m(mod n)$

4.与 RSA 算法相比，请简评 Paillier 算法。

答:

1) 与 RSA 算法类似，Paillier 算法的构造基于大整数的素因子分解问题，并且在此基础上，Paillier 算法还依赖n阶剩余类（复合剩余类）问题。从引入额外的困难问题假设的角度讲，Paillier 算法的安全性弱于 RSA 算法。

2) 支持的同态加密不同，RSA 支持乘法同态，Paillier 支持加法同态。

3) Paillier 的密文长度是 RSA 的两倍。

4) Paillier 加密需要进行两次幂运算，RSA 加密只需进行一次，RSA 加密效率更高。

5) Paillier 算法由于使用了随机数r，使用相同明文和公钥加密得到密文可能不同，而 RSA 算法中使用相同的明文和公钥加密得到的密文相同。

5. 什么是同态加密， Paillier 密码算法支持同态加密与 RSA 密码算法支持的同态加密有什么不同。

答:

同态加密：对经过加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与直接处理未加密的原始数据得到的输出结果是一样的。同态加密分为加法同态加密、乘法同态加密和全同态加密（同时满足加法和乘法同态）。

加法同态满足$D\left(E(m_1)\circ E(m_2)\right) = m_1+m_2$

乘法同态满足$D\left(E(m_1)\circ E(m_2)\right) = m_1 * m_2$

Paillier 密码支持加法同态，而 RSA 支持乘法同态

Paillier：

$$\begin{aligned} D\left(E(m_1) * E(m_2)\right) &= D(g^{m_1} * r^{n_1} * g^{m_2} * r^{n_2} mod n^2) \\ &= D(g^{m_1+m_2} * r^{n_1+n_2} mod n^2) = m_1+m_2 \end{aligned}$$

RSA:

$$D\left(E(m_1) * E(m_2)\right) = D({m_1}^e * {m_2}^e) = D((m_1 * m_2)^e) = m_1 * m_2$$