# 《密码学原理》作业 4 答案

1. 按照提示，使用中国剩余定理，我们只需要证明，对于所有的 x∈{0,1，…, N-1}，$(x^e)^d \equiv x \pmod p$ 并且 $(x^e)^d \equiv x \pmod q$。由 $ed \equiv 1 \pmod{\Phi(N)}$，我们有 $ed \equiv 1 \pmod{p-1}$。如果 p 不能整除 x，那么[x mod p] $\in Z_p^*$，因此 $(x^e)^d \equiv ([x \bmod p]^e)^d \equiv [x \bmod p] \equiv x \pmod p$。如果 p 能够整除 x，那么 $(x^e)^d \equiv 0 \equiv x \pmod p$。总之，对于所有的 x∈{0,1，…, N-1}，我们都有 $(x^e)^d \equiv x \pmod p$。类似地，也可以证明 $(x^e)^d \equiv x \pmod q$。

2. 按照提示，我们把求 half(x)的困难归约为求 lsb(x)的困难。与此相等价，我们只需要把求 lsb(x)归约为求 half(x)。假设我们有一个算法 A 能够具有一定概率求出 half(x)，那么我们构造一个具有同样概率求出 lsb(x)的算法 A’如下。A’首先计算 $y=[[x^e \bmod n]/2^e \bmod n]$。由于 $y=[(x/2)^e \bmod n]$，A’可以以 y 为输入去调用 A，求出 half(x/2)。然后，输出 half(x/2)即可。下面只须证明 half(x/2)=lsb(x)。当 half(x/2)=0 时，0<x/2<N/2，所以 0<x<N，亦即[x mod N] =x。考虑到 x/2 是一个整数，因此 x 必然是一个偶数，所以 lsb(x)=0。当 half(x/2)=1 时，N/2<x/2<N，所以 N<x<2N。虽然 x 仍然是一个偶数，但是[x mod N]=x-N 不再是一个偶数，反而是一个奇数。因此得到 lsb(x)=1。综合两种情况，总有 half(x/2)=lsb(x/2)。

3. 助教抽 1 名好学生，验证其加密、解密功能均正确后，再用他的程序来验证别人的程序（用他的加密功能验证别人的解密功能，用他的解密功能验证别人的加密功能）。

4.把题目中 scheme 的 security 归约到 ElGamal 的 security 上。我们先定义题目中 scheme 的 Game 如下：

Game1：challenger1 生成密钥，并把公钥发给 adversary A。A 随机选择两个明文$m_0$，$m_1$，并发给 challenger1；challenger1 随机选择一个比特 b，然后对$m_b$加密$\mathrm{E}(m_b) = (g^r, y^r m_b, g^s, g^s m_b)$，(r,s 是从 0,…,q-1 中独立随机选择的)并将其密文发给 A;A guess a bit $b'$.我们设 A 在这个 game 中的 advantage 是$\varepsilon$。

下面我们利用 A 构造一个 adversary B，攻击 ElGamal。

Game2：challenger2 生成 ElGamal 的密钥，并把其公钥发给 B。B 随机选择两个明文$\mu_0, \mu_1$，并发给 challenger2. Challenger2 随机选择一个比特 b，然后对$\mu_b$加密$\mathrm{E}(\mu_b) = (g^t, y^t \mu_b)$，t 是从 0,…,q-1 中随机选择的，然后 challenger2 把密文发给 B；B 开始 guess a bit，而 B 猜测的策略是：

B 模仿 Game1 里的 challenger1，把公钥发给 A（两个 scheme 的密钥算法是一样的）；A 随机选择两个明文$m_0$，$m_1$，并发给 B。此时 B 把$m_0$，$m_1$发给 challenger2，在向他 request a challenge ciphertext；challenger2 把密文$\mathrm{E}(m_b) = (g^u, y^u m_b)$发给 B，u 是从 0,…,q-1 中随机选择的。B 随机选择$\mathrm{v} \leftarrow \{0, \ldots, \mathrm{q}-1\}$，并把$(g^u, y^u m_b, g^{u+v}, g^{u+\mathrm{v}} m_b)$发给 A；A guess a bit $b'$. B 在 Game2 中给出猜测$b'$。

我们可以看出 B 在 Game2 的 advantage 等于 A 在 Game1 中的 advantage。而我们知道 ElGamal 是 CPA-secure 的，所以 B advantage 是 negl. 故 A 在 Game1 中的 advantage 也是 negl。

注：B 在 Game2 中向 challenger2 request two challenge ciphertexts；而我们知道 CPA-secure for multiple encryptions 等价于 CPA-secure 的。