# 6.17

(a) ;

(b)

(c) TILE

# 6.21

(a) 证明： ∵ a是模p的一个二次剩余

∴

又∵ 的平方根

∴ 有

(b) 证明：

(c) 证明： ∵ 是素数时有

∴

∴

(d)证明： 基于以上论述可知，模p的平方根是可以计算的。而且，因为 是素数时，对于所有的，有。所以 是可以有效计算的。

# 6.22

(a)证明：设密码体制下，有明文，是其中一个对应的密文，公钥为和。

令 ;

利用判断是否有:

;

必有一使得上式成立，其对应的即为密文对应的明文。

∴ 为可以被用作区分两个给定明文和的加密算法的一个子程序

(b)证明：设如DDH中的假设给定。定义和是密码体制的公钥，定义，令为随机取定。

令;

利用判断是否有：

;

必有一使上式成立，其对应的即为满足DDH中

的;

∴可以用作求解中 算法的一个子程序。