Homework 6

Sun Kai

5110309061

1. (a)The encoding algorithm E

   (b)Let m be the message. Then just send E(m)

   (c)发送消息的一方拥有另一套密码，设其中加密算法为 E_1，解密算法为 D_1，则将 E_1 公布。设要发的消息为 m，签名为 s，则发的消息为 $E(D_1(m), s)$。

2. 假设接受方的解密算法为 D（私有），提供的加密算法为 E（公开），发送方的解密算法为 D_1（私有），提供的加密算法为 E_1（公开），发送方签名为 s，消息为 m，则发的消息为 $E(D_1(m), s)$。

   （请问，第 1 题的(c)与第 2 题有什么区别?）