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E1，解密算法为D1，则将E1公布。设要发的消息为m，签名为s，则发的消息为E(D1(m), s)。

1. 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D1（私有），提供的加密算法为E1（公开），发送方签名为s，消息为m，则发的消息为E(D1(m), s)。

（请问，第1题的(c)与第2题有什么区别?）