2.1 有缺陷，窃听者只要截获从我这发出的一条信息以及从伙伴那发出的一条信息，两者异或的结果就是密钥

2.3 a. $P = (C \oplus -K_1) \oplus K_0$ ，$-K_1$为K_1的逆元

b. $C - C' = P \oplus K_0 - P' \oplus K_0$

无法得出K_0的唯一解

2.5. a. DS和MAC都能检测出来，DS中计算出的散列值不同，MAC中计算出的认证码不同

b. 两者都防御不了，因为散列值和认证码未发生改变

c. DS可以防御，只要用Oscar和Alice两人的公钥分别解密看哪个正确就说明是谁发的

MAC想要防御必须知道Oscar和Alice的秘密钥，看是否和Bob一样

d. DS可以，因为DS需要Alice的个人密钥才能发出来，只需用Alice公钥解密就能查看是否是Alice发的

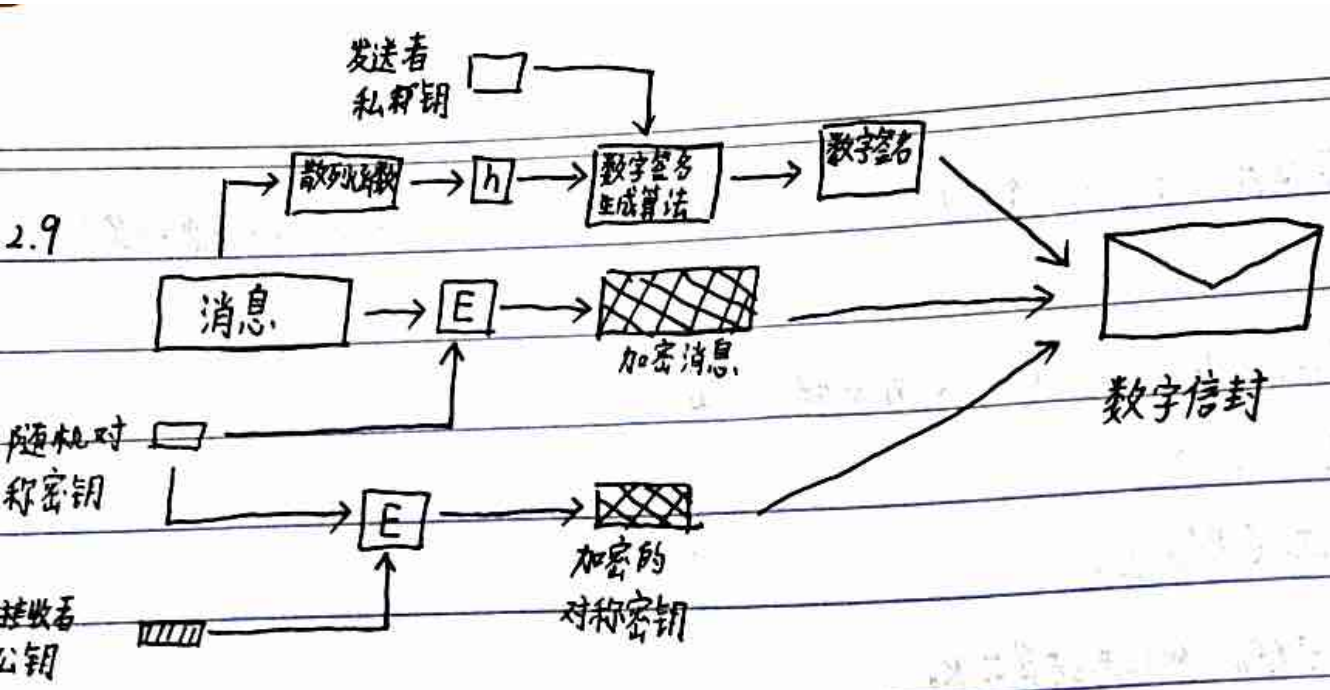
MAC不可以，MAC不具备不可否认性

2.8 a.

5	2	4	1	5
1	4	2	3	2
3	1	5	2	3
4	3	1	4	4
2	5	3	5	1

b. 假设p为明文，A使用M_2，B使用M_1和M_3，B选择一个随机数k，通过M_1映射为X，将X作为公钥发送给A，A使用将x，p加密得到Z；B得到Z后，与k一起用M_3解密得到p

c. 如果表足够大，且M_1，M_2足够随机，那么逆向操作时如果不知道k很难得出p


发送者
私钥
2.9
散列函数
h
数字签名
生成算法
数字签名
消息
E
加密消息
数字信封
随机对
称密钥
E
加密的
对称密钥
接收者
公钥