2.ecc原理及其应用

写一个关于john发送给BOb钱的交易结构

{

input:{//发送方john的信息，之后讨论

}

output:{//接收方Bob的信息

amount=5;

script PubKey=Bob的公钥;

}

}

一个密码学原理，单向得到

1.私钥（自己进行保管，可以得到公钥）

2.公钥

一般在具体使用的过程当中，会公开一些信息a

举例：通过

ECC("遗嘱“，私钥）=密文a;//密文a公开

只能使用公钥来把密文a来还原遗嘱//这里保证了遗嘱只能有本人（私钥拥有者）才能进行编写，公开的可以查看

ECC（“签名人”，公钥）=密文b：
只有私钥可以把密文b还原成hello//这个地方一般用于确认接收方是本人，偷偷给某人发消息。