密码学小测

20337251伍建霖

1.

一共能签2^l个签名，用了两个了，所以oscar能对2^l-2个新的消息签名

2.

（a）将椭圆曲线方程和2P=-P联立即可得出

（b）

3.  
δ为0说明x和a γ mod p-1同余，可直接算出a