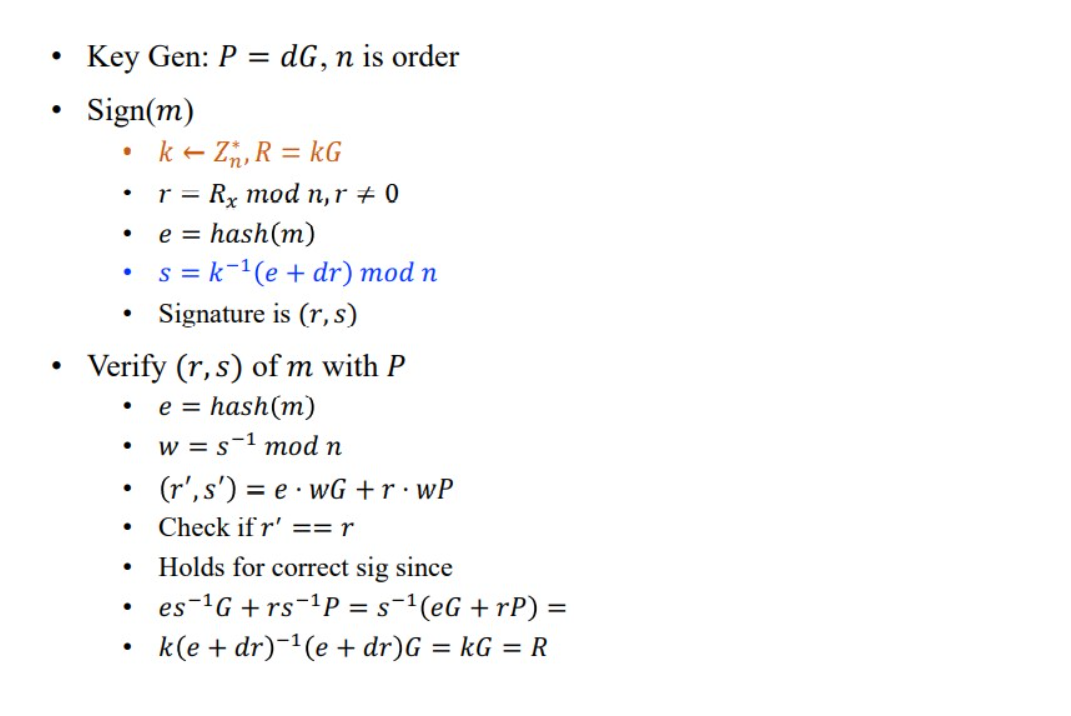
一：实验原理

课件中资料如下：



按照这种算法可以还原出私钥，前提是选取了一致的k

通过实现椭圆曲线算法，可以很实现算法中的各种运算是比较容易的 。

二：实验结果：

可以发现还原成功了。

同时测量了时间

