

## \*Project19: forge a signature to pretend that you are Satoshi

代码说明:

实现方法:

实现对于中本聪的伪造即要实现对于 ECDSA 签名的伪造

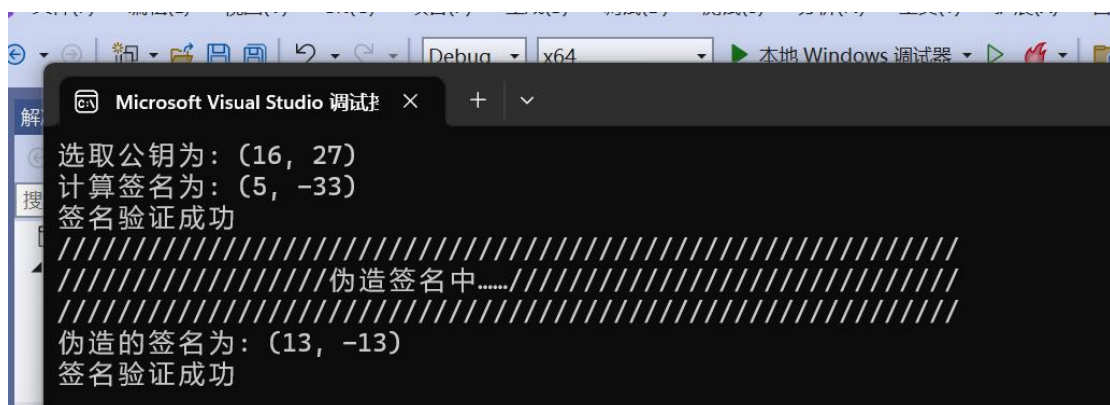
可以在已知公钥  $P$  的前提下, 通过构造  $e$  来重组合法签名。

第一步: 选取随机数  $u, v$ , 计算  $R = uG + vP$

第二步: 计算  $r = R.x$ 、 $s = r \cdot b^{-1} - 1$ 、 $e = r \cdot v^{-1} - 1$ . 其中  $e = H(m')$

$(r', s')$  即对消息  $m'$  的合法签名

运行结果:



```
Microsoft Visual Studio 调试器
选取公钥为: (16, 27)
计算签名为: (5, -33)
签名验证成功
////////////////////////////////////
//////////////////////////////////// 伪造签名中.....////////////////////////////////////
////////////////////////////////////
伪造的签名为: (13, -13)
签名验证成功
```

实现方式: C

分工: 自己独立完成