✅ Forge a signature to pretend that you are Satoshi

1.代码说明

假装你是中本聪，伪造一个ECDSA的签名

forge_signature.py

基本原理

1）随机选择**u** 和 **v** $u, v \in F_n^*$

$$u, v \in F_n^*$$

2）计算**R'**

$$R' = (x', y') = uG + vP$$

3）分别计算**r'**和**s'**

$$r' = x' mod(n) \qquad s' = r' v^{-1} mod(n)$$

4）伪造哈希值**e'**

$$e' = r' u v^{-1} mod(n)$$

5）伪造的签名值**signature'**

$$signature' = (R'_x, s')$$

6）验证伪造是否成功：验证计算出的**r**是否和**r'**相同即可证明

```
if r_forge % curve.n == r_:
        print("Verify passed!")
        print('Forge_signature_Success!')
    else:
        print("Falid!")
```

2.运行方式

python文件，直接在命令行中输入:

`python3 forge_signature.py`

3.实现效果

> 公私钥对是密钥生成算法得到
>
> **u, v**均是随机选择得到
>
> **R'** 利用u和v构造得到新的坐标**(x', y')**
>
> **e'** 是伪造的哈希值
>
> **s'** 是伪造的用于签名部分的内容

> **signature'** 是由**R'_x**以及**s'**组成