2019004600009 边照旗　　ECDSA 签名伪造.

一、ECDSA

1. 密钥生成：选择一条椭圆曲线 $E_p(a,b)$ 与基点 G
n为G的阶，选择私有密钥 $d<n$，利用基点G计算公开密钥 $P=dG$
即 $sk=d$，$pk=P$

2. 签名算法：$sign_{sk}(m)$
$k \leftarrow Z_n^*$，$R=kG$，$r=R_x \bmod n$（其中 $r\neq 0$，否则重新选择）
$e=hash(m)$，$s=k^{-1}(e+dr) \bmod n$　　输出签名 (r,s)

3. 验证算法：$vrfy_{pk}(m,r,s)$
$e=hash(m)$　$w=s^{-1} \bmod n$　　$(r',s')=e\cdot wG+r\cdot wP$
当且仅当 $r'==r$ 时，验证通过，输出1；否则输出0

4. 正确性证明：$es^{-1}G+rs^{-1}P=e\cdot wG+r\cdot wP=es^{-1}G+rs^{-1}P$
$\Rightarrow s^{-1}(eG+rP)=k(e+dr)^{-1}(eG+rP)=k(e+dr)^{-1}(eG+drG)$
$=k(e+dr)^{-1}(e+dr)G=kG=R=(r',s')$
$\because r=R_x \bmod n$　$\therefore$ 当且仅当 $r=r'$ 时，验证通过，正确性即证

二、ECDSA签名伪造.
PS：以下构造基于不要求具体的消息，而仅要求提供消息的Hash即可的情景.
已知的信息：公钥：P，公开参数：G，n
首先选择 $u,v\in F_n^*$
计算 $R'=(x',y')=uG+vP$，为了使验签算法通过，需令 $r'=x' \bmod n$
因为 $s'^{-1}(e'G+r'P)=uG+vP$
所以有 $\begin{cases} s'^{-1}r'=v \bmod n \\ s'^{-1}e'=u \bmod n \end{cases}$　　因此可先求出 $s'=r'v^{-1} \bmod n$
然后求出 $e'=r'uv^{-1} \bmod n=Hash(m')$
若Hash足够安全，则不以可忽略的概率有求出相应的 m'
但因此情景中，不要求求出 m'，求出 $Hash(m')$ 即可
因此可以成功伪造出公钥为 P 的用户对于 $Hash(m')=e'$ 的合法签名 (r',s')