*Project10: report on the application of this deduce technique in Ethereum with ECDSA

说明：

一、ECDSA 概述

ECDSA 是 Elliptic Curve Digital Signature Algorithm（椭圆曲线数字签名算的缩写。它是一种基于椭圆曲线密码学的数字签名算法。ECDSA 结合了椭圆曲线上的离散对数问题和哈希算法的安全性特性，提供了一种高效、安全的数字签名方案。

ECDSA 被广泛应用于各种加密和认证场景，包括数字证书、电子支付系统、区块链技术等。它的安全性基于椭圆曲线离散对数问题的困难性，即在给定椭圆曲线上的基点和一个点的情况下，计算出这个点的离散对数是困难的。这使得 ECDSA 具有相对较短的密钥长度和较高的计算效率。

ECDSA 的基本原理是使用私钥对消息进行签名，生成数字签名，然后使用对应的公钥对签名进行验证，确保签名的完整性和真实性。ECDSA 通过椭圆曲线上的点运算实现签名和验证操作，同时结合了哈希函数以增强安全性。

二、ECC 的实现

签名过程：

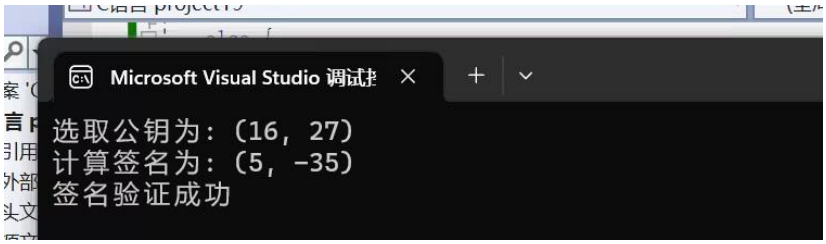
1. 选择一条椭圆曲线 Ep(a, b)和基点 G。
2. 选择私钥 k（k < n），其中 n 是基点 G 的阶数，通过计算公钥 K = kG。
3. 生成随机数 r（r < n），计算点 R = rG。
4. 将原数据和点 R 的坐标值 x、y 作为参数，计算哈希值 Hash = Hash(原数据, x, y)（通常使用哈希函数）。
5. 计算 s ≡ r - Hash * k (mod n)。
6. 如果 r 或 s 中有一个为 0，则重新从步骤 3 开始执行。

验证过程：

1. 接收方在收到消息 m 和签名值(r, s)后进行以下运算。
2. 计算 sG + H(m)P = (x1, y1)，其中 H(m)是对消息 m 进行哈希计算的结果。
3. 验证等式：r1 ≡ x1 (mod n)，其中 r1 为计算得到的临时值。
4. 如果等式成立，则接受签名；否则，签名无效。

实现方式：C

结果：在自己电脑上 CPU：11 代 i7



分工：自己独立完成