*Project21: Schnorr Bacth

说明:

Schnorr Signature

- Key Generation
  - $P = dG$
- Sign on given message M
  - randomly k, let $R = kG$
  - $e = hash(R||M)$
  - $s = k + ed \bmod n$
  - Signature is : (R, s)
- Verify (R, s) of M with P
  - Check sG vs $R + eP$
  - $sG = (k + ed)G = kG + edG = R + eP$

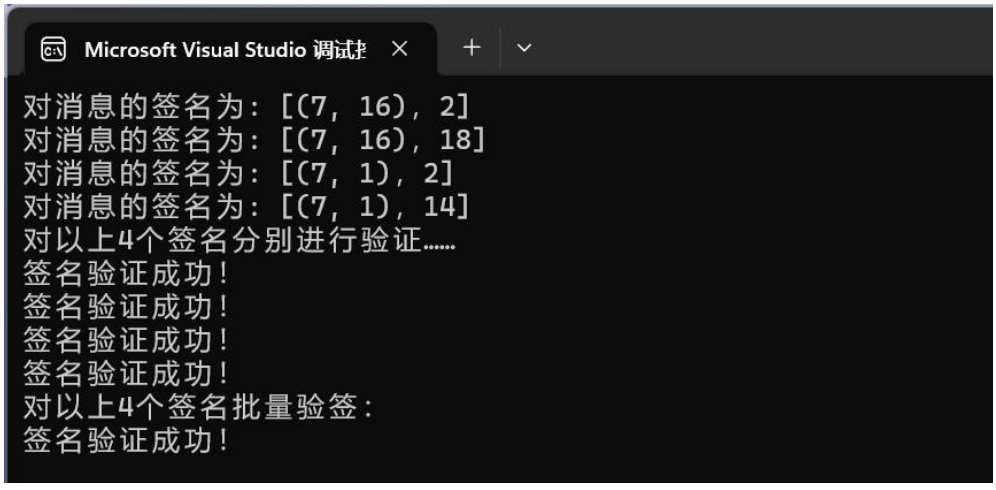
根据以上 Schnorr 签名方案实现基础的 Schnorr 签名以及认证。实现 Schnorr 签名的批量验签。

批量验证的原理:

给定有 n 个公钥、消息和签名元组 (Pi , mi , (Ri , si)), 验证者生成 n 个随机数 a1, ⋯ , an , 来计算 n 个挑战哈希值 ei = H(Pi , Ri , mi) , 然后检查:

(a1s1+a2s2+⋯+ansn)* G?=a1* R1+a2* R2+⋯+an* Rn+(a1e1)* P1+(a2e2)* P2+⋯+(anen)* Pn, 如果相等则通过验证。

运行结果:



实现方法:

本项目使用 C 语言编程实现

分工: 自己独立完成