2025年8月10日：

‌第一阶段：基础理论（1-2周）‌

1.‌区块链核心概念‌

a.公私钥加密（非对称加密）原理的核心在于使用数学关联但功能分离的密钥对实现安全通信，其运作机制与核心特性如下：

**🔑 一、核心原理**

1. ‌**密钥对生成**‌  
   用户生成唯一配对的公钥（Public Key）与私钥（Private Key），二者通过特定数学算法（如大整数分解、椭圆曲线离散对数）关联，但无法相互推导。私钥严格保密，公钥可公开分发。
2. ‌**加密与解密流程**‌
   * ‌**加密**‌：发送方使用接收方的公钥加密明文生成密文（如 Cipher = RSA\_Encrypt(明文, 接收方公钥)）。
   * ‌**解密**‌：接收方使用私钥解密密文（如 明文 = RSA\_Decrypt(Cipher, 私钥)）。

⚠️ 公钥加密的内容仅能由配对私钥解密，反之亦然。

1. ‌**单向陷门函数**‌  
   加密函数可高效计算（如 x^e mod n），但逆向解密依赖私钥参数（如指数 d），若无私钥则计算不可行（数学难题保障安全）。

**⚖️ 二、与对称加密的对比**

| ‌**特性**‌ | ‌**非对称加密（公私钥）**‌ | ‌**对称加密**‌ |
| --- | --- | --- |
| ‌**密钥数量**‌ | 密钥对（公钥+私钥） | 单一共享密钥 |
| ‌**密钥分发**‌ | 公钥可公开，私钥保密 | 需安全渠道传递密钥 |
| ‌**速度**‌ | 较慢（适合小数据） | 较快（适合大数据量） |
| ‌**典型算法**‌ | RSA、ECC、SM2 | AES、DES、SM4 |
| ‌**应用场景**‌ | 密钥交换、数字签名 | 文件加密、实时通信 |

**🛡️ 三、核心功能与应用**

1. ‌**保密通信**‌  
   发送方用接收方公钥加密数据，确保仅目标接收者可解密（如电子邮件加密）。
2. ‌**数字签名**‌
   * ‌**生成**‌：发送方用私钥对消息哈希值加密生成签名。
   * ‌**验证**‌：接收方用发送方公钥解密签名，比对消息哈希值验证来源真实性与完整性。
3. ‌**混合加密实践**‌  
   结合二者优势：用非对称加密传递对称密钥，再用对称密钥加密大量数据（如TLS/SSL协议）。

**🔐 四、安全基石与挑战**

1. ‌**数学难题保障**‌
   * RSA：大整数质因数分解难题（如分解300位整数需亿年）。
   * ECC：椭圆曲线离散对数难题（更短的密钥长度实现同等安全）。
2. ‌**量子计算威胁**‌  
   Shor算法可高效破解RSA与ECC，推动抗量子算法（如基于晶格的NIST标准）发展。

**💡 五、技术演进意义**

自1976年Diffie-Hellman开创非对称加密理论，到RSA成为首个实用系统，公私钥机制解决了对称加密的密钥分发瓶颈，奠定了数字证书（如X.509）与区块链（如比特币地址派生）的安全基础。