密码学基础

1. Calculate GCD(36,48), GCD(54,72)
2. Prime Factorization: 12250
3. Use Extended Euclidean Algorithm calculate x, y in $ax + by = GCD(a, b)$ with $a = 911, b = 999$
4. Calculate Modular Inverse of $911 \bmod 999$
5. What is Euler's Function
6. $\phi(10), \phi(36), \phi(100)$
7. Use Repeated Modular Multiplication compute $11^{15} \bmod 13$
8. What is Fermat's Little Theorem?
9. Use Fermat's Little Theorem Compute $11^{1,073,741,823} \bmod 13$
10. **判断 227 和 79 是否互质。**
11. **求 79 mod 229 的乘法逆元。**
12. **无需计算任何东西，只需查看数字，您能判断 7932 是否有乘法逆模 11958 吗？解释。**
13. **Show the steps of how to calculate $\phi(730)$.**
14. **Calculate $227^{54996213} \bmod 21$ as efficient as possible.**
15. 阿贝尔群的定义
16. 循环群的定义，之间的差异G�G�和G�G�
17. **is $\mathbb{Z}_6^*$ forms a cyclic group?**
18. **is $(\mathbb{Z}_5, +)$ cyclic? give a genrator of the group**
19. **is $(\mathbb{Z}_8^*, \times)$ cyclic? give a genrator of the group**
20. 什么是安全参数
21. 什么是高效算法
22. 什么是可忽略概率和可忽略函数
23. 简述如何生成随机素数
24. What is $GenGroup$ (Algorithm)
25. 什么是离散对数
26. Consider a cyclic group G with a prime order q. Let g be a generator of G. Suppose $h \in G$ and $h = g^x$ for some $x \in \mathbb{Z}_q$. Given $g = 7$, $q = 23$, and $h = 10$, calculate the discrete logarithm of h with respect to g.

    > hint: which is finding the x such that $10 = 7^x \mod 23$.

27. 什么是离散对数假设（DL）
28. 什么是计算 Diffie-Hellman 假设 (CDH)
29. 什么是决策性 Diffie-Hellman 假设 (DDH)
30. Given an element $h \in G$, how to (efficiently) compute its inverse element in G.
31. 描述公钥加密方案（语法）

32. 描述 Kerckhoffs 原理
33. 描述正确的安全保证
34. 四种威胁模型的攻击难度排名（各模型描述）
35. 什么是 El Gammal 加密
36. 描述数字签名方案（语法）
37. 描述数字签名的安全模型（EUF）
38. 什么是哈希函数
39. 描述Hash函数的三抗
40. 简单介绍MD5、SHA-1、SHA-256
41. 简要描述 SKE 与 SKE 之间的差异。PKE
42. 混合加密的过程
43. 简要描述数字证书的工作原理和CA
44. 描述 Diffie-Hellman 密钥交换协议

比特币

1. 什么是比特币账本
2. 什么是TXO和UTXO
3. 如何将币/TXO与其所有者绑定，以便只有币的所有者才能花费它?
4. 比特币的隐私保护相当薄弱。如何增强呢?
5. 解释使用Hash作为地址的含义
6. 交易 JSON 中输入和输出的内容?
7. 描述 scriptSig 和 ScriptPubKey
8. 如何判断一笔交易是否有效
9. 什么是默克尔树？比特币头部中使用Merkle Tree的含义
10. 什么是哈希指针？如何维护哈希链?
11. 块里面有什么？块头（4 个字段）和块体里面有什么?
12. **区块的哈希值不包含在区块本身中，既不在网络上传输，也不作为区块的一部分存储在存储中。为什么?**
13. **请注意，没有签名来保证 coinbase 交易的完整性。攻击者是否可以修改他人的coinbase交易来获得区块奖励和交易费用?**
14. 描述比特币的挖矿过程
15. 新难度公式
16. 交易如何记录在区块链上
17. 描述竞争条件
18. 描述比特币协议的默认策略
19. 数据存储在轻量级节点中
20. 数据存储在完全验证节点中
21. 共识目标
22. 为什么节点会诚实行事?
23. 为什么遵循/选择最长的链?
24. 这些区块何时实现最终性/稳定性并成为共识区块链的一部分?
25. 矿池中的矿池管理者和矿池成员是什么
26. 付费模式
27. 矿池的优点和缺点
28. 两种攻击方式
29. 比特币脚本中的 MULTISIG 是什么

30. 高效小额支付流程
31. 锁定时间流程
32. 热存储与冷存储的区别
33. 描述分层确定性算法
34. 如何存储和保护主密钥
35. 共识定义
36. FLP 不可能
37. CAP定理
38. 介绍比特币PoW共识和实验结果
39. 什么是拜占庭式失败
40. 什么是PBFT
41. 混币
42. 硬币洗牌

门罗币

1. 如何加强用户的隐私保护
2. 什么是隐形地址
3. 引入隐形地址
4. 引入环签名
5. 引入可链接环签名
6. 介绍承诺
7. 引入扩展可链接环签名