Fundamentals of Cryptography

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. **Determine whether 227 and 79 are relatively prime.**
11. **Find the multiplicative inverse of 79 mod 229.**
12. **Without calculating anything, by simply looking at the numbers, can you tell whether 7932 has a multiplicative inverse mod 11958? Explain.**
13. **Show the steps of how to calculate $\phi(730)$.**
14. **Calculate $227^{54996213} \bmod 21$ as efficient as possible.**
15. Definition of an Abelian Group
16. Definition of a cyclic group, diff between G and 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. What is Security Parameter
21. What is Efficient Algorithms
22. What is Negligible Probability and Negligible Function
23. Briefly describe How to generate a random prime
24. What is $GenGroup$ (Algorithm)
25. What is Discrete Logarithm
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. What is The Discrete Logarithm Assumption(DL)
28. What is The Computational Diffie-Hellman Assumption(CDH)
29. What is The Decisional Diffie-Hellman Assumption(DDH)
30. Given an element $h \in G$, how to (efficiently) compute its inverse element in G.
31. Describe Public Key Encryption scheme(syntax)
32. Describe Kerckhoffs' Principle

33. Describe the right Security guarantee
34. Ranking of Attack Difficulty for Four threat model (with each model describe)
35. What is El Gammal Encryption
36. Describe Digital Signature scheme(syntax)
37. Describe the Security Model (EUF) of Digital Signature
38. What is Hash Function
39. Describe Three resistance of Hash Function
40. Briefly introduce MD5, SHA-1, SHA-256
41. Briefly describe difference between SKE Vs. PKE
42. Procedure of Hybrid Encryption
43. Briefly describe how Digital Certificates works and CA
44. Describe Diffie-Hellman Key Exchange Protocol

Bitcoin

1. What is the Ledger of Bitcoin
2. What is TXO and UTXO
3. How to bind the coin/TXO with its owner, so that only the owner of a coin can spend it?
4. The privacy-protection of bitcoin is pretty weak. How to enhance it?
5. Explain the meaning of Using Hash as the Address
6. The content of inputs and outputs in a transaction JSON?
7. Describe scriptSig and ScriptPubKey
8. How to judge whether a transaction is valid
9. What is Merkle Tree? the meaning of use Merkle Tree in bitcoin header
10. What is Hash Pointer? how to maintain Hash Chain?
11. What inside a Block? What inside a block header(4 fields) and block body?
12. **The hash of the block is not included in the block itself, neither transmitting on network or storing as a part of the block in storage. why?**
13. **Note that there is not signature to guarantee that the coinbase transaction's integrity. Could an attacker modify other's coinbase transaction to get the block reward and transaction fee?**
14. Describe the Mining procedure in Bitcoin
15. Formula of new difficulty
16. How a transaction is recorded on Blockchain
17. Describe race condition
18. Describe Default policy of Bitcoin protocol
19. Data stored in lightweight nodes
20. Data stored in fully validating nodes
21. Target of consensus
22. Why does a node behave honestly?
23. Why follow/choose the longest chain?
24. when do the blocks achieve finality/stability and become one part of the consensus blockchain?
25. What is Pool Manager and Pool members in Mining Pools
26. Pay models
27. Pros and Cons of Mining Pools
28. Two kind of attacks
29. What is MULTISIG in Bitcoin Script
30. Procedure of Efficient micro-payment
31. Procedure of Lock Time

32. Diff Hot Storage vs. Cold Storage
33. Describe Hierarchical Deterministic Algorithm
34. How to store and protect the master secret key
35. Consensus Definition
36. FLP Impossibility
37. CAP Theorem
38. Introduce Bitcoin PoW Consensus and Experimental results
39. What is Byzantine failures
40. What is PBFT
41. Coin-Mix
42. Coin-Shuffle

Monero

1. How to Enhance user's privacy
2. What is Stealth Address
3. Introduce Stealth Address
4. Introduce Ring Signature
5. Introduce Linkable Ring Signature
6. Introduce Commitment
7. Introduce Extended Linkable Ring Signature