Symmetric Key Cryptography

1. What is one-time padding and why it satisfies the perfectly secret
2. For any perfect secure symmetric-key encryption, we must have key-space $\geq$ message-space. Why
3. Let $G : \{0,1\}^k \rightarrow \{0,1\}^{k+l}$ be a PRG. How to construct an IND-eavesdropper Enc (with fix length)
4. collision-resistant and one-wayness of hash function
5. Given $\mathrm{Hash}(\mathrm{m}_1, \mathrm{m}_2)$, where Hash is a collision-resistant hash function. Is it possible to find a $\mathrm{m}'_2 \neq m_2$ such that $\mathrm{Hash}(\mathrm{m}_1, \mathrm{m}_2) = \mathrm{Hash}(\mathrm{m}_1, \mathrm{m'}_2)$, why

Public Key Cryptography

1. How does the Diffie-Hellman key exchange work?
2. How does ElGamal work?
3. How does RSA encryption work?
4. Why ElGamal is not IND-CCA secure? (i.e., when the adversary can query the decryption oracle)
5. How does the textbook RSA signature works? Attacks to textbook RSA signature?
6. Hash-then sign paradigm of RSA signature

Network Security

1. man-in-the-middle attack to the Diffie-Hellman key exchange?
2. What is the structure of public key infrastructure (PKI)?
3. How does TLS 1.2/1.3 work

4. Applications of Diffie-Hellman key exchange in WhatsApp and Signal

Authentication

1. Three kinds of authentication method
2. How does password authentication work? The attacking strategy and the guessing probability
3. How does Biometric Authentication work? The main drawback of biometric authentication
4. How does Public key Authentication work?

PQC and FHE

1. Quantum Threat to public key cryptography and symmetric key cryptography
2. Why do we need to handle this problem right now
3. What is fully homomorphic encryption?
4. Applications of fully homomorphic encryption (what we can do with FHE in hand)
5. RSA encryption is a special homomorphic encryption which only supports multiplication

Zero-knowledge proof

1. Design a zero-knowledge protocol to show that two pictures are different. (i.e., Assume Alice knows the difference and wants to prove that they are different, but do not what to tell the difference directly)
2. Sigma protocol for knowing a of g^a
3. Sigma protocol for DDH relation

4. Sigma protocol to prove that an Elgamal ciphertext is the encryption of 0 or 4

Multiparty computation

1. What is multiparty computation
2. What is an oblivious transfer protocol
3. With oblivious transfer and AES encryption in hand how to compute the AND/OR gate between two semi-honest parties (by using Yao's Garble circuit)
4. Find some application scenarios for a Multiparty computation for any function.

Security and privacy in Blockchain

1. How does bitcoin (as a special blockchain) work?
2. What do the miners do in order to win 6.25 BTC reward? Or what is mining?
3. How to use the Merkle tree/proof to prove that a transaction is in the blockchain (since the blockchain usually only contains the block header which includes only the Merkle root)