1. As one of key blockchain applications, what are the advantages and disadvantages of cryptocurrencies?

Sample solutions:

Advantages

- Fast, safe and cheap
- Ease of use and high portable
- Pseudonymity
- Decentralization
- Active involvement of users
- Transparent and neutral

Disadvantages

- Unrecoverable once lost
- High market volatility
- Malicious activities (money laundering, scam)
- Lack of auditability
- Low Performance (high latency, low throughput)

(15 marks)

2. Why cryptography is not equal to security? Please justify your answers with some examples.

Sample solutions:

Cryptography is a part of computer security system to protect our confidential information. It must work with other components of computer security system together to ensure the security of the system.

For example, encrypting a confidential word document by a strong password can prevent it to be leaked to other untrusted persons though the security of this confidential document depends on many factors, such as the location, the sharing manner, and protection scheme of the document.

(10 marks)

3. What are the limitations of substitution ciphers? What are the limitations of symmetric cryptography? (20 marks)

Sample solutions:

1. Substitution ciphers' limitations:
   Substitution ciphers suffer from frequency analysis attacks. Some simple substitution ciphers (like Cæsar cipher) have limited number of keys, e.g., Cæsar cipher has only 26 alphabet characters.

2. Symmetric cryptography's limitations:
   Symmetric cryptography faces a challenge in key distribution since the increased number of communication pairs will lead to the explosion of keys, e.g., n(n-1)/2 keys for n users.

(20 marks)

4. Consider that Alice and Bob conduct Diffie-Hellman key exchange. They have agreed on a prime p= 13, and α = 2. Then, Alice and Bob have chosen their secrete keys X_A and X_B to be 5 and 4, respectively. Please prove that they can achieve the key exchange by the Diffie-Hellman scheme.

Sample solutions:

1) Alice calculates $Y_A=2^5 \bmod 13 = 6$.
2) Bob calculates $Y_B=2^4 \bmod 13 = 3$.
3) Alice then calculates $K=3^5 \bmod 13 = 243 \bmod 13 = 9$
4) Bob then calculates $K'=6^4 \bmod 13 = 1296 \bmod 13 = 9$
5) Thus, K=K'. Alice and Bob can successfully exchange their key K.

(20 marks)

5. In digital signatures, signing can be done at both the whole message or on the hash of the message? Is this statement correct? What are the benefits to sign on the hash of the message?

Sample solutions:

Correct, signing can be done either on the whole message or on the hash of the message.

The benefit to sign on the hash of the message is to save the computational time in encrypting the whole message since digital signature typically relies on public key algorithms, which require extensive computation time to encrypt a message.

(15 marks)

6. Please compare Client-Server and P2P architectures in terms of pros and cons.

Sample solutions:

	Client-Server	P2P
Pros	• Easy to maintain security and reliability • Enable a wide range of services • Easy to design and implement	• Distributed trust • Balanced resource load • High resource capacity and high scalability • High fault-tolerance and resiliency against DoS attacks
Cons	• Central point of failure and compromise of malicious attacks • Performance bottleneck due to central resource management and administration • Central point of trust: fully controlled by a center (or a platform) • Poor scalability: decreased throughput with the increased number of clients	• Costly backup, high bandwidth consumption • Hard to control • Hard to maintain security and consistency • Unstable due to churns (nodes joining or leaving)

(20 marks)