1. As one of key blockchain applications, what are the advantages and disadvantages of cryptocurrencies? (15 marks)

2. Why cryptography is not equal to security? Please justify your answers with some examples. (10 marks)

3. What are the limitations of substitution ciphers? What are the limitations of symmetric cryptography? (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 XA and XB to be 5 and 4, respectively. Please prove that they can achieve the key exchange by the Diffie-Hellman scheme. (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? (15 marks)

6. Please compare Client-Server and P2P architectures in terms of pros and cons. (20 marks)