Problem 1 [30 points]

1. What is the difference between Collision-Resistance and Preimage-resistance in hash functions? Which condition is stronger? [5 points]

2. Suppose a hash function uses 256 bits to represent the message digest. What is the minimum size of the message space (i.e., the total number of messages) to guarantee that we have at least one collision? [5 points]

3. Consider a hash function $h : (\mathbb{Z}_2)^5 \to (\mathbb{Z}_2)^3$ by the rule $h(x) = xA$ where all operations are modulo 2 and the linear hash function is given by: [20 points]

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

   Consider the following messages:
   $x_1 = (0, 1, 0)$
   $x_2 = (1, 1, 1)$
   Find all the preimages for x_1 and x_2.

Problem 2 [20 Points]

Let $\mathcal{P} = \{A, B, C\}$ and let $\mathcal{K} = \{K_1, K_2, K_3\}$ denote the set of messages and the set of keys, respectively. Let $\mathcal{C} = \{1, 2, 3, 4\}$ and suppose the encryption functions are represented by the following encryption matrix:

	A	B	C
K_1	1	2	3
K_2	2	3	4
K_3	3	4	5

The probability distribution over the set of keys is given by $Pr(K_1) = Pr(K_2) = Pr(K_3) = \frac{1}{3}$. Does this cryptosystem achieve perfect secrecy. Show all the necessary calculations.

Problem 3: [21 Points (3 points per question)]

Briefly answer the following questions:

1. How does Bitcoin protocol prevents people from copying transactions in the ledger?
2. Explain the notion of overspending in a digital ledger. How does Bitcoin protocol prevents overspending?
3. How Bitcoin ensures that everyone in the system has the same ledger? In other words, in the case of having conflicting chain of ledgers, how the Bitcoin users decide which ledger to trust? Explain your answer.
4. With the increasing number of miners, how is it possible to reduce the probability of collision in the hash functions used for Proof of Work?
5. How Bitcoin keeps the ledger blocks in order? Draw the schematic of a few Bitcoin blocks and show how they are kept in order.
6. Consider Alice received two Block Chains that are only different in the very last block. What Bitcoin suggests to resolve the conflict?
7. Why the miners' reward gets cut in half almost every four years?

Problem 4 [29 Points]

Consider two dimensional lattice with base vectors $V_1 = [1, 0, 2]$ and $V_2 = [1, 0.1, 2]$.

1. Find the angle between the two vectors. [5 points]
2. Draw the lattice. [4 points]
3. Find the closest point to $P = [4, -1, 2]$. Use linear Algebra and the system of linear equations to solve the problem. [15 points]
4. What can we say about the difficulty of the problem? [5 points]