Suppose we have two implementations (Machine A and machine B, namely) of the same instruction set architecture. For some program which has 1 million instructions,

Machine A has a clock cycle time of 100ps and an average CPI of 4.0.

Machine B has a clock cycle time of 130ps and an average CPI of 3.0.

a. What machine is faster for this program, and by how much?

b. If overclocking (i.e., driving the given machine with faster clock speed) of the slower machine is possible, what clock rate should be used to execute the given program to achieve the same execution time of the faster machine?
Assume you are given a hard disk with 512B sector, 15,000RPM, 3ms average seek time, 150MB/s transfer rate and 0.1ms controller overhead. Calculate the average time for reading a sector.

What if you spin disks twice faster (i.e., 30,000RPM)? Calculate the average time for reading a sector again.
The delay is the time between the start of a process and its completion, and throughput is amount of work done per unit time.

1) Calculate the delay and throughput of the system shown as follows:

```
+-------------------+ 30ns  +-------------------+
|                  |       |                  |
| Comb Logic C      |       | REG              |
|                  |       |                  |
|                  |       |                  |
+-------------------+ 3ns    +-------------------+
|                  |       |                  |
CLK               |       | CL                 |
```

2) In order to increase the throughput, we design the following 3-stage pipeline system. Please calculate its delay and throughput.

```
+-------------------+ 8ns    + 3ns    + 2ns    + 6ns    + 3ns    + 2ns    + 2ns    + 10ns    + 3ns    +
|                  |       |       |       |       |       |       |       |       |
| Comb Logic C1    |       | REG   |       | Comb Logic C3 |       | Comb Logic C4 |       | Comb Logic C5 |       |
|                  |       |       |       |       |       |       |       |       |
|                  |       |       |       |       |       |       |       |       |
+-------------------+ 3ns    + 3ns    + 2ns    + 10ns    + 3ns    + REG   +       |       |
|                  |       |       |       |       |       |       |       |       |
CLK               |       |       |       |       |       |       |       |       |
```

3) Please try to rearrange the above structure in section 2) to further optimize the performance, and calculate the delay and throughput of your improved design.
Consider a two bit comparator

a) Design it using 1 bit comparators shown in the figures.
b) Design the two-bit comparators as a single block (Derive the gate-level realization as shown above for 1-bit comparator)

c) For both designs calculate maximum propagation delay. Assume that a gate introduces 1ns delay.
Find the minimal sum of products (SOP) expression, the canonical POS expression, and the canonical SOP expression for \( H(a, b, c, d) = \prod M(7, 8, 9, 10, 12, 14, 15) \).
Answer the following questions given the function $f(A, B, C, D) = \sum m(0,1,2,7,9,13,15) + d(3,5)$

a) Find the minimal POS expression for $f$.

b) Implement $f$ using NAND gates only.
Simplify the following functions using Boolean algebra. DO NOT USE K-MAPS.

a) \( F = (x+z)(w+x)(y'+z)(w+y') \)

b) \( H = \bar{x} + yz + \bar{y}z \)
The schematic below is for an edge triggered D flip flop. Answer the following questions.

a) Draw a gate-level representation for a master-slave D flip flop.

b) Describe the operational similarity and differences between an edge triggered flip flop and an edge sensitive flip flop such as a master-slave configuration.
(a) List five paradigms of Computational Intelligence. With aid of a diagram, give examples of five hybrids with a brief explanation of each.

(b) The figure below represents the McCulloch-Pitts model of an artificial neuron.

Fig. Q1
(i) Write the output equation $y_i$ of the neuron given that cell body consists of a tanh function.

(ii) The summation unit in Fig. Q1 is replaced by a product unit, repeat (i).
(a) Write out the forward propagation equation for a Jordan recurrent neural network (size: \((n+r) \times m \times r\)) and a Jordan simultaneous recurrent neural network (size: \((n+r) \times m \times r\)).

(b) What is the difference between supervised, unsupervised and reinforcement learning?
Having introduced swarm intelligence and studied particle swarm optimization (PSO) in class, describe the following:

(a) The origins and five principles of Swarm Intelligence (SI)

(b) What is the difference between PSO and SPPSO? Provide the two advantages and disadvantages of these algorithms.
(a) With aid of diagrams describe three neurocontrol strategies.
(b) Describe how the exploration and exploitation principles are embedded in the ant colony optimization algorithm.
For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a linear block cipher $EL$ that encrypts 128-bit blocks of plaintext into 128-bit blocks of ciphertext. Let $EL(k,m)$ denote the encryption of a 128-bit message $m$ under a key $k$ (the actual bit length of $k$ is irrelevant). Thus:

$$EL(k,[m1 \ XOR \ m2]) = EL(k,m1) \ XOR \ EL(k,m1)$$

for all 128-bit patterns $m1$, $m2$

Describe how, with 128 chosen ciphertexts, an adversary can decrypt any ciphertext without knowledge of the secret key $k$. (A "chosen ciphertext" means that an adversary has the ability to choose a ciphertext and then obtain its decryption. Here, you have 128 plaintext/ciphertext pairs to work with and you have the ability to choose the value of the ciphertexts.)
Answer the questions below.

1. Alice wants to send a single bit of information (a yes or no) to Bob by means of a word of length two. Alice and Bob have four possible keys available to perform message authentication. The following matrix shows the two-bit word sent for each message under each key.

<table>
<thead>
<tr>
<th>Key</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>00</td>
</tr>
<tr>
<td>3</td>
<td>01</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>10</td>
</tr>
</tbody>
</table>

a. The preceding matrix is in a useful form for Alice. Construct a matrix with the same information that would be useful for Bob.

b. What is the probability that someone else can successfully impersonate Alice?

c. What is the probability that someone can successfully replace an intercepted message with another message?

2. What is the difference between strong and weak collision resistance, in the context of a cryptographic hash function?

3. What is the difference between diffusion and confusion in encryption?
A Hamming code can be described by its parity check matrix $P$ of $n$ columns, each corresponding to one of the $n$ bits of the encoded word, and $r$ rows, each corresponding to one of the parity check bits.

a. Construct a parity matrix of 15-bit SECDED (Single error correcting, double error detecting) Hamming code, where $k = 11$ ($k$ is the number of information bits) and $r = 4$ ($r$ is the number of check bits).

b. Derive Boolean equations for check bits and error address bits.
A redundant system, \( R_{sys}(t) \), consists of 5 identical components, \( R(t) \). On average of continuous, \( R(t) \) fails every 1,000 hours. Shown below is the reliability diagram for \( R_{sys}(t) \). Using the exponential failure law, find \( R_{sys}(100) \), which is the reliability of the overall system at \( t = 100 \).