1. Do you know who is "The Person of Year 2006" from Time Magazine? (5%)
   Explain the reason why. (5%)
2. Structured programmers use flowcharts to design their programs. Please draw a flowchart
   which shows the conversion from degrees Celsius and Fahrenheit. (10%)
3. Suggest ways to improve the running time of Quicksort. (5%)
4. Please simplify the Boolean expression of \(a\bar{c}+a'b'+b'c'+ab\) to the simplest form. (5%)
5. Please convert (76.33)_8 to a binary number. (3%)
6. Comment on the following statement: Problem \(A\) is an \(NP\) problem because no polynomial time
   algorithm has ever been designed for it. (5%)
7. Give a set of \(n\) items \(\{1, 2, \ldots, n\}\), each \(i\) of is characterized by two attribute values \(\alpha_i\) and \(\beta_i\).
   Assume \(n\) is an even number. Let \(\pi_1\) be a sequence of the \(n\) items sorted in non-decreasing order of \(\alpha_i\)
   and \(\pi_2\) a sequence of the \(n\) items sorted in non-decreasing order of \(\beta_i\). We want to arrange the \(n\) items
   into sequence \(\text{Seq}[1:n]\) by the following segment of codes. Describe the data structure(s) that you use
   to implement the procedure, and analyze the time complexity of your implementation. (8%)
   
   For \(i = 1\) to \(n\) do
   
   If \(i\) is odd then Retrieve the first element of \(\pi_1\);
   else Retrieve the first element of \(\pi_2\);
   
   Seq[i] = the retrieved element;
   Delete the retrieved element from both \(\pi_1\) and \(\pi_2\).

8. The following is Kruskal’s algorithm for finding a minimum spanning tree of a connected weighted
   graph. Determining if a cycle is created when adding a new edge is crucial. Describe how to
   implement the detection of cycle. (7%)

Kruskal’s Algorithm for Minimum Spanning Tree

Input: Connected weighted graph \(G = (V, E)\), where \(V\) and \(E\) are the vertex set and edge sets,
respectively.

Step 1: Tree \(T = \varnothing\).
Step 2: Sort the edges of \(E\) in non-decreasing order of weights.
Step 3: While \(T\) contains less than \(|V|-1\) edges do
   
   Select from \(E\) the edge \(e\) with the smallest weight.
   If \(T \cup \{e\}\) does not contain a cycle then \(T = T \cup \{e\}\).
   Remove edge \(e\) from \(E\).

Step 4: Report \(T\).
9. CPU Scheduler: There are \( n \) computing tasks \( \{J_1, J_2, \ldots, J_n\} \) on a CPU. Task \( J_i \), \( 1 \leq i \leq n \), can be considered for processing from time \( r_i \) onwards and its processing will take \( t_i \) units of time. Assume interruption is allowed. That is, the scheduler can suspend the task under processing for serving a new task and the suspended task can be resumed later when the CPU is free. Let \( C_i \) denote the time at which task \( J_i \) is finished. The CPU scheduler’s consideration is to schedule the tasks so as to minimize the sum of completion times of all jobs, i.e., \( \sum_{i=1}^{n} C_i \), which measures the average completion time of the tasks.

(a) Give a scheduling policy for the scheduler. Use the given data set to demonstrate the proposed policy. (5%)

<table>
<thead>
<tr>
<th></th>
<th>( J_1 )</th>
<th>( J_2 )</th>
<th>( J_3 )</th>
<th>( J_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r_i )</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>( t_i )</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

(b) Can the proposed policy optimally solve any input instance? Prove or disprove it. (8%)

10. (a) There are two types of encryption: link encryption and end-to-end encryption. What is the difference between these two encryption techniques? Detail their pros and cons. (9%)

(b) IP Security (IPSec) and Secure Socket Layer (SSL) are two widely used security protocols. Are they complementary to each other? Detail your comments. (9%)

11. Please explain the following terminologies: (16%)

(a) Pretty Good Privacy (PGP)

(b) Information Security Management System (ISMS)

(c) Role-Based Access Control (RBAC)

(d) Universal Description, Discovery and Integration (UDDI)