2018-19
B. TECH. (WINTER SEMESTER) EXAMINATION
COMPUTER ENGINEERING
COMPILER DESIGN
CO406

Maximum Marks: 60
Credits: 04
Duration: Two Hours

Answer all questions.
Assume suitable data if missing.
Notations and symbols used have their usual meaning.

Q.No. Question CO M.M.
1(a) Give unambiguous grammar for arithmetic expression. For your grammar, give rightmost derivation and parse tree for the following string – (CO1) [7.5]

\[ id * id * id \]

1(b) Why look ahead is needed in order to identify a token during lexical analysis phase? Take suitable example to explain. (CO1) [7.5]

2(a) Construct canonical parsing table for the following grammar – (CO3) [7.5]

\[ S \rightarrow BB \]
\[ B \rightarrow bB | d \]

2(b) Define following terms – 1) Synthesized Attribute 2) Inherited Attribute 3) L-Attributed Definition (CO1) [7.5]

OR

2'(a) Consider following grammar for arithmetic expression consisting of multiplication (*) and exponential (^) operator – (CO2) [7.5]

\[ E \rightarrow E \ast E | E^E | id \]

Construct SLR parsing table for above grammar. Use operator precedence and associativity to eliminate conflict in the parsing table.

Contd...2.
2'(b) For the following grammar, construct predictive parsing table after eliminating left-recursion -
\[ E \rightarrow E + E \mid E \cdot E \mid id \]

3(a) Describe type expression for function and record by taking suitable example.

3(b) Give back-patching based syntax directed translation scheme to translate boolean expression (consisting of &&, ||, not and relational operator) to three address code.

OR

3'(a) How is intermediate code generated for goto statement? Describe.

3'(b) Consider a three-way branching statement as described below –
\[ ON \ x \ negative \ S_1 \ zero \ S_2 \ positive \ S_3 \]
Statement S_i is executed when number x is negative else statement S_2 is executed when x is zero, otherwise statement S_3 is executed when x is positive. Give syntax directed translation scheme to translate three-way branching statement to three address code.

4(a) Identify blocks and construct flow graph for following three address code –
1. \( x = a + b \)
2. \( if \ x < 100 \ goto \ (4) \)
3. \( goto \ (11) \)
4. \( if \ x == p \ goto \ (6) \)
5. \( goto \ (8) \)
6. \( y = a - b \)
7. \( goto \ (2) \)
8. \( y = c - d \)
9. \( x = x + 1 \)
10. \( goto \ (2) \)
11. \( y = y + x \)

4(b) Write a short note on induction variable elimination.
Maximum Marks: 60
Credits: 04
Duration: Two Hours

Assume suitable data if missing.
Notations and symbols used have their usual meaning.

Q.No.  Question  CO  M.M.
1(a)  Answer in one word/line:
   i. What is the range of reserved port number?
   ii. Mention two important services of proxy server.

1(b)  Each swarm of traditional Bit Torrent has a centralized tracker. Discuss the
      scheme devised to decentralize the working of tracker.

1(c)  Write in short about Firewalls, its characteristics and limitations.

2(a)  Answer in one word:
   i. Name functions that are used to send and receive messages in socket
       programming.
   ii. What standard is used by SMI (Structure of Management Information)
       to encode data?

2(b)  Differentiate between Little-endian and Big-endian byte order. What byte
      order is used for network communication? Explain Value-Result
      Arguments with an example.

2(c)  Why is there no need for the IGMP message to travel outside its own
      network? Explain the concept of Reverse Path Broadcasting with an example

OR

2(c')  Explain the Multiple-byte Options available with IPv4.

3(a)  Distinguish between:
   i. Cryptography and Steganography
   ii. Avalanche Effect and Completeness Effect

   Contd......2
3(b) Explain Optimal Asymmetric Encryption Padding (OEAP). What is its benefit? (CO3) [6]

3(c) What is Cryptanalysis? Explain Playfair Cipher and Vigenere Cipher with their Cryptanalysis (CO3) [6]

OR

3(b') Explain the Data Security Services and also the Security Mechanisms required to provide those services. (CO1) [6]

3(e') Given the super increasing tuple= [7, 11, 19, 39, 79, 157, 313] r=29, and modulus n = 700, encrypt and decrypt the letter "k" using the knapsack cryptosystem. Use [4 2 5 3 1 7 6] as the permutation table. (CO4) [6]

4(a) Answer in one word/line:
   i. Two most common methods for measuring characteristics associated with fingerprints are _________ and _________. (CO1) [2+1]
   ii. Write one main difference between Digital Signature and Asymmetric Cryptosystem.

4(b) Define Kerberos and name its servers. Briefly explain the functions of each server. (CO3) [6]

4(e) What is the significance of Digital Signature? Explain the concept of Blind Signature. (CO3) [6]

OR

4(b') What is Zero-Knowledge Authentication? Explain Fiat-Shamir protocol to elaborate your answer. (CO4) [6]

4(e') Explain the role of each phase in SSL Handshake Protocol. (CO4) [6]
2018-19  
B. TECH. (AUTUMN SEMESTER) EXAMINATION  
COMPUTER ENGINEERING  
NETWORK SECURITY  
CO-445  

Maximum Marks: 60  
Credits: 04  
Duration: Two Hours  

Answer all questions.  
Assume suitable data if missing.  
Notations and symbols used have their usual meaning.

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(a)</td>
<td>What is the difference between an unconditionally secure cipher and a computationally secure cipher?</td>
<td>(CO1)</td>
<td>[05]</td>
</tr>
<tr>
<td>1(b)</td>
<td>Explain Chinese Remainder theorem and its uses in cryptography.</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
<tr>
<td>1(e)</td>
<td>DES symmetric key cryptography uses several rounds of computation. Prove that each of these rounds is reversible if the key is available, that is, if Ln+1 and Rn+1 is given, then Ln and Rn can be computed.</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
</tbody>
</table>

**OR**

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(e')</td>
<td>Using suitable diagram explain Substitute bytes Transformation of Advanced Encryption algorithm (AES)</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(a)</td>
<td>What types of attacks are addressed by message authentication?</td>
<td>(CO3)</td>
<td>[05]</td>
</tr>
<tr>
<td>2(b)</td>
<td>What is a significance of “Birthday Paradox” in estimating Collision resistance attack?</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
<tr>
<td>2(c)</td>
<td>What is a cryptographic hash function? What are four different possible uses of hash function in cryptography?</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
</tbody>
</table>

**OR**

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(e')</td>
<td>Give an example of chosen cipher text attack on RSA. Also explain the technique to counter attack such as Chosen Cipher Attack (CCA) on RSA?</td>
<td>(CO2)</td>
<td>[05]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3(a)</td>
<td>What are the properties a digital signature should have?</td>
<td>(CO3)</td>
<td>[06]</td>
</tr>
</tbody>
</table>

Contd...2.
3(b) A local area network vendor provides a key distribution facility, as illustrated in Figure below.

i. Describe the scheme shown in the figure

ii. What are the pros and cons of the scheme?

![Key distribution center diagram]

OR

3'(a) List and explain types of security services defined in the OSI security architecture

3'(b) What is a Kerberos? What problem was Kerberos designed to address?

4(a) How does a behavior-blocking software work?

4(b) In context of intrusion detection, explain the significance of the base-rate fallacy.

OR

4(b') What is an importance of “Honey-pots” in intrusion detection?

4(c) What services are provided by the SSL Record protocol?

OR

4'(c) What is S/MIME? How is a clear-signed S/MIME content type created?
Maximum Marks: 60  
Credits: 04  
Duration: Two Hours

**Answer all questions.**

*Assume suitable data if missing.*

*Notations and symbols used have their usual meaning.*

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(a)</td>
<td>Distinguish between Persistent and Non-Persistent connection.</td>
<td>(CO1)</td>
<td>[05]</td>
</tr>
<tr>
<td>1(b)</td>
<td>The distance between two stations M and N is L kilometres. All frames are K bits long. The propagation delay per kilometres is t seconds. Let R bits/second be the channel capacity. Assuming that processing delay is negligible, calculate the minimum number of bits for the sequence number field in a frame for maximum utilization, when the sliding window protocol is used.</td>
<td>(CO2)</td>
<td>[04]</td>
</tr>
<tr>
<td>1(c)</td>
<td>Describe why an application developer might choose to run an application over UDP rather than TCP.</td>
<td>(CO3)</td>
<td>[03]</td>
</tr>
<tr>
<td>1(d)</td>
<td>Why is it said that FTP sends control information &quot;out of band&quot;?</td>
<td>(CO1)</td>
<td>[03]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(a)</td>
<td>Briefly describe the structure of a TCP segment.</td>
<td>(CO1)</td>
<td>[07]</td>
</tr>
</tbody>
</table>

**OR**

<table>
<thead>
<tr>
<th>Q.No.</th>
<th>Question</th>
<th>CO</th>
<th>M.M.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(a')</td>
<td>List the characteristics of selective repeat protocol. What is the size of window used? Give the validation of window size in selective repeat protocol.</td>
<td>(CO4)</td>
<td>[07]</td>
</tr>
<tr>
<td>2(b)</td>
<td>A 20 Kbps satellite link has a propagation delay of 400 ms. The transmitter employs the &quot;go back n ARQ&quot; scheme with n set to 10. Assuming that each</td>
<td>(CO2)</td>
<td>[04]</td>
</tr>
</tbody>
</table>

[Contd... 2]
frame is 100 byte long, what is the maximum data rate possible?

2(c) Suppose that the five measured SampleRTT values are 106 ms, 120 ms, 140 ms. Compute the EstimatedRTT after each of these SampleRTT values is obtained, using a value of $\alpha = 0.125$ and assuming that the value of EstimatedRTT was 100 ms just before the first of these three samples were obtained. Compute also the DevRTT after each sample is obtained, assuming a value of $\beta = 0.25$ and assuming the value of DevRTT was 5 ms just before the first of these three samples was obtained. Last, compute the TCP TimeoutInterval after each of these samples is obtained.

3(a) Give a brief overview of the components of a router. Consider sending a 2600-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 400. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?

3(b) i) Consider the network shown below, and assume that each node initially knows the costs to each of its neighbours. Consider the distance-vector algorithm and show the distance table entries at node b.

![Network diagram]

ii) A router has just received the following new IP addresses: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21, and 57.6.120.0/21. If all of them use the same outgoing line, can they be aggregated? If so, to what? If not, why not?

OR

...
3(b') i) Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses that satisfy these constraints.

ii) A router has the following (CIDR) entries in its routing table:

<table>
<thead>
<tr>
<th>Address/mask</th>
<th>Next hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>135.46.56.0/22</td>
<td>Interface 0</td>
</tr>
<tr>
<td>135.46.60.0/22</td>
<td>Interface 1</td>
</tr>
<tr>
<td>192.53.40.0/23</td>
<td>Router 1</td>
</tr>
<tr>
<td>default</td>
<td>Router 2</td>
</tr>
</tbody>
</table>

For each of the following IP addresses, what does the router do if a packet with that address arrives?

(a) 135.46.63.10 (b) 135.46.57.14 (c) 135.46.52.2 (d) 192.53.40.7

(e) 192.53.56.7  (f) 192.53.42.1

4(a) i) Given the value of CRC generator as 10011, obtain CRC code word for the data bit sequence 1101011111.

ii) The round trip propagation delay for a 20 Mbps Ethernet having 48 bit jamming signal is 46.4 µs. What would be the minimum frame size?

OR

4(a') Derive the mathematical expression for efficiency of CSMA/CD.

4(b) i) What is DHCP? How does it work?

ii) Explain capture effect in Ethernet's exponential backoff algorithm?
B. TECH. (AUTUMN SEMESTER) EXAMINATION
COMPUTER ENGINEERING
PRINCIPLES OF MACHINE LEARNING
CO-461

Maximum Marks: 60
Credits: 04
Duration: Two Hours

Answer all questions.
Assume suitable data if missing.
Notations and symbols used have their usual meaning.

Q.No. Question CO M.M.
(a) Why machine learning has become possible in recent times? (CO1) [2] 
(b) List and discuss different types of machine learning? (CO1) [7] 
(c) If we want to apply machine learning for real world problems, what are the different things we should look upon? Explain clearly. (CO1) [6] 

2(a) Consider the training dataset given below. A, B, and C are the attributes and Y is the class variable.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Can you draw a decision tree having 100% accuracy on this training set? If your answer is yes, draw the decision tree. If your answer is no, explain why? Which attribute among A, B and C has the highest information gain? Explain your answer. (CO2) [6]

OR

2(a') Suppose that we want to build a neural network that classifies two dimensional data (i.e., \(X = [x_1, x_2]\)) into two classes: diamonds and crosses.
We have a set of training data that is plotted as follows: Draw a network that can solve this classification problem. Justify your choice of the number of nodes and the architecture.

2(b) What is bagging? Discuss different steps of bagging.

OR

2(b') What do you mean by boosting? Explain clearly the intuition behind boosting.

2(c) Why neural network learning is called connectionist learning? What is perceptron? Discuss different limitations of perceptrons. State the Perceptron convergence theorem and Perceptron cycling theorem.

OR

2(c') List and discuss different steps of Backpropagation algorithm used to train multi-layer feed forward neural networks.

3(a) What do you mean by Markov Decision Process (MDP)? List different ways to define a MDP structure.

OR

3(a') What is Linear Quadratic Regulator (LQR)? Explain clearly.

3(b) What is Q-learning? Discuss its different steps with the help of a suitable example.

OR

3(b') What is value function approximation? How we can perform value function approximation by linear combination of features? Discuss different steps of Temporal Difference (TD) based reinforcement learning for linear

continued...
3(c) What is factor analysis? List different steps of factor analysis. What are the problems with factor analysis? [6]

OR

3(c') What is Principal Component Analysis (PCA)? List different steps of PCA with the help of a suitable example. (CO3) [6]

4(a) What is deep learning? How it is different from traditional multi-layer networks learning? What is vanishing gradient problem? In what way, the Long Short Term Memory (LSTM) networks can combat this problem? Explain clearly. (CO4) [8]

4(b) What is visual question answering? Draw the architecture of the deep learning system used for visual question answering and discuss. (CO4) [7]