**AKTC KALSEKAR TECHNICAL CAMPUS**

INNOVATIVE TEACHING   EXUBERANT LEARNING

*Knowledge Resource & Relay Centre (KRRC)*

AIKTC/KRRC/SoET/ACKN/QUES/2018-19/      Date: _____

School: <u>SoET-CBSGS</u>    Branch: <u>COMP. ENGG.</u>   SEM: <u>VII</u>

To,
**Exam Controller,**
**AIKTC, New Panvel.**

Dear Sir/Madam,

Received with thanks the following **Semester/Unit Test-I/Unit Test-II (Reg./ATKT)** question papers from your exam cell:

| Sr. No. | Subject Name | Subject Code | Format | | No. of Copies |
|---|---|---|---|---|---|
| | | | SC | HC | |
| 1 | Digital Signal Processing | CPC701 | | | |
| 2 | Cryptography and System Security | CPC702 | | ✓ | 02 |
| 3 | Artificial Intelligence | CPC703 | | ✓ | 02 |
| 4 | Elective-II ERP & Supply Chain mgmt | CPE7042X | | ✓ | 02 |
| 5 | | | | | |
| 6 | | | | | |
| | | | | | |
| | | | | | |

Note: SC – Softcopy, HC - Hardcopy

(Shaheen Ansari)
**Librarian, AIKTC**

B2 - sem - VII - USGS - LU Migr

13/5/19

**(3 hours)**　　　　　　　　　　　　　　　　**Marks:[80]**

**N.B**
1. Question No. 1 is compulsory.
2. Attempt any 3 out of remaining 5.

Q.1   a) Explain the different software flaws with example.　　　　　05
       b) Define goals of security and mechanism to achieve them.　　　05
       c) Define the properties and applications of Hash function.　　　05
       d) Explain handshake protocol in SSL.　　　　　　　　　　05

Q.2   a) How is security achieved in Transport and Tunnel modes of IPSEC?　10
       Explain the role of AH and ESP.

       b) How does PGP achieve confidentiality and authentication in emails?　10

Q.3   a) Why are digital certificates and signatures required? What is role of　10
       digital signature in digital certificates? Explain any one digital signature
       algorithm.

       b) What are the different components of Intrusion Detection System?　10
       Compare signature based IDS to anomaly based IDS.

Q.4   a) Discuss DES with reference to following points　　　　　　10
- Block size and key size
- need of expansion permutation
- role of S-box
- weak keys and semi weak keys
- possible attacks on DES

       b) Explain Diffie Hellman key exchange algorithm. What types of attacks　10
       are possible on it explain with example.

Q.5   a) Explain briefly the following attacks with example　　　　　10
        (I) Session hijacking　　　　(II) Salami Attack
        (III) SQL injection　　　　　(IV) Buffer overflow

       b) What is Denial of Service attack? What are the different ways in which　10
       an attacker can mount a DOS attack on a system?

Q.6   a) Explain the working of Kerberos.　　　　　　　　　　10

       b) Elaborate the steps of key generation using RSA algorithm. In RSA　10
       system the public key (E, N) of user A is defined as (7,187). Calculate
       $\Phi(N)$ and private key 'D'. What is the cipher text for M=10 using the public
       key.

Time: 3 Hours
Total Marks = 80

Note:
(i) Each question carries 20 marks
(ii) **Question 1** is compulsory
(iii) Attempt any **three (3)** from the remaining questions
(iv) Assume suitable data wherever required

Q1.    Attempt any **four (4)** questions from the following:                              [20]
(a) Compare Model based agent with Goal based agent.
(b) Given a full 5-gallon jug and an empty 3- gallon jug, the goal is to fill the 3-gallon jug with exactly one gallon of water. Give state space representation
(c) Explain conditional independence relation in belief network with example
(d) Describe the environmental characteristics of WUMPUS world Puzzle.
(e) What is Supervised and Unsupervised learning? Give example of each.

Q2 (a) Draw and illustrate the Architecture of Learning agent. Describe each of its   [6+4]
component w.r.t. Medical diagnosis system
(b) Distinguish between Propositional logic (PL) and first order predicate logic   [10]
(FOPL) knowledge representation mechanisms. Take suitable example for each
point of differentiation.

Q3 (a) Consider the following set of sentences                                          [10]

a) Whoever can read is literate
b) Birds are not literate
c) Some birds are intelligent

Prove the following using forward reasoning "**Some who are intelligent
cannot read**"

(b) Evaluate **IDA\* search** algorithms based on performance measures such as   [6+4]
Complete, Optimal, Time and Space complexity with justification. Illustrate its
working with a suitable example.

Q4 (a) Apply Alpha-Beta Pruning on following example                                    [10]

006FBA1142B8E6298C01453C5045D4ED
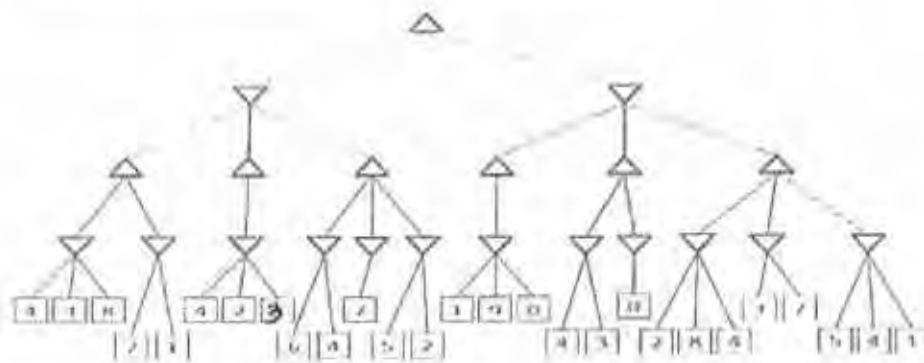
(b) Define Belief Network. Describe the steps of constructing belief network with an example. What types of inferences can be drawn from that?  [2+6+2]

Q5 (a) Explain Partial order planning with example.  [10]

(b) Describe each component in the architecture of Expert System? What are the limitations of Expert System?  [10]

Q6 Answer any **two (2)** of the following  [20]

(a) Construct the decision tree from the following set of training data. Classify the new record: outlook=rain, temp =70, humidity=65, windy=true.

| Tid | Refund | Marital Status | Taxable Income | Cheat |
|---|---|---|---|---|
| 1 | Yes | Single | >100 | No |
| 2 | No | Married | 80-100 | No |
| 3 | No | Single | <80 | No |
| 4 | Yes | Married | >100 | No |
| 5 | No | Divorced | 80-100 | Yes |
| 6 | No | Married | <80 | No |
| 7 | Yes | Divorced | >100 | No |
| 8 | No | Single | 80-100 | Yes |
| 9 | No | Married | <80 | No |
| 10 | No | Single | 80-100 | Yes |

(b) What are steps involved in natural language processing (NLP) of an English sentence? Explain with an example sentence.

(c) Write a short note on local search algorithms.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

006FBA1142B8E6298C61453C5045D4ED

Time: 3 Hours                                                    Marks: 80

N.B.    (1) Question 1 is compulsory.
        (2) Solve any three questions from the remaining

| Q1 | a | List and explain various ERP technologies, also state where it is used. | [10] |
|---|---|---|---|
|    | b | Explain the major drivers of Supply chain | [10] |

| Q2 | a | Draw and explain the implementation lifecycle of an ERP system | [10] |
|---|---|---|---|
|    | b | Explain Electronic Data Interchange (EDI) and its benefit | [10] |

| Q3 | a | How is BPR connected with ERP explain | [10] |
|---|---|---|---|
|    | b | What do you mean by bill of material? Explain with an example | [10] |

| Q4 | a | Explain SCOR Model | [10] |
|---|---|---|---|
|    | b | Explain the strategy used by these Mumbai Dabbawallas and also what can larger organization with many more resources learn from this simplistic system? | [10] |

| Q5 | a | How ERP helps in better decision making in a company | [10] |
|---|---|---|---|
|    | b | Explain the characteristics of Agile Supply Chain | [10] |

| Q6 |  | Explain (Any Two) |  |
|---|---|---|---|
|    | a | Sales and Distribution business module of an ERP | [10] |
|    | b | Strategic decision in SCM | [10] |
|    | c | Enterprise Application Integration | [10] |
|    | d | Make Vs Buy Model | [10] |

---

32D6CAE73823A2A9FE2C2E7C159A927E