(Set-A_1)

B.Tech-5th (CS & IT)

Cryptography and Network Security

Full Marks : 70

Time : 3 hours

Answer six questions including **Q.No.1** which is compulsory.

The figures in the right-hand margin indicate marks.

Symbols carry usual meaning.

1. Answer *all* questions : 2×10

   (*a*) Find the result of following operations :
   (*i*) –78 mode 13
   (*ii*) 22 mod 7

   (*b*) List all multiplicative inverse pairs in modulus 20.

   (*c*) Find the multiplicative inverse of 132 in Z_{180} using the Extended Euclidean algorithm.

   (*d*) What is One-time pad ? Who has invented one-time pad ?

(e) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key.

(f) Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.

(g) Define an S-box and mention the necessary condition for an S-box to be invertible.

(h) What is the block size in DES ? What is the cipher key size in DES ?

(i) What is Euler's totient function ?

(j) Distinguish between a session and connection with respect to SSL protocol.

2. (a) What is cryptanalyis ? What are the four common cryptanalysis attacks ? Explain them with block diagrams. 5

(b) Distinguish between diffusion and confusion properties of block cipher. Explain the working of a product cipher made of two rounds and show how the above properties are achieved in it. 5

(Continued)

3. (*a*) Distinguish between symmetric key and asymmetric key cryptography. Define a trap-door one-way function and explain its use in an asymmetric-key cryptography. 5

(*b*) Compare and contrast a conventional signature and a digital signature. Explain the Elgamal digital signature scheme. 5

4. (*a*) Using the RSA scheme, let $p = 809$, $q = 751$, and $d = 23$. Calculate the public key e. Then sign and verify the mesage with $M = 100$. 5

(*b*) List and explain the security services provided by a digital signature. State the attacks possible on a digital signature. Differentiate between existential forgery and selective forgery on a digital signature. 5

5. (*a*) Define the Diffie-Hellman protocol and its purpose. Explain the man-in-the middle attack in D-H protocol. 5

(*b*) Compare and contrast the Handshake and Record protocols in SSL and TLS. 5

6. (*a*) A Public-Key Infrastructure (PKI) is essential for large-scale applications of public-key cryptography. Name three checks (or verifications) that ought to be performed by the recipient of a digital certificate. What is a CRL (Certificate Revocation List) and why is it necessary ? 5

(*b*) What is the need of modes of operation in modern symmetric key ciphres like DES and AES ? Describe the five modes of operation of the modern block ciphers. 5

7. (*a*) Differentiate between differential cryptanalysis and linear cryptanalysis. What is the block size in Blowfish and IDEA ? What is triple DES ? 5

(*b*) Use the Vigenere cipher with keyword 'HEALTH' to encipher the message 'Life is full of surprises'. 5

8. Write short notes on any *two* : 5 × 2

(*a*) Electronic Money

(*b*) Kerberos

(*c*) S/MIME

(*d*) Pretty Good Privacy.

B. Tech- 5 (CS & IT)

Microprocessors & Microcontrollers

Full Marks : 70

Time : 3 hours

Answer any six questions including **Q.No.1** which is compulsory.

The figures in the right-hand margin indicate marks

Symbols carry usual meaning

1. Answer *all* questions : 2×10

(*a*) Write the types of different operands in an instruction with one example for each.

(*b*) Differentiate between serial and parallel transmission.

(*c*) What is PSW in microprocessor 8085 ?

(*d*) Distinguish between RAR and RRC instruction in 8085.

(*e*) Write at least two differences between 8085 and 8051.

(*f*) What is a vectored interrupt program ?

(Turn Over)

(g) Give an application where microcontroller is preferred over a microprocessor.

(h) How to resolve conflicts on arrival of interrupts RST 7.5, RST 6.5 and RST 5.5.

(i) Which hardware devices in microprocessor 8086 allow a 2- stage pipeline ?

(j) What do you mean by assembler directive ? Write at least two assembler directives.

2. (a) Write a program in assembly language of 8085 to sort 10 numbers stored at memory location 2050H. 5

(b) Write a program in assembly language 8085 to obtain 25 microsecond delay. Compute the total space in bytes required for the above program in Q2 (a) 5

3. (a) Explain the difference between SRAM and DRAM. What are the merits and demerits of DRAM? refreshing 5

(b) Interface a 8K × 8 ROM and 8K × 8 RAM to microprocessor 8085 so that the starting address of ROM in 0000H whereas the starting address of RAM is 8000H. Write the connection diagram and memory map assuming the IC of size 4K × 4 are available for both RAM and ROM. 5

4. (*a*) How many types of interrupts are available in 8085 ? Computer the vector address of each type of interrupt. How these interrupts are different from the interrupt of 8086 ? 5

   (*b*) Explain the purpose of each bit position of operation command words of PIC 8259. 5

5. (*a*) Draw the schematic block diagram of microprocessor 8086. Explain the maximum mode signals. 5

   (*b*) What is the role of 8288 bus controller ? Draw the block diagram of 8288 bus controller. 5

6. (*a*) What are the main characteristics of microcontroller 8051 ? Explain the difference between 8051 microcontroller and 8085 microprocessor. 5

   (*b*) What is the need of multiplexing ? Discuss the advantages and disadvantages of multiplexing. 5

7. (*a*) Explain the interrupt structure of microcontroller 8051 with examples. 5

   (*b*) Write the different regions of address space available in microcontroller 8051. 5

8. (*a*) Specify the name of timers in microcontroller 8051. Explain how these timers can be programmed. 5

(*b*) Explain the functions of each bit of SCON and PCON registers. 5

(Set-A_1)

B.Tech-5th (CS & IT)

Graph Theory

Full Marks : 70

Time : 3 hours

Answer six questions including Q.No.1 which is compulsory.

The figures in the right-hand margin indicate marks.

Symbols carry usual meaning.

1. Answer *all* questions : 2 × 10

(*a*) Define maximal matching in a graph. Explain it by taking suitable example.

(*b*) Let G be a complete undirected graph on 6 vertices. If vertices of G are labelled, then calculate the number of distinct cycles of length 4 in G.

(*c*) Define the following terms with example :
(*i*) Path, (*ii*) Walk.

(*d*) Let G be a simple undirected planar graph on 12 vertices with 16 edges. If G is a connected graph, then calculate the number of bounded faces in any embedding of G on the plane.

(*Turn Over*)

(e) Compute the diameter and radius of the complete bipartite graph $K_{m,n}$.

(f) Find the Adjacency matrix and Incident matrix of a graph by taking suitable example.

(g) What is the chromatic number of an n-vertex simple connected graph which does not contain any odd length cycle ? Assume $n \geq 2$.
(i) 2, (ii) 3, (iii) $n-1$, (iv) n.

(h) What do you mean by clique of a graph ?

(i) Define a Hamiltonian path. Find an example of a non-Hamiltonian graph with a Hamiltonian path.

(j) Prove that a simple graph with n vertices and k components can have at most $(n-k)(n-k+1)/2$ edges.

2. (a) Prove that a graph X is isomorphic to graph Y, if there exist an isomorphism from X to Y. 5

(b) Which of the following are graphic sequences ? Provide a construction or a proof of impossibility for each.

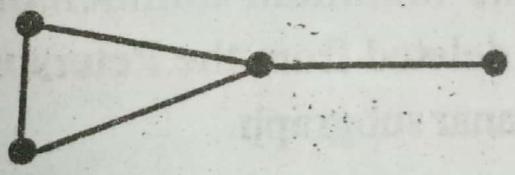
(*i*) (5,5,4,3,2,2,2,1)

(*ii*) (5,5,4,4,2,2,1,1)

(*iii*) (5,5,5,3,2,2,1,1)

(*iv*) (5,5,5,4,2,1,1,1) 5

3. (*a*) In a graph below, find all the maximal paths, maximal cliques, and maximal independent sets. Also find all the maximum paths, maximum cliques, and maximum independent sets. 5



(*b*) Prove that every loopless graph G has a bipartite subgraph with at least $e(G)/2$ edges. 5

4. (*a*) Prove that every 3-regular graph with no cut-edge has a 1-factor. 5

(*b*) Prove that if G is a bipartite graph, then the maximum size of a matching in G equals the minimum size of a vertex cover of G. 5

5. (*a*) If a connected plane graph G has exactly n vertices, e edges, and f faces, then $n - e + f = 2$. Prove it. 5

(Continued)

(*b*) Prove that Brooks' theorem is equivalent to the following statement : every $k-1$ regular k-critical graph is a complete graph or an odd cycle. 5

6. (*a*) Every 3-connected graph G with at least five vertices has an edge e such that Ge is 3-connected. Prove it. 5

(*b*) Determine the minimum number of edges that must be deleted from the Peterson graph to obtain a planar subgraph. 5

7. (*a*) Prove that a simple 2-edge-connected 3-regular plane graph is 3-edge-colorable if and only if it is 4-face-colorable. 5

(*b*) Prove that every Hamiltonian 3-regular graph has a Tait coloring. 5

8. (*a*) A graph G having at least three vertices is 2-connected if and only if for each pair $u, v \in V(G)$ there exist internally disjoint u,v-paths in G. 5

(b) There are five cities in a network. The travel time for travelling directly from i to j is the entry $a_{i,j}$ in the matrix below. The matrix is not symmetric (use directed graphs), and $a_{i,j} = \infty$ indicates that there is no direct route. Determine the least travel time and quickest route from i to j for each pair i, j. 5

$$\begin{pmatrix} 0 & 10 & 20 & \infty & 17 \\ 7 & 0 & 5 & 22 & 33 \\ 14 & 13 & 0 & 15 & 270 \\ 30 & \infty & 17 & 0 & 10 \\ \infty & 15 & 12 & 8 & 0 \end{pmatrix}$$

(Set-A_1)

B. Tech- 5 (CS & IT)
Software Engineering And OOAD

Full Marks : 70

Time : 3 hours

Answer any **six** questions including **Q.No.1** which is compulsory.

The figures in the right-hand margin indicate marks

Symbols carry usual meaning

1. For each of the following questions only one of the options is correct. Choose the correct option.

Answer *all* questions : 2×10

(*a*) Why is writing easily modifiable code important?

(*i*) Easily modifiable code results in quicker run time.

(*ii*) Most real world programs require change at some point of time or other.

(*iii*) Most text editors make it mandatory to write modifiable code.

(*iv*) Several people may be writing different parts of code at the same time.

(*b*) Which of the following is the principle reason for developing a prototype ?

(*i*) It can be used as an early production tool.

(*ii*) It may solve a problem that is not included in the requirements.

(*iii*) It allows the customer to provide feedback about requirements.

(*iv*) It reduces the schedule for development through alpha testing.

(*c*) Which one of the following statements is implicitly assumed by the COCOMO model ?

(*i*) Cost is the most fundamental attribute of a software product, based on which the project size and duration are estimated.

(*ii*) Size is the most fundamental attribute of a software product, based on which the project cost and duration are estimated.

(*iii*) Effort is the most fundamental attribute of a software product, based on which the project size and cost are estimated.

(*iv*) Duration is the most fundamental attribute of a software product, based on which the project size and effort are estimated.

(*d*) A software requirements specification (SRS) document should avoid discussing which one of the following ?

(*i*) Functional requirements

(*ii*) Non-functional requirements

(*iii*) Design specification

(*iv*) Constraints on the implementation

(*e*) Which one of the following is not a goal of requirements analysis ?

(*i*) Weed out ambiguities in the requirements

(*ii*) Weed out inconsistencies in the requirements

(*iii*) Weed out non-functional requirements

(*iv*) Weed out incompleteness in the requirements

(*f*) The modules in a good software design should have which of the following characteristics :

(*i*) High cohesion, low coupling

(*ii*) Low cohesion, high coupling

(*iii*) Low cohesion, low coupling

(*iv*) High cohesion, high coupling

(*g*) In a procedural design approach, during the detailed design stage, which of the following is undertaken ?

(*i*) Module structure is designed

(*ii*) Data flow representation is developed

(*iii*) Data structures and algorithms for the individual modules are developed

(*iv*) Structure chart is developed

(*h*) Consider the statement: 'An employee is either a worker or a manager.' Assuming that Employee and Manager to be two classes, what can be said about the relationship between these two classes ?

(*i*) Association

(*ii*) Generalization-specialization

(*iii*) Containment

(*iv*) Polymorphism

(*i*) Which of the following can be considered to provide the most accurate measure of the size of a user interface:

(*i*) LOC of the GUI components

(*ii*) Number of scenarios

(*iii*) Number of windows

(*iv*) Sizes of input and output data

(*j*) If branch coverage has been achieved on a unit under test, which one of the following is coverage is implicitly implied ?

(*i*) Path coverage

(*ii*) Multiple condition coverage

(*iii*) Statement coverage

(*iv*) Data flow coverage

2. (*a*) Identify five reasons as to why the customer requirements may change after the requirements phase is complete and the SRS document has been signed off. 5

(*b*) Schedule slippage is a very common form of risk that almost every project manager has to encounter. Explain in 3 to 4 sentences how you would manage the risk of schedule slippage as the project manager of a medium-sized project. 5

3. (*a*) At which point in a waterfall-based software development life cycle (SDLC), does the project management activities start ? When do these end ? Identify the important project management activities. 5

(*b*) Draw a class diagram using the UML syntax to represent the fact that the fleet of vehicles at a travel agency consists of vehicles of the types Tata Indica, Maruti van, and Mahindra Xylo. The regular customers of the travel agency can rent any vehicle they want. The details of the customers such as the name, address, and phone number are maintained by the agency in a customer register. 5

4. (*a*) What are the different types of relationships that might exist among the classes in an object-oriented design ? Give examples of each. 5

(*b*) What do you understand by coding standard ?

(*i*) When during the development process is the compliance with coding standards is checked ?

(*ii*) List two coding standards each for (*i*) enhancing readability of the code, (*ii*) reuse of the code, (*iii*)enhancing code maintainability. 2 + 1 + 2

5. (*a*) Distiguish between software verification and software validation. Can one be used in place of the other ? Justify your answer. In which phase (s) of the iterative waterfall SDLC are the verification activities performed and in which phase (s) are the validation activities performed ? 5

(*b*) Design the black- box test suite for a function named quadratic-solver. The quadratic-solver function accepts three floating point numbers (*a, b, c*) representing a quadratic equation of the form $ax^2+bx+c=0$. It computes and displays the solution. 5

6. (*a*) What is statistical testing ? In what way is it useful during software development ? Explain in the different steps of statistical testing. Identify the main difficulties in performing satisfactory statistical testing. 5

(*b*) What are the different quality levels the SEI CMM ? What do you understand by Key Process Area (KPA), in the context of SEI CMM ? Identify the KPAs for any one level of your choice. 5

(Set-A_1)

B.Tech-5th (CS & IT)

Operating System

Full Marks : 70

Time : 3 hours

Answer six questions including Q.No.1 which is compulsory.

The figures in the right-hand margin indicate marks.

Symbols carry usual meaning.

1. Answer *all* questions : 2 × 10

(*a*) In priority scheduling a priority number is associated with each process. The CPU is allocated to the process with the highest priority (smallest integer is of highest priority). The problem of starvation is resolved by :

(*i*) Terminating the process

(*ii*) Aging

(*iii*) Mutual Exclusion

(*iv*) Semaphore

Justify your answer.

(b) Explain the difference between deadlock prevention and deadlock avoidance.

(c) How the clone ( ) operation supported by Linux is used to support both processes and threads.

(d) What are the advantages and disadvantages of supporting memory mapped I/O to device control registers ?

(e) State the differences between process and thread.

(f) Consider a machine with 64 MB physical memory and a 32-bit virtual address space. If the page size is 4 KB, what is the approximate size of the page table ?

(g) What is Kernel I/O ?

(h) What do you mean by the term 'Thrashing' ?

(i) What is the merit and demerit of segmentation ?

(j) Define lazy swapper. State its use.

2. Write down the main services of an operating system ? State the essential properties of the following types of operating systems :

(*i*) Batch

(*ii*) Interactive

(*iii*) Time sharing

(*iv*) Real time

(*v*) Distributed. 10

3. (*a*) What is the purpose of scheduling ? Explain scheduling as the basis of multiprogramming. 4

(*b*) Consider the following snapshot of a system :

	Allocation			Max			Available		
	A	B	C	A	B	C	A	B	C
P0	0	1	0	7	5	3	3	3	2
P1	2	0	0	3	2	2			
P2	3	0	2	9	0	2			
P3	2	1	1	2	2	2			
P4	0	0	2	4	3	3			

Answer the following questions using the Banker's algorithm :

(*i*) What is the content of the matrix need ?

(*ii*) Is the system in a safe state ?

(*iii*) If a request from process P1 arrivs for (1, 0, 2), can the request be granted immediately ?

(*iv*) If a request from process P4 arrives for (3, 3, 0), can the request be granted immediatly ?

(*v*) If a request from process P0 arrives for (0, 2, 0), can the request be granted immediately ? 6

4. (*a*) Consider the following set of processes with length of CPU burst time given in millisecs : 6

Process	burst time	priority
P2	10	3
P0	1	1
P7	2	3
P1	1	4
P9	5	2

The processes are assumed to have arrived in the order P2 P0 P7 P1 P9 all at time zero. Draw Gantt chart illustrating execution of these processes using SJF and also find its turnaround time.

(*b*) Let m[0].....m[4] be mutexes (binary semaphores) and p[0].....p[4] be processes. Suppose each process p[i] executes the following :

wait (m[i]); wait(m[(i + 1) mod 4]);

.....

.....

release (m[i]); release (m[(i + 1) mod 4]);

Could this cause *thrashing* or *starvation* or *deadlock* ? Identify and explain your answer. 4

5. Differentiate between the following terms : 2.5×4

(*i*) Short-term scheduler and Long-term scheduler

(*ii*) External fragmentation and internal fragmentation

(*iii*) System call and Cooperating process

(*iv*) Paging and Segmentation.

6. (*a*) Discuss the components of LINUX operating system with a neat diagram. 4

(*b*) Consider the following page reference string :

1, 2, 3, 4, 2, 1, 5, 6, 2, 1, 2, 3, 7, 6, 3, 2, 1, 2, 3, 6.

How many page faults would occur for the following replacement algorithms for taking one, two, three frames ? (Remember all frames are initially empty, so your first unique pages will all cost one fault each.

(*i*) LRU replacement
(*ii*) FIFO replacement
(*iii*) Optimal replacement.

Which one is the better algorithm ? Justify your answer. 6

7. (*a*) Explain the Dining Philosophers problem using semaphore. 5

(*b*) Explain different file access methods with its recovery techniques. 5

8. Write short notes on any *two* : 5 × 2

(*a*) Inter process communication

(*b*) Disk reliability and management

(*c*) Window NT

(*d*) Virtual Memory.