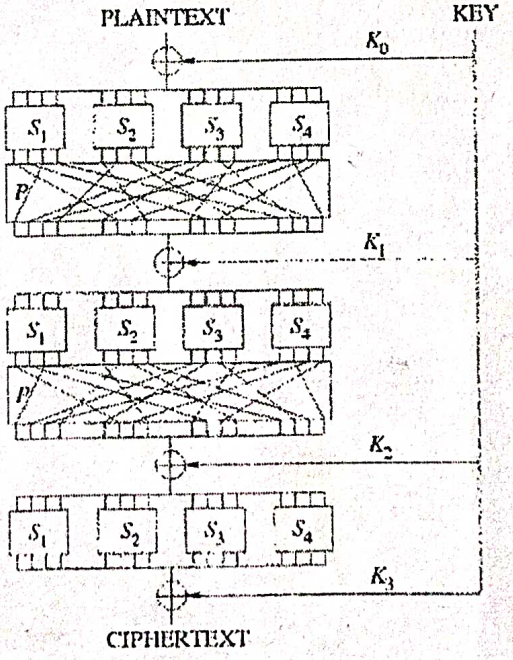
Indian Institute of Engineering Science and Technology
Department of Information Technology

B.Tech (IT) 7th Semester Mid Semester Examinations, September 2022
Information and Systems Security (IT-4101)

Full Marks: 30 Time: 2 hours

Attempt ALL questions

Q.No.	Particulars	Marks
1.	(a) Does inverse of 21 exist in Z_{100}? If yes, calculate 21^{-1} *mod* 100, showing each step of calculation clearly. If not, justify why. (b) Derive the key space of the following cipher, designed for an alphabet with 15 letters: $T = (P \times k_1) \bmod 15$ $C = (T + k_2) \bmod 15$ where P,C belong to Z_{15} represent the plaintext and ciphertext, respectively, and (k_1, k_2) represents the key.	5×2=10
2.	(a) Draw a block diagram to demonstrate the Data Encryption Standard (DES) encryption process. In a separate figure, draw details of the DES Round Function showing its components clearly. (b) Let $DES(P,K)$ represent the Data Encryption Standard (DES) encryption of plaintext P with key K. Prove that $DES(P,K) = DES(\overline{P},\overline{K})$.	5×2=10
3.	Following is a *Substitution Permutation Network* (SPN), which is a mathematical model used in modern day block cipher algorithms:  Comment on the followings: (a) Degree of *Diffusion* achieved by the above cipher, after every round. (b) Degree of *Confusion* achieved by the above cipher, after every round.	5×2=10

****

Indian Institute of Engineering Science and Technology, Shibpur

B.Tech (IT) 7th Semester End Semester Examinations, 2022
Information and Systems Security (IT-4101)

Full Marks: 50 **Time: 3 Hours**

Attempt ANY FIVE questions

1. (a) State the RSA parameters generation algorithm. How are the parameters used for encryption and decryption?
(b) Prove that the possibility of factorization of large numbers will compromise the security of RSA encryption.

[5×2=10]

2. (a) Describe the idea of the Markle-Damgard scheme and explain why this idea is important for the design of a cryptographic hash function?
(b) Suppose a person uses RSA to digitally sign a document D where he actually signs the MD4 digest of D, and not D itself. Given: $|D| < 448$. Justify how the MD4 digest helps to make this system more secure against "chosen message attack", as compared to another system, whereby D itself is digitally signed using RSA, without the involvement of any hash function.

[5×2=10]

3. Using the RSA digital signature scheme, where p=809, q=751, and d=23, do the following:
(i) Calculate the public key e.
(ii) Sign and verify the message M1 = 100. Call the signature S1.
(iii) Sign and verify the message with M2 = 50. Call the signature S2.
(iv) Show that if M = M1×M2 = 5000, then S = S1×S2.

[10]

4. (a) Prove the following w.r.t. Cipher Block Chaining (CBC) mode of modern block ciphers, with the help of a diagram:
"A single bit error in ciphertext block C(j) during transmission is propagated to a single bit in plaintext block P(j+1) but multiple bits in P(j), at the decryption site."
(b) Encrypt the text "meetatfour" using Playfair cipher with the following secret key:

L	G	D	B	A
Q	M	H	E	C
U	R	N	I	F
X	V	S	O	K
Z	Y	W	T	P

Is the above cipher a monoalphabetic or polyalphabetic cipher? Why?

[5×2=10]

5. Prove that, given hash length of 2^n bits, the minimum number of queries (q) required to succeed in preimage attack against a cryptographic hash function with a success probability of at least ½ is approximately 0.69×2^n.

[10]

6. Prove that, given hash length of 2^n bits, the minimum number of queries (q) required to succeed in collision attack against a cryptographic hash function with a success probability of at least ½ is approximately $O(2^{n/2})$.

[10]

****

Indian Institute of Engineering Science and Technology, Shibpur

B.Tech. (IT) 7th Semester Final Examination 2022

INTERNET TECHNOLOGY (IT 4102)

Full Marks: 50 **Time: 3 hours**

Answer any five questions. Each question carries 10 marks

1. Explain the three phases of simple mail transfer protocol using a proper diagram. Explain with a sequence diagram shows how the POP3 protocol pull the mail from the server? Explain the working principle of a web crawler. [4+3+3]
2. Explain a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). Explain with a proper diagram how the two processes transfer data between themselves in the Internet following OSI seven-layer architecture. [5+5]
3. What is a port number? Explain the socket address. What is the difference between the User Datagram Protocol and Transmission Control Protocol? [2+2+6]
4. Explain the little-endian and big-endian byte ordering. Explain the following functions:
   a. int inet_aton(const char *strptr, struct in_addr *addrptr);
   b. char *inet_ntoa(struct in_addr inaddr);
   c. const char *inet_ntop(int af, const void *restrict src, char *restrict dst, socklen_t size);
   [5+5]
5. What is the role of the root server, primary server and secondary server in domain name systems? Explain the iterative and recursive name to address the resolution technique with a diagram. [5+5]
6. How will a system retrieve its IP address through the DHCP protocol? Explain with DHCP state diagram. Write down some of the benefits of JavaScript to make the website. [6+4]

Indian Institute of Engineering Science and Technology, Shibpur
B.Tech. 7th Semester Mid-term Examination 2022
Internet Technology IT 4102

Time: 2 hours Full Marks: 30

1. Explain the concept of sub-netting and super-netting with a suitable example. [6]
2. What is the port number? Discuss different types of port numbers. What is a cyclic redundancy check? [2+2+2]
3. Discuss the root server in the domain name system tree. Explain different types of names to IP address resolving techniques. [2+4]
4. Discuss ARP and RARP; where does it work? [3+3]
5. In socket programming, how the client socket and the server socket will establish reliable communication explain with a suitable example. [6]

B.Tech/ B Arch 4th Year 7th Semester(AE/MET/CST/ETC/IT/EE/ARCH)

Mid Term Examination Sept'22

FINANCE ECONOMICS &MANAGEMENT for Engineers(HSS III)(HU - 4101)

FullMarks:30 (Start writing Answers for each Module from a separate page) Time:2hours

Module I

Finance

I. What do you understand by the Term Cost? (2)

II. Explain Element wise classification of cost
Or Functional Classification cost. (3)

III . From the given data, calculate only Works Overheads :

Items	Rs
Direct Materials	10,00,000/
Direct Wages	2,00,000/
Indirect Materials	60,000/
Indirect Wages	1,00,000/
Advertisement	50,000/
Rent:	
Office	1,15,000/
Factory	75,0000/
Lighting	88,0000/
(50% for Factory)	
Power	60,000/
Depreciation of Plant	1,15,500/
Salary of Works Manager	95,000/
Lubricant	10,000/
Factory Guards Salary	30,000/
Salary of Administrative staff	80,000/
Insurance of Plant	25,000/

(5)

##########

Module II

ECONOMICS

A. The supply and demand functions are given below. Determine which one among these equations is the equation of supply and which one is the equation of demand and explain with logic. Find the equilibrium price (in Rs) and quantity (in Kgs). (4)

P= -2Q+100 and P=3Q-30

B. What are the assumptions of cardinal utility analysis? (3)

C. As a result of a 10% increase in the income of a consumer, its demand rises from 200 to 240 units. Find out the income elasticity of demand and comment on the nature of goods. (3)

OR (this alternative is only for question C)

What are the characteristics of the Indifference Curve and what do you mean by budget line? (2+1=3)

##########

Module III
Management

Answer any two questions. Each question carries 5 marks. (2 × 5 = 10)

1. What is Management? Discuss the features or characteristics of management.

2. Discuss different levels of Management.

3. Discuss 'Management is both a science as well as an art'.

##########

B.Tech/ B Arch 4th Year 7th Semester(AE/MET/CST/ETC/IT/EE/ARCH)

END Semester Examination November, 2022

FINANCE ECONOMICS & MANAGEMENT for Engineers (HSS III) (HU - 4101)

Answer Module I & II in the 1st Half and Module III in the 2nd half answer scripts.

FullMarks:50 Two marks for neatness . Time: 3 hours

Module I

Finance (16)

A. From the following information prepare a Cost Sheet for the month ended 31st October 2022:

Items		Amount (Rs.)
Raw material	:	1,50,000
Direct Labour	:	1,00,000
Packaging charge	:	10,000
Lubricant	:	5,000
Office salary	:	24,000
Factory Rent	:	10,000
Postage	:	500
Salesman salary	:	10,000
Sales	:	3,50,000

[8]

B. What is Leverage? Explain with example the concept of different types of Leverages. [8]

OR

Discuss the different sources of Long Term Funds available for Corporate Finance. Also discuss the concept of Cost of Capital in this context. [8]

Module II

ECONOMICS (16)

1. (a)State and explain the Law of Variable Proportions with a diagram.
   (b)What is the relationship between the average product and marginal product curve? (4+2)
2. (a) Why the minimum point of the short-run average cost (SRAC) curve lies to the right of the minimum point of the short-run marginal cost (SRMC) curve? Why SRAC curve is U shaped?
   (b)What are the differences between Isoquant and Iso-cost? How does a producer achieve equilibrium?
   (c) What is the difference between opportunity and sunk cost? (3+2+1)
3. (a) "All marketable production is economic production but all economic production is not marketable"- Explain.
   (b) When it will have a contractionary effect on the circular flow of the economy of a three-sector model? What are the leakages and injections in the economy of four sector model? (2+2)

Or (this alternative is only for question 3)

(a) What is an investment multiplier?

(b) Suppose the nominal GNP of a country i.e. GNP estimated at current prices, in the year 2012 is given at INR 500 billion, and the price index number is given as base year 2012=100. Now let the nominal GNP increase to INR 600 billion in the year 2017 and PIN rise to 110. Find the real GNP. (2+2)

Module III
Management (16)
Answer any FOUR(4 x 4=16)

I. Explain three basic styles of Management.

II. Discuss Ansoff Product-Market Matrix.

III. Under what conditions would you recommend to use Turn Around Strategy in an organization?

IV. Distinguish between Concentric and Conglomerate Diversification with suitable examples.

V. Differentiate between Cost Leadership and Differentiation Strategies.

VI. Explain the process of Communication.

Indian Institute of Engineering Science and Technology, Shibpur

B.Tech. Information Technology, 7th Semester Mid Semester Examinations, September, 2022

Graph Algorithms

IT-4123

Full Marks:30 Answer any five questions Time: 2 Hours

1. a) How will you measure the maximum density of a graph? How to measure the actual density of a graph? Justify your answer. [3]
   b) What is the average degree of a network? What is its significance? [3]

2. a) Define the closeness centrality of a node. When should you use the normalized closeness centrality? [3]
   b) What is harmonic centrality of a graph? How is it different from the closeness centrality? [3]

3. a) Define the betweeness centrality of a node. State when it will have a high value. [3]
   b) Explain the role of the damping factor in the page-rank algorithm. [3]

4. a) Explain the Louvain modularity algorithm with an example. [3]
   b) Explain the Label Propagation algorithm in brief. [3]

5. a) Prove the following: "For a directed graph, a back-pointing edge (u,v) in BFS can exist whenever v lies closer to the root than u does." [3]
   b) Explain how you can find cycles in a graph using Depth First Search. [3]

6. a) What is an articulation vertex? State an algorithm to find it/them in a graph. [3]
   b) Prove that the Prim's algorithm for determining Minimum Spanning Tree is correct. [3]

7. a) Propose a method to find the Maximum Spanning Tree. [3]
   b) Define maximum flow, total positive flow entering or exiting a node. [3]

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (IT), 7th Semester End Semester Examinations, 2022

Graph Algorithms (IT-4123)

Time: 3 Hours

Full Marks: 50

Answer any five questions

1. a) What is the damping factor in the page-rank algorithm? Explain with an example what would be the problem if no damping factor is used. [5]
   b) Explain the PUSH and PULL operations in the label propagation algorithm. [5]

2. a) What is an articulation vertex in a graph? Explain how the articulation vertices in a graph can be determined using Depth First Search (DFS). [5]
   b) Prove that Prim's algorithm outputs a Minimum Spanning Tree of a weighted graph. [5]

3. a) State and explain the time complexity of the Floyd Warshall algorithm to find the all pair shortest paths. [5]
   b) What is a flow network? State the properties of a flow network. [5]

4. a) Explain how you can find the maximum flow of a flow network with multiple sources and multiple sinks. [5]
   b) What is a residual network? Explain with an example. [5]

5. a) State and explain the max-flow min-cut theorem. [5]
   b) Propose an algorithm to find the maximum bipartite matching in a graph. [5]

6. a) State an algorithm to find the Eulerian trail and circuit in a graph. [5]
   b) State how you can find the Hamiltonian cycle in a dense graph. [5]

7. a) What is a DFS graph? What are the spine and stem of a cycle corresponding to an edge e where i) e is a tree edge and ii) e is a back-edge? [5]
   b) Give the fundamental steps of the Hopcroft and Tarzan algorithm for finding the cycle in a graph. [5]