Code : 241702

B.Tech 7th Semester Exam., 2020

PERSONNEL MANAGEMENT AND INDUSTRIAL RELATIONS

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

(iv) Question No. 1 is compulsory.

1. Answer any *seven* of the following in short : 2×7=14

   (a) What is job analysis?

   (b) List any four roles of a personnel manager.

   (c) Give any two objectives of transfer.

   (d) Mention two differences between discharge and dismissal.

   (e) Define the term 'social security'.

   (f) What do you understand by off-the job training methods?

   (g) Define trade union.

   (h) What do you understand by living wage?

   (i) Differentiate between time rate and piece rate methods of wage payment.

   (j) Define employee induction.

2. Why is social security important for workers? Discuss social insurance and social assistance as social security measures. 14

3. Today personnel management has taken a central role in organizations. Why? 14

4. List and explain the various steps involved in employee selection. 14

5. Explain the meaning of employee development. Discuss any four methods of employee development. 14

6. How has the concept of industrial relations changed in recent times? Discuss the major players in industrial relations in India. 14

7. Discuss the meaning and purpose of wages and salary administration. 14

8. Define performance appraisal. Discuss the objectives of performance appraisal. 14

9. Discuss the types and methods of trade unions in India. 14

★ ★ ★

Code : 051735

B.Tech 7th Semester Special Exam., 2020

COMPUTER GRAPHICS

Time : 3 hours *Full Marks* : 70

Instructions:

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Explain any *seven* of the following terms : 2×7=14

   (a) Computer graphics

   (b) Simulation

   (c) Image processing

   (d) Virtual reality

   (e) Snapshot and frame

   (f) Frame buffer

   (g) Raster-scan systems

   (h) Persistence

   (i) Resolution

   (j) Brightness

2. Explain the following : 7+7=14

   (a) Jag free images on a raster CRT

   (b) Interactive graphics processor for digital logic situation system

3. (a) Compare point wise the following :

   (i) LCD monitors vs CRT monitors

   (ii) Random scan display vs Raster scan display

   (b) Consider a raster system with resolution 1280 by 1024. What size of frame buffer is needed for given system to store 24 bits per pixel? How many colors are possible in given system? What is the access time per pixel if refreshing rate is 60 frames per second? 8+6=14

4. (a) What are graphics standards in 3-D models? Why do you need a graphic standard? Explain.

   (b) How does a graphic standard work with a graphic application? Explain. 7+7=14

5. (a) Describe GKS. What are the functionality and limitations of GKS? Explain.

   (b) What are the uses of different classes of functions available in GKS? Explain. 7+7=14

6. Explain the following with respect to graphical work stations : 7+7=14

   (a) Routing output to graphical work stations

   (b) Types of GKS and work stations

7. (a) List and describe the methods of creating animations.

   (b) Define motion path. Explain various specifications to define motion path.

   (c) What is morphing? Explain. 6+6+2=14

8. Explain the 3-D reconstruction and its applications in detail. 14

9. Write short notes on any *three* of the following : 14

   (a) Raster CRT

   (b) 3-D shading

   (c) Digital image processing

   (d) Ray tracing

   (e) Uses of computer animations in education

   (f) Uses of computer animations in entertainment

* * *

Code : 051718

B.Tech 7th Semester Special Exam., 2020

CRYPTOGRAPHY

Time : 3 hours | *Full Marks* : 70

Instructions:

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Choose the correct option of the following (any *seven*) : **2×7=14**

(a) DES follows

(i) hash algorithm

(ii) Caesar cipher

(iii) Feistel cipher structure

(iv) SP-network

(b) Find the solution of $x^2 \equiv 16 \bmod 23$.

(i) $x = 6$ and 17

(ii) $x = 4$ and 19

(iii) $x = 11$ and 12

(iv) $x = 7$ and 16

(c) In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.

(i) 1024

(ii) 512

(iii) 256

(iv) 1248

(d) When a hash function is used to provide message authentication, the hash function value is referred to as

(i) message field

(ii) message digest

(iii) message score

(iv) message leap

(e) Which one of the following is not a public-key distribution means?

(i) Public-key certificates

(ii) Hashing certificates

(iii) Publicly available directories

(iv) Public-key authorities

(f) The Data Encryption Standard (DES) was designed by

(i) Microsoft

(ii) Apple

(iii) IBM

(iv) None of the above

(g) Which of the following encryption keys is used to encrypt and decrypt the data?

(i) Public key

(ii) Private key

(iii) Symmetric key

(iv) Asymmetric key

(h) In asymmetric key cryptography, the private key is kept by

(i) sender

(ii) receiver

(iii) both sender and receiver

(iv) all the connected devices to the network

(i) Network layer firewall has two sub-categories as

(i) statefull firewall and stateless firewall

(ii) bit-oriented firewall and byte-oriented firewall

(iii) frame firewall and packet firewall

(iv) None of the above

2. *(a)* What is the OSI security architecture? List and briefly define the three key objectives of computer security. **7**

(b) List and briefly define the categories of passive and active security attacks. List and briefly define the categories of security services. **7**

3. Encrypt the message "meet me at the usual place at ten rather than eight O'clock" using the Hill cipher with the key $\begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$.

Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. 14

4. (a) What is the difference between diffusion and confusion? What are the critical aspects of Feistel cipher design? 7

(b) What is the output of the first round of the DES algorithm when the plaintext and the key both are all zeros? 7

5. (a) Describe SubBytes, Shift Rows, MixColumns and AddRoundKey of AES. 7

(b) Find all irreducible polynomials of degree 3 over GF(2). 7

6. One of the most attractive applications of public-key algorithms is the establishment of a secure session key for a private-key algorithm such as AES over an insecure channel. Assume Bob has a pair of public/private keys for the RSA cryptosystem. Develop a simple protocol

using RSA which allows the two parties Alice and Bob to agree on a shared secret key. Who determines the key in this protocol, Alice, Bob or both?

Do the questions mentioned below on RSA : 7×2=14

(a) In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

(b) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

7. Briefly explain Diffie-Hellman key exchange. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 157$ and a primitive root $\alpha = 5$.

(a) If Alice has a private key $XA = 15$, find her public key YA. 7

(b) If Bob has a private key $XB = 27$, find his public key YB. 7

8. (a) What problem was Kerberos designed to address? What entities constitute a full service Kerberos environment? What are the threats associated with user authentication over a network or an Internet? 7

(b) Explain X.509 certificate. 7

9. Write short notes on the following : 14

(a) S/MIME

(b) HMAC

(c) Digital signature

(d) Denial of service attack

* * *

Code : 051813

B.Tech 8th Semester Exam., 2021

COMPUTER NETWORKS

Time : 3 hours | *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Choose the correct answer of the following (any *seven*) : 2×7=14

(a) What layer in the TCP/IP stack is equivalent to the transport layer of the OSI model?

(i) Application

(ii) Host-to-host

(iii) Internet

(iv) Network access

(b) Which topology covers security, robust and eliminating traffic factor?

(i) Mesh

(ii) Ring

(iii) Star

(iv) Bus

(c) Internetworking protocol is known as

(i) TCP

(ii) IP

(iii) ISP

(iv) TCP/IP

(d) Which device uses logical addressing system?

(i) Hub

(ii) Switch

(iii) Bridge

(iv) Router

(e) Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a time-out occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission.

(i) 8 MSS

(ii) 14 MSS

(iii) 7 MSS

(iv) 12 MSS

(f) Which transmission media has the highest transmission speed in a network?

(i) Coaxial cable

(ii) Twisted pair cable

(iii) Optical fiber

(iv) Electrical cable

(g) What is the maximum size of data that the application layer can pass onto the TCP layer below?

(i) Any size

(ii) 2^16 bytes-size of TCP header

(iii) 2^16 bytes

(iv) 1500 bytes

(h) The maximum window size for data transmission using the selective reject protocol with *n*-bit frame sequence numbers is

(i) 2^n

(ii) $2^{(n-1)}$

(iii) $2^n - 1$

(iv) $2^{(n-2)}$

(i) Station *A* needs to send a message consisting of 9 packets to Station *B* using a sliding window (window size 3) and go-back-*n* error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that *A* transmits gets lost (but no

(b) An ISP is granted a block of addresses starting with 120.60.4.0/22. The ISP wants to distribute these blocks to 100 organizations with each organization receiving just eight addresses. Design the sub-blocks and give the slash notation for each sub-block. Find out how many addresses are still available after these allocations. 7+7=14

6. (a) Explain in detail about TCP/IP protocol suite with neat diagram.

(b) Differentiate between forwarding and routing. 7+7=14

7. (a) Compare and contrast the protocol field at the network layer with the port numbers at the transport layer. What is their common purpose? Why do we need two port-number fields but only one protocol field? Why is the size of the protocol field only half the size of each port number?

(b) With a neat diagram, explain distance vector routing protocol. 7+7=14

8. Draw and describe the TCP header. Assume that a host receives a UDP segment with 01011101 11110010 (we separated the values of each byte with a space for clarity) as the checksum. The host adds the 16-bit words over all necessary fields excluding the checksum and obtains the value 00110010 00001101. Is the segment considered correctly received or not? What does the receiver do? 14

9. Differentiate between POP3 and IMAP4. Suppose Alice, with a Web-based e-mail account (such as Hotmail or Gmail), sends a message to Bob, who accesses his mail from his mail server using POP3. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts. 14

* * *