International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE, Final Examination, Spring 2022

Course Code: CSE-4743Course Title: Computer Security

Total marks: 50 Time: 2.5 hours

Marks CO DL

Part A

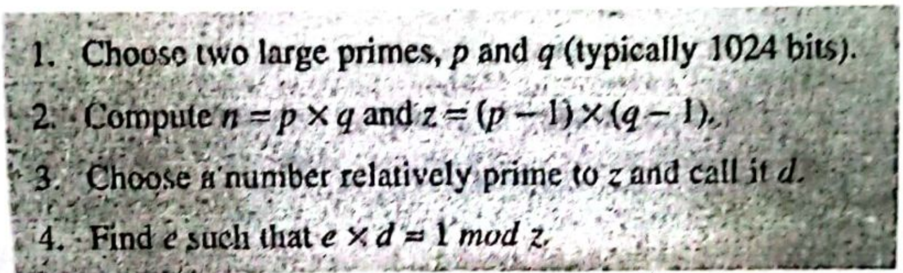
[Answer the questions from the followings]

1 (a) Write the purpose of encryption with private key and encryption with public key in Public key cryptosystems. 5 CO2 App

OR (of 1a only)

(a) Explain symmetric secret key distribution between two parties ensuring confidentiality and authentication. 5 CO2 App

(b) The initial steps of RSA are: 5 CO2 App



1. Choose two large primes, p and q (typically 1024 bits).
2. Compute $n = p \times q$ and $z = (p-1) \times (q-1)$.
3. Choose a number relatively prime to z and call it d.
4. Find e such that $e \times d = 1 \ mod \ z$.

During decryption in RSA you use the equation P= C^d (mod n), private key consists of (d,n). A person does not know d and he is trying to estimate d. how does choice (whether p and q are small or large primes) of p and q effect estimation of d?

2 (a) Justify the following sentence for password policy-"There should be a tradeoff between usability and security". 2 CO2 U

(b) Explain the CIA for computer security. What is the benefit of using salt in passwords? 3 CO1 U

(C) Draw a block diagram and briefly explain the working steps of Intrusion Prevention Systems (IDS). Compare the benefits and drawbacks of IPS with IDS. 5 CO2 An

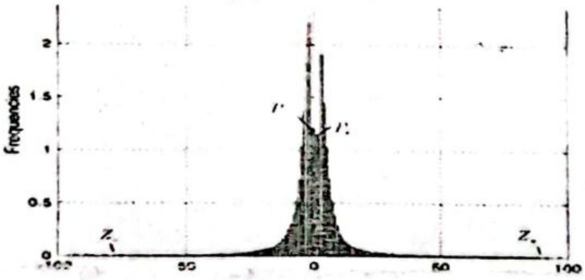
OR (of 2c only)

(C) What are the desired attributes of a cryptographic hash function? Use examples if required. 5 CO2 U

Part B

[Answer the questions from the followings]

3 (a)	Explain the social engineering attack cycle. List the organizational and technical defense mechanisms against social engineering attacks.	4	CO3	R
(b)	What is a Phishing attack? Write down the current protection methods against phishing attacks.	3	CO2	U
(c)	Explain how non-repudiation is ensured by using a digital signature.	3	CO2	An
4 (a)	What are the drawbacks of Cryptography that can be overcome by Steganography and how?	3	CO1	R
(b)	Define embedding Payload and embedding capacity. Briefly explain the steps of the Basic pixel reference errors (BPRE) histogram-based scheme.	5	CO2	U
(c)	Do you think an intruder can guess the existence of the secret message from the histogram below? Justify your answer.	2	CO1	An



5 (a)	Discuss some intrusion detection methods.	4	CO4	U
(b)	In Cryptocurrency, how the integrity and authenticity of a transaction are ensured?	6	CO3	An

OR

5 (a)	Demonstrate some packet filtering policies that are configured in your firewall.	4	CO4	App
(b)	Explain Proof of work in Blockchain. Why is it an expensive process? What makes forging of a block difficult in Blockchain?	6	CO3	U

International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE Final Examination, Spring 2022

Course Code: CSE-4747

Course Title: Mathematical Analysis for Computer Science

Total marks: 50 *Time: 2 hours 30 minutes*

[Answer all the questions. Write concisely, keeping your handwriting legible. Figures in the right hand margin indicate full marks.]

Group A

1.

a) A fair coin is flipped three times. Consider the following three events A, B and C: **5**
A ≡ more heads than tails showed up.
B ≡ more tails than heads showed up.
C ≡ same side showed up in all three flips.
With this backdrop, show that *pairwise independence does not necessarily imply mutual independence.*

b) A prize is hidden behind, uniformly at random, one of the four closed, identical doors in a game show. A contestant initially picks a door uniformly at random. Then the host of the show reveals one of the other three doors that do not hide the prize. At this stage the contestant is given a choice of finally picking a door out of the three unopened doors (including the one she already has picked). She is hesitant whether sticking to her original pick is any worse than switching to one of the two other (unopened) doors. Analyze her options and conclude which of them, if any, yields higher likelihood of her winning the prize. **5**

2.

a) A computer program crashes at the end of each hour of use with probability p, if it has not crashed already. What is the probability that there will be no crash in a given day (assuming, the day starts with the program remaining operational)? In addition, what is the expected time until the program crashes? **4**

OR

Your uncle gives you the following present for your doing well in the studies. First he has you flip a coin that lands heads with probability 1/3. If it lands heads, he gives you \$10. If it's tails he has you roll a (fair, regular, six-sided) die, and he gives you a number of dollars equal to whatever the die shows. What is the probability that you would get more than four dollars? What is the expected reward?

b) A rat is trapped in a maze. Initially it has to choose one of two directions. If it goes to the right, then it will wander around in the maze for three minutes and will then return to its initial position. If it goes to the left, then with probability 1/3 it will depart the maze after two minutes of traveling, and with probability 2/3 it will return to its initial position after five minutes of traveling. Assuming that the rat is at all times equally likely to go to the left or the right, what is the expected number of minutes that it will be trapped in the maze? **4**

OR

If an aircraft is present in a certain area, a radar detects it and generates an alarm signal with probability 0.99. If an aircraft is not present, the radar generates (false) alarm, with probability 0.10. We assume that an aircraft is present with probability 0.04. What is the probability that an aircraft is indeed present, given that an alarm is generated?

c) Briefly explain the Simpson's paradox. **2**

OR

What is linearity of expectation?

Group B

3.

a) Each of the n nodes in a local area network transmits its packet in the shared channel at any given slot with probability p. Whenever more than one node transmits in a particular slot, collision occurs and no transmitted packet can be successfully received.

i. Find the probability that a particular node's transmission in a given slot will encounter collision. 2

ii. Find the expected number of nodes that transmit in a given slot. 2

iii. Find the probability that two successive slots on the channel see successful transmissions. 2

iv.

b) Zayed, Bakr and Hasan decide to play a game. Each player puts \$2 on the table and secretly writes down either "heads" or "tails". Then one of them tosses a fair coin. The \$6 on the table is divided evenly among the players who correctly predicted the outcome of the coin toss. If everyone guessed incorrectly, then everyone takes their money back. Now, explain the outcome when Zayed and Hasan are colluding and always make opposite guesses. 4

4.

a) What is Markov property? 2

b) Formulate a mathematical model to deduce the probability that a gambler reaches his target of \$T starting with \$n ($T > n$), before ever going broke. In each round, he wins \$1 with probability p or loses the same amount with probability $1 - p$. His play stops if he ever goes broke, i.e., reaches \$0. 4

c) How can random walk be employed to calculate the ranks of the pages in a Web-graph? Illustrate how the scheme works with a Web-graph of 4 webpages and at least 7 hyperlinks (directed edges). 4

5.

a) In this corona situation IIUC giving loan to five talented and needy students. According to the recent situation. the probability of a students living in these conditions for CGPA 3.7 or more is 2/3 Calculate the probability that after 3.7 CGPA. *[Hint. you can use Binomial distribution.]* 5

(a) All five-students needy.

(b) Exactly two students are needy

(c) at least three students are needy.

OR

A prisoner in a dark dungeon discovers three tunnels leading from his cell. The first tunnel reaches a dead-end after 50 feet and the second tunnel reaches a dead-end after 20 feet, but the third tunnel leads to freedom after 100 feet. Each day, the prisoner picks a tunnel uniformly at random and crawls along it. If he reaches a dead-end, he has to crawl back to his cell. Find the expected distance that he crawls before he reaches freedom

b) Packets are transmitted in slots over a communication channel that is either in good or bad/noisy condition. Packets transmitted during any bad/noisy slots get lost. The bad/noisy channel remains so in the next slot with probability 0.4 and turns good with probability 0.6 and. On the other hand, the channel retains the good condition in the next slot with probability 0.8 and becomes bad/noisy with probability 0.2. 5

Find the steady-state probability that the channel will be found in a good or bad/noisy condition.

If the channel is seen to be good in the k-th slot, what is the probability that it will remain good during the $(k + 4)$th slot?

OR

Auto vehicles arrive at a petrol pump, having one petrol unit, In Poisson fashion with an average of 10 units per hour. The service is distributed exponentially with a mean of 3 minutes. Find the following:

i. Average waiting time for customer

ii. Average length of queue

iii. Probability that a customer arriving at the pump will have to wait.

iv. The utilization factor for the pump unit.

v. Probability that the number of customers in the system is 2.

International Islamic University Chittagong

Center for General Education (CGED)

Semester End Examination: Spring 2022
Course Code: URIH-4701

Program: Undergraduate
Course Title: A Survey of Islamic History & Culture
Full Marks: 50

Time: 2 hours and 30 minutes.

Instructions:
All Questions are Compulsory.
Figures in the right margin indicate full marks.
ii. Course Learning Outcome (CLO) and Bloom's levels are mentioned in additional columns.

Bloom's Levels of the Questions.						
Letter of Symbol	R	U	App	An	E	C
Meaning	Remember	Understand	Apply	Analyze	Evaluate	Create

		Text of the Questions	Marks	Bloom's Level	CLO
1		Analyze the credit and achievement of Muawia bin Abu Sufian (R.) as the founder of Umayyad *Khilafah.*	10	An	CLO1
2		Review the expansion of Islamic territories under *Khalifah* Al-Walid bin Abdul Malik. How did these expansions make changes in the social order of the conquered territories?	10	An	CLO2
		Or			
		Assess the reforms of Umar bin Abdul Aziz. What are the implications of these reforms to ensure good governance in the contemporary state system?	10	E	CLO2
3		Analyze the causes of decline and fall of the Umayyads *Khilafah.* What lessons you might suggest for the contemporary political elites in the light of said events.	10	An	CLO3
4	a	Estimate the reign of khalifah Harun al-Rashid as a great ruler in the history of the world.	6	E	CLO3
	b	How do you explain his dynamic foreign policy in the context of contemporary Muslim world?	4	An	CLO3
5		Appreciate the contributions of Muslims to the development of Geography and Astronomy. How are the modern Geography and Astronomy indebted to these developments?	10	E	CLO3

================

Moderation

International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE, 7th Semester, Final Term Examination

Spring 2022

Course Code: CSE 4741
Total marks: 50

Course Title: Computer Graphics
Time: 2 hours 30 minutes

[Answer all the *five* questions. Separate answer scripts must be used for Group A and Group B. Figures in the right-hand margin indicate full marks.]

Course Outcomes and Bloom's Levels are mentioned in additional Columns

Course Outcomes (COs) of the Questions	
CO1	Develop specific project requirements and goals for a software project.
CO2	Explain the basic concepts and application techniques in software design.
CO3	Analyze the performance of protocols and networks.
CO4	Demonstrate a familiarity with major network and security algorithms and protocols.
CO5	Identify and apply applications of computer networks with determining suitable alternatives of the networks for the alternative conditions.

Bloom's Levels of the Questions						
Letter Symbols	R	U	App	An	E	C
Meaning	Remember	Understand	Apply	Analyze	Evaluate	Create

GROUP A

			CO	DL
1.	Explain Weiler AthertonPolygon Clipping Algorithm.	6	CO2	C2
a)	Define convex and concave polygon.			
b)	Clip the polygon P_1.........P_9 in figure 1 against the window ABCD using the Southerland Hodgeman algorithm.	4	CO3	C2

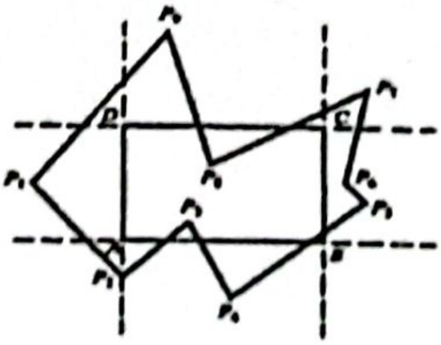


fig. 1

OR

Clip the polygon P_1.........P_9 in figure 1 against the window ABCD using the Weiler Atherton Polygon Clipping Algorithm.

2. a) Use the Cohen Sutherland algorithm to clip two lines P1(40,15)-P2(75,45) and P3(70,20)-P4(100,10) against a window A(50,10),B(80,10),C(80,40),D(50,40). 4 CO4 C3

OR

Find a transformation Av which aligns a given vector V with the vector K along the positive z axis.

b) Given a 3D object with coordinate points A(0, 3, 1), B(3, 3, 2), C(3, 0, 0), D(0, 0, 0). Apply the translation with the distance 1 towards X axis, 1 towards Y axis and 2 towards Z axis and obtain the new coordinates of the object. 4 CO4 C3

c) Given a 3D unit cube. Find the mirror reflection of the object about yz plane. 2 CO1 C2

OR

What are the basic differences between 3D rotation and 2D rotation?

GROUP B

3. a) What is the difference between orthographic and oblique projection. Describe some subcategories of these two projections. 3 CO1 C3

b) A unit cube is projected onto the xy plane. Draw the projected image using the standard perspective transformation with 4 CO1 C3

i) d = 5

where d is the distance from the view plane.

OR

Find the transformation for

a) Cabinet with $\theta = 45^\circ$

b) Draw the projection of the unit cube for each transformation.

c) Describe the anomalies of perspective transformation. 3 CO1 C1

4. a) What is Wireframe model? Write the advantages and disadvantages of wire-frame model. 3 CO3 C1

b) What is hidden surface removal? What steps are required to determine whether any given point p1(x1,y1,z1) obscures another point p2(x2,y2,z2)? 3 CO2 C2

c) Give a suitable example of z buffer algorithm and describe it. 4 CO2 C3

OR

Give a suitable example of scan line Hidden Surface Removal algorithm and describe it.

5. a) What do you mean by Constant shading, Gouraud shading and Phong shading? 2 CO2 C1

OR

Describe the basic principle of pinhole camera.

b) Describe a recursive ray tracing method. 4 CO2 C1

c) A ray is represented by r(t)=2I+J-3K and d=I+2K. Find the coordinates of the points on the ray that corresponds to t=0,1 and 3 respectively 4 CO2 C3

International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE, 7th Semester, Final Examination

Spring 2022

Course Code: **CSE 3633**

Course Title: **Computer Networks**

Time: 2 hours 30 minutes

Full Marks: 50

(i) The figures in the right-hand margin indicate full marks

(ii) Course Outcomes and Bloom's Levels are mentioned in additional Columns

Course Outcomes (COs) of the Questions	
CO1	**Develop** specific project requirements and goals for a software project.
CO2	**Explain** the basic concepts and application techniques in software design.
CO3	**Analyze** the performance of protocols and networks.
CO4	**Demonstrate** a familiarity with major network and security algorithms and protocols.
CO5	**Identify and apply** applications of computer networks with determining suitable alternatives of the networks for the alternative conditions.

Bloom's Levels of the Questions						
Letter Symbols	R	U	App	An	E	C
Meaning	Remember	Understand	Apply	Analyze	Evaluate	Create

Part A

[Answer the questions from the followings]

1. a) Apply LSR algorithm on the following network in fig-1 to construct a routing table of router 'R1'. CO2 Ap 5

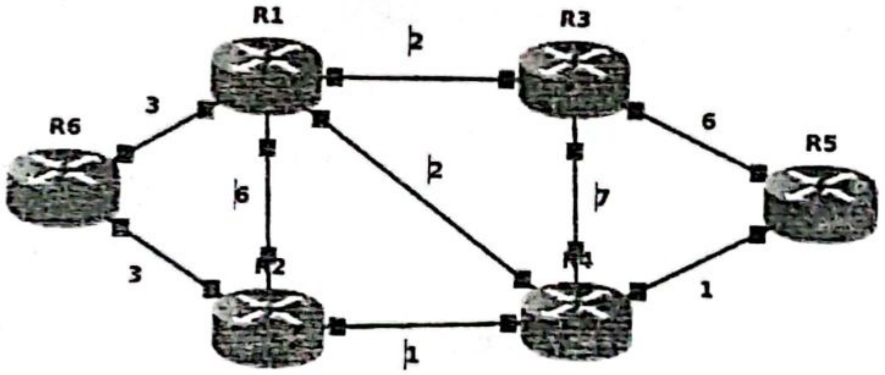


Fig-1

1. b) Apply the DVR algorithm on the above network in fig-1 to construct a routing table of router 'R1'. CO2 Ap 5

2. a) Explain with a figure how the Link State database is built. CO4 U 5

2. b) With a suitable figure, compare the fields in TCP and UDP headers. Why do you think the TCP header has more fields than UDP header? CO2 E 5

OR

2. a) Write down the advantages and disadvantages of hierarchical routing with the help of an appropriate network diagram. CO4 U 5

2. b) Why does UDP exist? Would it not have been enough to just let user processes send raw IP packets? Who executes Connect primitive? Why Listen primitive is necessary? CO2 E 5

Part B

[Answer the questions from the followings]

3. a) Discuss the roles of the Application layer and transport layer in flow control for both sender and receiver of data. CO1 U 5

3. b) Explain MPLS (Multi Protocol Label Switching) with a figure. Also mention how it improves traditional routing. CO3 An 5

4. a) TCP is the main protocol of the transport layer, then why UDP exists? CO4 Un 5

4. b) What is the silly window syndrome? How to avoid silly window syndrome? CO4 Un 5

5. a) Analyze the weakness of substitution or Caesar cipher CO3 Ap 5

5. b) Encrypt a plain text message "F(=6)" by using RSA encryption. Also show the decryption of the Ciphertext you derived. CO4 U 5

OR

5. a) Suppose you have registered your newly created website named [illegible] with a DNS server. Describe the DNS recursive query for searching the IP address of your cse web server. CO3 An 5

5. b) How does email architecture differ from web architecture? CO4 U 5

International Islamic University Chittagong

Department of Computer Science & Engineering

Program: B.Sc in CSE; Semester:7th

Final LAB Quiz Exam, Spring-22

Course Code: CSE- 4744. **Time: 15 mins**
Course Title: Computer Security Lab.

1. What is the Principle of Least Web Privilege? 1x1=1
2. Write some applications of Cryptographic Hash Functions? 1x2=2
3. What is the simple command for Hash function? 1x1=1
4. What is substitution technique? 1x1=1
5. What is the process of encoding information in a way so that only someone with a key can decode it?
   a) Compression
   b) Systemic variation
   c) Encryption

6. In computer terms, what is a hash?
   a) A delicious way to cook potatoes
   b) An encrypted value
   c) A decryption key

7. What is the purpose of encryption?

   a) To keep data secure during transmission
   b) To hide files from third parties
   c) To reduce the file size

8. In which form of encryption do the sender and receiver share the same private key?
   a) Symmetric encryption
   b) Asymmetric encryption
   c) Hashing encryption
   d) PGP encryption

9. The phrase ____ describe viruses, worms, Trojan horse attack applets and attack scripts.
   a) Spam
   b) Phishing
   c) Malware
   d) Virus

10. A firewall
    a) Separates a network into multiple domains
    b) May need to allow http to pass
    c) Limits network access between the two security domains and maintains and logs all connections
    d) is a computer or router that sits between the trusted and untrusted.

11. What is a proxy server?
    a) A server that retrieves data from host servers before sending it to a computer
    b) A virtual server that can behave like a mail server, Web server or FTP server
    c) A waiter who never seems to be in the restaurant when your water glass is empty.

12. What does SSL stand for?
    a) Secure Sockets Layer
    b) Secret Service Logarithm
    c) Systematic Security Level

13. What is "Symmetric encryption".

    a) A mathematical procedure that is using a symmetric group.
    b) A form of cryptosystem that is based on groups of symmetry.
    c) A form of cryptosystem in which encryption and decryption are performed using the same key.

14. What is the name of the encryption/decryption key known only to the party or parties that exchange secret messages?
    a) E-signature
    b) Digital certificate
    c) Private key
    d) Security token

International Islamic University Chittagong

Department of Computer Science & Engineering

B. Sc. in CSE Semester Final Examination, Spring 2022

Course Code: CSE 4745 Course Title: Numerical Methods

Total Marks: ***50*** Time: 2 Hours 30 Minutes

[Answer *all* the questions. Figures in the right hand margin indicate full marks.
Separate answer script must be used for Group A and Group B]

Group A

1.a) *Gauss Seidel method* is similar in principle to *Jacobi method.* Then what is the difference between them? 2 CO1 U

b) Solve the following system of equation by using Basic Gauss elimination method 3 CO1 U

$3x_1 + 6x_2 + x_3 = 16$

$2x_1 + 4x_2 + 3x_3 = 13$

$x_1 + 3x_2 \mp 2x_3 = 9$

c) Monthly faculty salary in three departments of an institute is given below. Assuming that the salary for a particular category is same in all the departments, calculate the salary of each category of the faculty using ***Cramer's rule* / Gaussian Elimination method.** 5 CO2 A

Departmnet	Number of Faculty			Total Salary
	Professor	Asst. Professor	Lecturer	(in Thousands)
A	6	2	3	78
B	1	5	3	46
C	2	4	7	58

2. a) Compare *least squares method* with *interpolation.* 2 CO3 U

b) Describe the *least square method* to fit a straight line. 3 CO3 U
OR
Derive an equation to fit a *parabola.*

c) In some determination of the volume v of carbondioxide dissolved in a given volume of water at different temperatures θ, the following pairs of values were obtained: 5 CO4 A

θ	0	5	10	15
v	1.80	1.45	1.00	0.50

Find a relation of the form $v = a + b\,\theta$, which best fits to these observations by the method of least squares.

Group B

3.a) Derive the first order and second order differentiation formula based on equal spaced interval. 3 CO5 U

b) A rod is rotating in a plane. The following table gives the angle θ in radians through which the rod has turned for various values of the time t seconds. Calculate the *angular velocity* and the *angular acceleration* of the rod, when t = 0.3 sec. 5 CO6 A

t seconds	0.0	0.2	0.4	0.6	0.8	1.0
θ radians	0.0	0.22	0.48	1.10	2.0	3.2

c) Explain how numerical differentiation can be used to find *the maximum* and *minimum* values of a tabulated function. 2 CO5 U

4.a) When do we need to use a numerical method instead of analytical method for *integration*? 1 CO5 U

b) Derive the general quadrature formula using Newton's forward difference formula. 4 CO5 U

OR

Calculate the value $\int_0^1 \frac{1}{(1+x)}dx$ correct up to 3 significant figures taking six intervals by trapezoidal rule

c) The velocity of a train which starts from rest is given by the following table, the time being recorded in minutes from the start and the speed in km/hour. 5 CO6 A

t (minutes)	2	4	6	8	10	12	14	16	18	20
Y (km/hr)	16	28.8	32	46.4	51.2	32.0	17.6	8	3.2	0

Estimate approximately the total distance run in 20 minutes using i) *Trapezoidal rule* ii) *Simpson's 1/3 rule.*

5.a) Write the advantages and limitations of i) *Taylor's series method* ii) *Euler's method.* 2 CO5 U

b) Describe the *Taylor's series method* for the numerical solution of ordinary differential equation. 3 CO5 U

OR

Describe the *Euler's method* for the numerical solution of ordinary differential equation.

c) Use the *fourth order Runge-Kutta method* to solve 5 CO6 A

$$\frac{dy}{dx} = 2x^2 + y^2$$

$$y(0) = 1$$

for the interval $0 < x \leq 0.4$, with $h = 0.2$.