Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
4^{th} year 1^{st} Semester Final Examination - 2023
Session—**2019-20** Course No.—**SWE 429**
Course Title—**Information and Network Security**
Time—**2 Hours** Credit: **2.00** Total Marks#**50**

Part A

1. Answer the following Questions. (Any Five) $5 \times 1 = 5$

(a) What is the unicity distance?

(b) What is a digital certificate?

(c) What are the two general approaches to attacking a cipher?

(d) What types of attacks are addressed by message authentication?

(e) Eve has tricked Alice into decrypting a bunch of ciphertexts that Alice encrypted last month but forgot about. What type of attack is Eve employing?

(f) What is Masquerading?

2. Answer the following Questions. (Any Four) $4 \times 2.55 = 10$

(a) Calculate the GCD(320,13) using the Euclidean Algorithm

(b) Differentiate between different access control mechanisms.

(c) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?

(d) A man-in-the-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates two public-private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.

(e) Bob is arguing that if you use Electronic Codebook (ECB) mode twice in a row to encrypt a long message, M, using the same key each time, it will be more secure. Explain why Bob is wrong in the case of using a binary one-time pad encryption scheme.

3. Answer the following Questions. (Any Two) $2 \times 5 = 10$

(a) Suppose you are given the following text "CAT" and a random matrix K. Now find the cipher text using Hill Cipher. $K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$.

(b) In a public-key system using RSA, you intercept the ciphertext C=20 sent to a user whose public key is e =13, n=77. What is the plaintext M?

(c) Encrypt the following message using Hill cipher algorithm.
Message: ATTACK IS TONIGHT
Key: DKTTJQJEQ
*Hint: For the key use a 3*3 block matrix*

Part B

4. Answer the following Questions. (Any Five) $5 \times 1 = 5$

(a) What is "Quid Pro Quo"?

(b) What does C.I.A. means?

(c) What is MAC?

(d) What do you understand by a Man-in-the-Middle attack?

(e) What do you understand by the term "Security by obscurity"?

(f) How many distinct keys 'n' users need for communication if they are all communicating among themselves and using a symmetric cryptosystem?

5. Answer the following Questions. (Any Four) $4 \times 2.5 = 10$

(a) Compare and contrast symmetric encryption with public-key encryption, including the strengths and weaknesses of each.

(b) Write short notes on different attacks on the Hash functions.

(c) If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

(d) What is 7^{120} *mod* 143?

(e) Why can't Bob use the pair (1,n) as an RSA public key, even if n = pq, for two large primes, p, and q?

6. Answer the following Questions. (Any Two) $2 \times 5 = 10$

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

[i] If Alice has a private key $X_A = 15$, find her public key Y_A.

[ii] If Bob has a private key $X_B = 27$, find his public key Y_B.

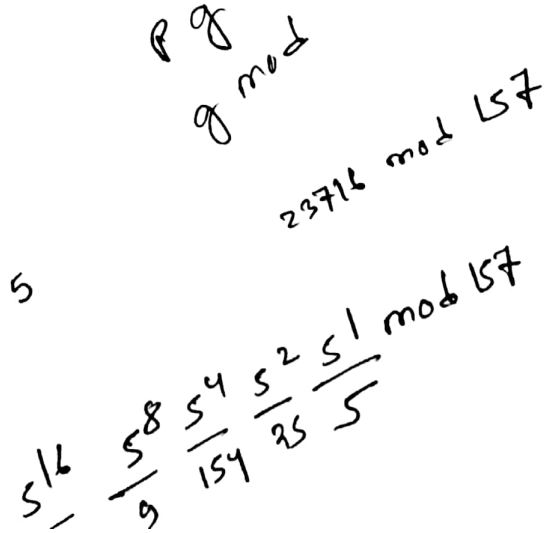
[iii] What is the shared secret key between Alice and Bob?

(b) Suppose Alice and Bob use an Elgamal scheme with a common prime q = 157 and a primitive root $\alpha = 5$. If Bob has a public key $Y_B = 10$ and Alice chose the random integer $k = 3$, what is the ciphertext of M = 9?

(c) Suppose Alice chose a prime number $p = 7$ and a generator $g = 3$. She will use Elgamal Cryptosystem for encryption and decryption.

[i] Find the public key and private key for Alice. [2]

[ii] If Bob wants to send a message $M = 13$ to Alice what will be the ciphertext of Bob? [3]



Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
Software Engineering
4th Year 1st Semester Final Examination' Jun 2023 (Session: 2019-20)
Course Code: SWE 425 Credits: 2 Course Title: Software Project Management
Time: 2 hrs Total Marks: 50

Group A

[Answer all the questions]

5x1=5

1. Answer any FIVE

a) What is cost variance?

b) Write the goals of project management.

c) What are the key characteristics that distinguish projects?

d) What are the objectives of an activity planning?

e) List the factors used to identifying the risk.

f) Define capability maturity model

g) What is the use of checkpoints in monitoring?

4x2.5=10

2. Answer any FOUR

a) Write down the problems of measuring risk in software project management.

b) What are called "free floats" and "interfering floats"? How are they calculated?

c) What is Work Breakdown Structure (WBS)? Show the hierarchical diagram of a simple PBS.

d) Discuss the "Maslow's hierarchy of needs" motivation model.

e) Discuss the four leadership styles based on the axes of directives vs. permissive and autocratic vs. democratic.

f) When and how Net Present value is calculated for a project?

2x5=10

3. Answer any TWO

a) Suppose you are a software manager at 'XYZ' company. Now you are working to manage a recent project for your company. But due to inflation rates this project tends to exceed its allocated budget. As a project manager what steps you will take to complete the project within budget. Briefly explain your actions.

b) In a retail company, the management notices a lack of enthusiasm and initiatives among its employees, leading to decreased sales and customer satisfaction. Considering McGregor's theory X and Theory Y, They decide to analyze their managerial approach. How might identifying whether the organization leans towards Theory X or Theory Y influence their strategies for motivating and engaging employees?

c) You are the project manager for a critical software development project at a mid-sized technology company. The project has encountered several risks that have the potential to impact its successful completion.

Based on the provided information, conduct a detailed analysis of the following risk categories: Schedule risks, budget risks, and operational risks.

Group B

[Answer all the questions]

4. Answer any FIVE **5x1=5**

a) What is contract management?

b) What is the cost performance index'?

c) What are the assessments needed in technical part for Software Project Management?

d) What is the significance of 'working in groups'?

e) What is Critical path?

f) Difference between earliest start and earliest finish.

g) What is LOC?

5. Answer any FOUR **4x2.5=10**

a) What is a Product Breakdown Structure (PBS)? Show the hierarchical diagram of a sample PBS.

b) What are the activities covered by project management? Explain.

c) Explain three commonly used Network Planning Models in Project Management.

d) With a suitable example explain the different activities handled by software project management.

e) Discuss with a suitable example the process of 'selecting the right person for the job' in detail.

f) How do you identify hazards in software Project Management?

6. Answer any TWO **2x5=10**

a) Considering the following table, develop a critical path diagram (network) and determine the duration of the critical path and slack times for all activities.

Activity	Designation	Immed. Pred.	Time (Weeks)
Assess customer's need	A	None	2
Write and submit proposal	B	A	1
Obtain approval	C	B	1
Develop service vision and goals	D	C	2
Train employees	E	C	5
Quality improvement pilot groups	F	D, E	5
Write assessment report	G	F	1

b) Define the cash flow forecasting with different cost-benefit evaluation techniques.

c) Discuss the organizational behavior with example.

Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
Software Engineering
4rd Year 1st Semester Final Examination' July 2024 (Session: 2019-20)
Course Code: SWE 431 Credits: 2 Course Title: Human Computer Interaction
Time: 2 hrs Total Marks: 100

Group A

[Answer all the questions]

1. Answer any FIVE **5x2=10**

a) What do you understand by "gulf of execution"?
b) What is a functional-task requirement in the context of user interaction?
c) What do you understand about the term "User Experience (UX)".
d) Define "Earcon"?
e) What do you understand by Field of View (FOV)?
f) What is the WIMP interface?
g) What do you understand by human's short term memory?

2. Answer any FOUR **4x5=20**

a) What do you understand about the term "Universal Usability" and how to achieve it?
b) How to design the system to reduce memory load?
c) What are the differences between HCI guidelines and principles? Explain with an example.
d) Discuss any 4 guidelines that you should be aware of when designing for small devices (mobile).
e) Explain Fitt's Law.
f) When designing icons, what should be your concerns?

3. Answer any TWO **2x10=20**

a) Suppose you are designing a mobile health app for elderly users. How do cognitive and physical limitations of elderly users affect their interaction with mobile apps? What design elements can be implemented to accommodate these limitations?

b) Based on Nielsen's ten general UI heuristics, identify and discuss three specific improvements you would recommend for this e-commerce website to enhance its usability. Provide examples of potential issues and explain how your recommendations would address these issues according to the heuristics.

A new e-commerce website designed for a popular fashion brand. The website allows users to browse and purchase clothing, accessories, and footwear. Here are some key features of the website:
- A home page with featured products and special offers.
- A search bar at the top of every page.
- Product pages with images, descriptions, prices, and customer reviews.
- A shopping cart where users can view and manage selected items.
- A checkout process that includes filling in shipping details, selecting payment methods, and confirming orders.
- Customer support is accessible via live chat.

c) What do you understand by "Predictive Performance Assessment"? Suppose there is a task to delete a file. For this define two task models (for general user and for expert user) and then estimate time taken for each task model.

Estimates of Time Taken for Typical Desktop Computer Operations from GOMS are given below:

Type of Operation	Time Estimate
K: Keyboard input	Expert: 0.12s Average: 0.20s Novice: 1.2s
T(n): Type n characters	280 X n ms
P: Point with mouse to something on the display	1100 ms
B: Press or release mouse button	100 ms
BB: Click a mouse button (press and release)	200 ms
H: Home hands, either to the keyboard or mouse	400 ms
M: Thinking what to do (mental operator)	1200 ms
W(t): Waiting for the system (to respond)	t ms

Group B

[Answer all the questions]

4. Answer any FIVE **5x2=10**

a) What is the Control-Display (C/D) ratio?
b) What is GOMS methodology?
c) What do you understand about the degrees of freedom for haptic displays?
d) What is wireframing?
e) What do you understand by the term "Augmented Virtuality"?
f) What is static posture?
g) State one guideline for good survey.

5. Answer any FOUR **4x5=20**

a) What do you understand about the principle of "Know Thy User"?
b) What should be the considerable criteria for designing an icon? Describe the statement: "Icons should provide useful information" with examples.
c) Why is it important to refresh the user's memory?
d) Describe 2 guidelines for the visual display layout with explanation.
e) What does the inside-out and outside-in method for tracking 3-D motion involve?
f) What is the difference between supplementary pointing and symbolic gestures? Describe each gesture type and provide examples to illustrate their distinctions.

6. Answer any TWO **2x10=20**

a) Design two interaction models, each at a different level of detail, for the task of "connecting to a Bluetooth speaker from a smartphone." The models should cater to two distinct user types: novice users and expert users.
b) Suppose you have developed a new user interface for a mobile health application aimed for elderly users. To evaluate your system, what key aspects should you keep in mind during focus interviews? How would you handle potential ethical and safety issues during the evaluation process?
c) How do emerging computing platforms influence HCI technologies and what impact do they have on the future of HCI?

Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
4^{th} year 1^{st} Semester Final Examination - Jun 2023 (Session: **2019-20**)
Course: **SWE 423** Title: **Computer Graphics and Image Processing** Total Marks#**100**
Time: **3 Hours** Credit: **3.00**

Part A

$5 \times 2 = 10$

1. Answer the following Questions (Any **Five**).
   (a) What is a digital image?
   (b) What is the relationship between RGB and CMY color model?
   (c) What is the relation among the rotations R_θ, $R_{-\theta}$, $R_\theta{}^{-1}$?
   (d) If $d_i = 3$, $x_i = 3$, $y_i = 3$, $dx = 3$, $dy = 2$ what will be the x_{i+1} and y_{i+1} for Bresenham's line drawing algorithm?
   (e) In the direct coding method If we use 10 bits for each primary color, how many possible simultaneous colors do we have?
   (f) Apply point clipping for $(5, 4)$ and $(-2, 10)$ against a window with corners $(-3, 8)$ and $(5, 6)$.
   (g) We have a 800×800 inch image with total pixel count of 40960000, what would be the resolution of that image in ppi?

$4 \times 5 = 20$

2. Answer the following Questions (Any **Four**).
   (a) In the derivation of Bresenham's circle algorithm we have used a decision variable d_i=D(T)+D(S) to help choose between pixels S and T. However, function D as defined in the text is not a true measure of the distance from the center of a pixel to the true circle. Show that when d_i=0 the two pixels S and T are not really *equally* far away from the true circle. Use suitable figures to prove it.
   (b) Given points $P_1(1, 2)$, $P_2(3, 6)$ and $P_3(2, 4)$, determine the points for updated coordinates $x'y'$ for the following coordinate transformations: $\bar{S}_{(1,2)}$, then $\bar{T}_{(-1,5)}$
   (c) Tilting is defined as a rotation about the x-axis followed by a rotation about the y-axis: (i) find the tilting matrix; (ii) does the order of performing rotation matter? Show mathematically.
   (d) Use Bresenham's line algorithm to draw a line from (2,3) to (5,8). Show the steps and the resulting raster location.
   (e) Apply image processing techniques for the following tasks:
      [i] noise reduction
      [ii] change detection
      [iii] masking
   (f) Write the general form of a scaling matrix with respect to a fixed point P(4, 5), where $S_x = a$, $S_y = b$.

$2 \times 10 = 20$

3. Answer the following Questions (Any **TWO**).
   (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). Also, find the clipping position.
   (b) The vertices of $\triangle BCD$ are B(1,-1), C(2,6), and D(5,1) undergo a composition of transformations described as: $\triangle BCD$ is rotated 90° about the origin then a translation of 3 units to the right and down 7. After all the transformations are applied what will be the triangle coordinates? Does the order of transformation matter?
   (c) Determine all the pixel coordinates using 8-way symmetry of the following circle equation using Bresenham's algorithm: $(x - 10)^2 + (y - 15)^2 = 36$

Part B

4. Answer the following Questions (Any **Five**). $5 \times 2 = 10$

   (a) How do you model an object in computer graphics?

   (b) What is region code? What does each bit represent?

   (c) Find the transformation of mirroring by the line $y = x$ for point P(x,y).

   (d) Find the transformation for mirror reflection of a point P(x,y,z) with respect to the xy plane. Use suitable figures.

   (e) What is "Histogram Equalization" in image processing?

   (f) What is the storage requirement of a 300×300 image If we use a 3-byte 256-entry lookup table?

   (g) Determine the clipping category of a line segment with endpoints $(-4, 2)$ and $(-1, 7)$ against a window with corners $(-3, 1)$ and $(2, 6)$.

5. Answer the following Questions (Any **Four**). $5 \times 4 = 20$

   (a) What are the types of Image Compression Techniques? Differentiate between them.

   (b) Find the normalization transformation that maps a window whose lower left corner is at (1,1) and upper right corner is at (3,5) onto a viewport that has a lower left corner at $(0, 0)$ and upper right corner $(\frac{1}{2}, \frac{1}{2})$.

   (c) Write the standard 3D parallel projection matrix. Derive the equations of parallel projection of a point P(x,y,z) onto the xy plane in the direction of projection $\mathbf{V}=a\mathbf{I}+b\mathbf{J}+c\mathbf{K}$. Use suitable figures.

   (d) Draw a line using DDA Algorithm from $(0, 0)$ to $(4, 6)$.

   (e) When eight-way symmetry is used to obtain a full circle from pixel coordinates generated for the 0°to 45°or the 90°to 45°octant, certain pixels are set or plotted twice.

      [i] What is this phenomenon called?

      [ii] Identify where this phenomenon occurs?

      [iii] Is that harmful besides wasting time?

   (f) Find the scan conversion coordinates of a point $P(2, 6, 4)$ after applying a rotation of 30°about the z-axis.

6. Answer the following Questions (Any **Two**). $2 \times 10 = 20$

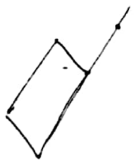
   (a) Consider a Triangle $\triangle ABC$ with vertices A(2,2), B(10,2), C(2,10). Perform the following transformations in succession and find the raster locations.

      [i] Scale it with respect to point $P(2, 2)$ by scaling factors $S_x = 2,\ S_y = 2$

      [ii] Rotate by 90°

   (b) Use the Lian-Barksy algorithm to clip a line AB against a clipping window whose lower left corner is at $(10, 10)$ and upper right corner is $(40, 40)$; where $A(5, 20)$ and $B(50, 30)$.

   (c) Find a transformation A_V which aligns a given vector V with the vector K along the positive z axis.



x, y
y, x
-y, x
-x, y
-x, -y
-y -x
y, -x
x, -y