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: SWE 425 (Software Project Management)
Credits: 2 Time: 2 hrs Total Marks: 50

Group A

[Answer all the questions]

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

a) What are the three main constraints of project management?

b) What is the purpose of project evaluation?

c) Define technical assessment in project evaluation.

d) What are the objectives of an activity planning?

e) What is meant by cash flow forecasting?

f) Mention any one cost-benefit evaluation technique.

g) What is the use of checkpoints in monitoring?

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

a) What do you mean by "contract management" in project management?

b) Explain the triple constraint of projects (time, cost, quality) with examples.

c) Differentiate between **strategic assessment** and **technical assessment**.

d) What is the purpose of cash flow forecasting in project evaluation?

e) Explain the role of **strategic assessment** in project evaluation. How does it align with organizational goals?

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

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

a) **Case Scenario:** A software company is developing a large e-commerce platform for a client. During the project, frequent requirement changes and contract disputes occur. As the project manager, explain how change control procedures and contract management practices can be applied to keep the project on work.

b) Explain risk evaluation in project management. Why is it important in the early stages of a project?

c) Compare and contrast economic, strategic, and technical assessments in project evaluation.

Group B

4. Answer any FIVE *[Answer all the questions]*

5x1=5

a) Define earned value in project management.

b) What does change control help to manage in a project?

c) Name one common source of stress in software project teams.

d) Define leadership in the context of project management.

e) State one characteristic of an effective project team.

f) How can contract management support effective project monitoring?

g) Explain why motivation is critical for software project team performance.

5. Answer any FOUR

4x2.5=10

a) Explain how cost monitoring is carried out in software project management..

b) What is earned value analysis in project monitoring?

c) Write down the HACKMAN JOB CHARACTERISTICS MODEL in brief.

d) Write short notes on Short notes on Leaders style.

e) What is Maslow's Hierarchy Needs?

f) Explain how the delayed projects can be brought back on track.

6. Answer any TWO

2x5=10

a) **Case scenario:** A project is scheduled for 12 months with a budget of $120000. After 6 months, the planned value is $60000, the earned value is $50000, and the actual cost is $70000. Perform Earned Value Analysis and comment on project status. How does Earned Value Analysis help to monitor and control software projects?

b) Discuss in detail the challenges of managing people in software projects. How can stress and conflict be effectively managed?

c) **Case scenario:** You are managing a software development team working under high stress to deliver a product within 3 months. Discuss how leadership and motivational strategies could help manage the team and ensure success.

Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
Software Engineering
4th Year 1st Semester Final Examination 2024 (Session: 2020-21)
Course: SWE 431 Credits: 2 Course Title: Human Computer Interaction
Time: 2 hrs Total Marks: 50

Group A
[Answer the following questions]

1. Answer any TWO **2×2.5 = 5**

a) Surveys and questionnaires are commonly used in user experience evaluation, but their effectiveness depends on how well they are designed.
What key guidelines should be followed when preparing usability surveys to minimize bias and ensure clarity of responses? Explain why factors like clear wording and appropriate scaling (e.g., Likert scale) are important for obtaining reliable results.

b) In the Double Diamond model, when does divergent thinking occur? Why is it important?

c) A user tries to use a password manager but gets locked out because of confusing recovery steps. Which *usability goal* does this problem relate to, and why?

2. Answer any TWO **2×5 = 10**

a) Mobile devices are now the most common platform for accessing applications, from social media to online shopping. However, their small screen size and touch-based interaction introduce unique design challenges, such as ensuring that buttons are large enough to tap easily and minimizing unnecessary typing.
Explain the key HCI guidelines that apply specifically to mobile devices. Provide an example of how a poorly designed mobile app violates these guidelines and how redesigning it according to HCI principles would improve the user experience.

b) What is inclusivity in design? Create a real-life scenario where inclusivity is not satisfied (for example, in a website, app, or physical product), and suggest one design improvement to make it more inclusive.

c) What are the key differences between Heuristic Evaluation, Cognitive Walkthrough, and User Studies in UX research, and when should each method be applied?

3. Answer any ONE **1×10 = 10**

a) You have been asked to design a smart wristband system for night-shift nurses that helps them maintain alertness to manage patient-care tasks.
For each step of the Double Diamond (Discover, Define, Develop), complete the sub-task below. Answer in 1-2 sentences or a quick sketch/bullet list as appropriate.

I. **Discover:** How would you do contextual inquiry (where/when/who), and what do you hope to learn? (4 points)
II. **Define:** State a clear problem statement derived from your Discover step, plus one usability goal. (2 Points)
III. **Develop:** Produce two divergent ideas that would address the problem (brief text or sketches). (2 Points)
IV. **Develop:** List the criteria you would use to choose between those ideas and justify the one you would carry forward. (2 points)

b) Below is a contextual interview transcript captured while observing a customer using a mobile grocery shopping app during their weekly shopping routine. Read it carefully, then complete the tasks that follow.
R (Researcher): You just opened the grocery app on your phone—what's your typical first action? **P (Participant):** I usually go straight to search because I have a specific list, but the search bar is tiny and hidden under this banner ad for energy drinks. I have to scroll up to find it. **R:** What happened when you searched today? **P:** I typed "Greek yogurt" and got 47 results, but half of them were regular yogurt or protein bars. The filters said "Greek" but didn't actually help narrow it down to what I wanted. **R:** How did that make you feel? **P:** Frustrated because I know they carry the brand I want—I buy it in-store—but I couldn't find it in this mess of results. **R:** Walk me through adding items to your cart. **P:** I finally found my yogurt, but when I tapped the "+" button, nothing happened visually. No animation, no cart update, nothing. I wasn't sure if it worked, so I tapped it three more times. **R:** What did you discover? **P:** Later I checked my cart and had four containers instead of one. The app was just slow to respond, but there was no loading indicator or anything to tell me to wait. **R:** Tell me about the checkout process. **P:** I selected my usual delivery time slot—Thursday 2-4pm—but after entering all my payment info, it said that slot was no longer available. I had to go back and pick a different time, which meant re-entering my credit card details. **R:** How did this experience affect your shopping? **P:** I was already running late for a dinner party, so I couldn't wait around to fix the yogurt quantity

or reorder missing items. I just accepted that I'd have too much yogurt and not enough of everything else. Ended up stopping at a physical store on the way, which defeated the whole purpose of ordering ahead.

I. **User-journey map**: Draw a table to present different phases of the customer's journey from opening the grocery app to checkout. Include activity, pain points, and opportunities. (6 points)

II. **Design insights**: Derive two actionable insights for improving the mobile app or overall grocery delivery service. (4 points)

Group B

[Answer the following questions]

4. Answer any TWO **2×2.5 = 5**

a) Contrast low-fidelity vs high-fidelity prototypes in terms of their pros and cons.

b) List two pitfalls to avoid during ideation sessions and explain why.

c) An interface displays 20 items, all using the same color, font, and similar icons. To view basic information, the user must click each item individually.

5. Answer any TWO **2×5 = 10**

a) A travel website asks users to re-enter their booking confirmation number every time they log in, instead of showing a list of their past bookings.

I. Which memory process does this design rely on: recall or recognition?

II. Why would it be better to support the other process instead?

III. Design a different scenario (in any app or system) where the design relies on the same memory process.

b) With one example for each, define the *gulf of execution* and the *gulf of evaluation*. Mention one design principle that can help to reduce each of these gulfs.

c) Answer the below questions related to inclusive design consideration:

I. What design considerations should be prioritized when creating applications for older adults to ensure usability and accessibility? (3 marks)

II. How culture may impact design considerations? (2 marks)

6. Answer any ONE **1×10 = 10**

a) Suppose you are planning a field interview of restaurant owners to improve the online food delivery app experience. The interview will be of the semi-structured type.

I. Who will you interview, and why? (2 marks)

II. At what location will you hold the interview, and why? (2 marks)

III. Provide at least two interview questions you'll use to get data about that user's way(s) of going about the food delivery app. (2 marks)

IV. What are two things as an interviewer you should avoid in a field interview and why? (2 marks)

V. How will you extract the key information from the interview? (2 marks)

b) Nielsen's 10 usability heuristics are widely used principles for evaluating user interfaces.

I. Briefly list any six of Nielsen's heuristics. (6 marks)

II. Draw one real or hypothetical software interface (e.g., a mobile app, website, or desktop program) and analyze how it supports or violates two of the heuristics you listed. (4 marks)

Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
Software Engineering
4th Year 1st Semester Final Examination, 2024
Course: Information and Network Security (SWE 429)
Time: 2 hours **Credits: 2** **Total Marks: 50**

Group A

[Answer all the questions]

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

a) If a symmetric cryptosystem is used among n users, derive the total number of secret keys required. Calculate the number of keys if there are 12 users.
b) Explain the following attacks: Baiting, Quid pro quo.
c) What do you understand by click-jacking?
d) Find the value of $\phi(119)$.
e) What is C.A. and a self-signed certificate?
f) What is session hijacking, and how can an attacker exploit a user's session to gain unauthorized access?

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

a) Illustrate a comparison between the following access control mechanisms: Access control lists, Capabilities, and RBAC.
b) What is the encryption of the following string using the Caesar cipher: "THELAZYFOX" Shift key=3
c) Explain the strengths and weaknesses of using symmetric encryption, like AES, versus a public-key cryptosystem, like RSA.
d) Explain the "circular trust problem" with digital certificates.
e) Suppose you are proposing a simple cryptosystem:

Plaintext (P) : 0 1 0 1

Key (K) : 1 1 0 0

Ciphertext (C): 1 0 0 1 (P **XOR** K)

If you use the same pad(key) multiple times, what issue may arise? Does the cryptosystem maintain the properties of good cryptography proposed by Claude Shannon in 1949? What are the properties, and briefly explain each.

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

a) Consider the RSA cryptosystem with primes P = 7 and Q = 11. Let the public exponent be e = 7.
   I. Encrypt the plaintext message M = 4 using the public key (e,n). Show all intermediate steps. **[2]**
   II. Decrypt the ciphertext using the private key (d,n) and verify that you recover the original message. **[3]**

b) Considering Figure 1, determine the **First Round Key** applying AES-128 for the following input text and initial key:

Input text in Hex (128 bits):

54	77	6F	20	45	6E	65	20	4E	69	6E	65	20	54	77	6F

Key in Hex (128 bits):

54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

c) I. What is a cryptographic hash function? List at least three key properties it must satisfy. **[2]**
II. Why is a digital signature applied to the hash of a message rather than the entire message? Which security goals are achieved by combining a cryptographic hash function with RSA, and how? **[3]**

Group B

[Answer all the questions]

4. Answer any FIVE 5x1=5

a) Validate(True/False) the following statements and justify your choice:

I. Pseudonyms are some trusted agents who are willing to engage in communications or actions for an individual, such that the real individuals can not be traced back.

II. Eavesdropping is an active attack on an information system.

b) What is the Digest of a message?

c) What is Security Usability? Give an example of a scenario where this fails.

d) What is the mathematical hardness assumption on which RSA security is based?

e) What is DNS cache poisoning?

f) Why is Diffie-Hellman vulnerable to a man-in-the-middle attack?

5. Answer any FOUR 4x2.5=10

a) What do you understand about the term "dictionary attack"? Suppose an attacker performs a dictionary attack at 1000 passwords per millisecond. How long would it take to try 100,000 entries?

b) Discuss why probabilistic primality testing is "good enough" for cryptography, even though it does not guarantee primality.

c) What is the birthday attack in the context of cryptographic hash functions? Mathematically prove that effective complexity decreases 2^n to approximately $2^{n/2}$ in such an attack.

d) What is Session, and why do we need one? Explain two different approaches to manage sessions.

e) Describe how HTTPS (via TLS) ensures secure communication between a client and a server. Explain the TLS handshake mechanism step by step.

6. Answer any TWO 2x5=10

a) Let Prime number, p=23, and Generator, g=5. Alice picks a private key a=6 and Bob picks a private key b=15.

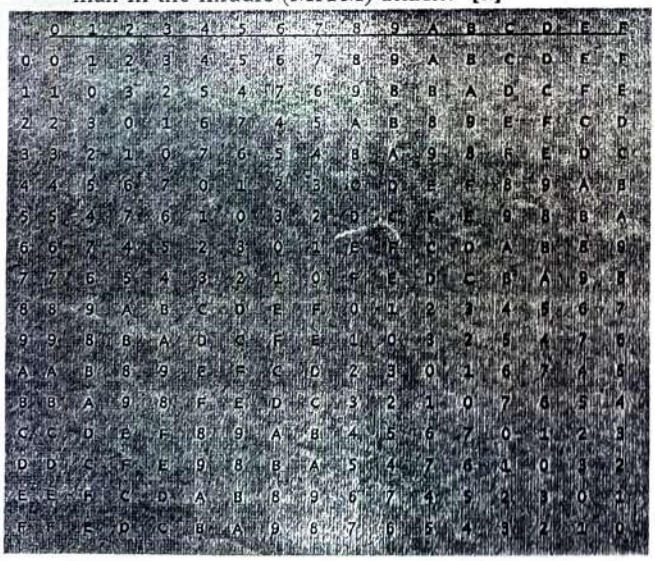
I. Show step by step how Alice and Bob compute their public values A and B, exchange them, and then calculate the shared secret key with the Diffie-Hellman key exchange protocol. Verify that both get the same secret. **[3]**

II. Eve can see (p, g, A, B). Explain why Eve cannot compute the shared secret from this information. What hard mathematical problem would she need to solve, and why is this infeasible when p is very large? **[2]**

b) Explain how AES-128 encryption works. Describe the initial round and the steps in each subsequent round (without explaining the key expansion process). Finally, state how many round keys are needed in AES-128.

c) I. What is a Message Authentication Code (MAC)? How does the MAC mechanism work? **[3]**

II. Which security goals are achieved by using a MAC to protect messages against a man-in-the-middle (MITM) attack? **[2]**



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 1: Hexadecimal Number X-OR Table & S-Box (Substitute Bytes Table)

Shahjalal University of Science & Technology
Institute of Information and Communication Technology
B.Sc.(Engg.) in Software Engineering
4th Year 1st Semester Final Examination 2024
Course: SWE 435 (Neural Network and Deep Learning)
Credit: 3.0 Marks: 100 Time: 3 Hours

Group A

5 X 2

1. Answer any **FIVE**:
   a) With a diagram, show how Machine Learning differs from classical programming?
   b) Briefly define word embedding and give one reason why embedding is useful in NLP?
   c) What is meant by adding dropout in regularization of a model?
   d) What are the two essential characteristics of how deep learning learns from data?
   e) Discuss the different evaluation protocols of a model on a validation dataset.
   f) What is feature engineering?
   g) What key characteristics gives Convolution Neural Network an upper hand compared with a densely connected Artificial Neural Network in image classification.

4 X 5

2. Answer any **FOUR**:
   a) How Artificial Intelligence, Machine Learning, and Deep Learning are all related to each other? Explain with a diagram.
   b) Give real-world examples of data tensors of rank-2 to rank-5?
   c) Discuss the stochastic gradient descent algorithm.
   d) What is learning rate? What happens when the learning rate is too high or too small? Explain with a figure.
   e) What is meant by vectorization in data preprocessing? Explain with an example.
   f) How does splitting a dataset into train, dev, and test sets help identify overfitting?

2 X 10

3. Answer any **TWO**:
   a) Given a tabular regression problem (predict house price from 20 numeric features), design a simple feedforward NN (layer sizes, activations, loss, and optimizer). Explain your choice of architecture, how yo would preprocess the data (mathematically), and one metric you'd report.
   b) i) Draw the architecture of a Convolution Neural Network where: (7)
      - Input is an 8x8 grayscale image.
      - There are two convolution layers:
        - In the 1st convolution layer, a 2x2 kernel is used with 'valid' padding and stride 2.
        - In the 2nd convolution layer, two 2x2 kernels are used with 'same' padding and no stride.
      - Then max pooling is done by a 2x2 filter and stride 2.
      - The output of the pooling is flattened and then two hidden dense layers with 10 units each are applied.
      - There are three output classes

      ii) What activation function(s) are used? (1)
      iii) What is the number of learning parameters in each layer of the entire network? (2)
   c) Discuss the geometric interpretation of Tensor operations. How this geometric interpretation can be related to Deep Learning?

Group B

5 X 2

4. Answer any **FIVE**:

a) What is data curation?

b) Distinguish among batch, mini batch, and true batch Stochastic Gradient Descent optimization.

c) Distinguish between optimization and generalization of a model.

d) What will be last-layer activation and loss function for the following problem types:

Problem type	Last-layer activation	Loss function
Binary classification		
Multiclass, single-label classification		
Multiclass, multilabel classification		

e) Why are the non-linear activation functions necessary in Deep Learning?

f) Distinguish between multi-hot and one-hot encoding.

g) What are the different model deployment options?

4 X 5

5. Answer any **FOUR**:

a) What are the technical forces that bring Deep Learning into deployment?

b) What is meant by generalization? What things are important for a model to be generalized?

c) What is meant by value normalization in data preprocessing? What common practices are followed during value normalization?

d) What is the difference between parameter and hypermeter? Give one example of each.

e) How can you fine-tune a pretrained model? Briefly explain.

f) Explain the points that you will consider in deploying a Deep Learning model on a device.

2 X 10

6. Answer any **TWO**:

a) i) Briefly explain the steps of converting raw text to vectors with a block diagram. (7)

ii) Create Bag-of-words vectors for the following documents. (3)

it was the worst of times,
it was the age of times,
it was the best of wisdom,
it was the age of foolishness

b) i) What is the basic principle of Recurrent Neural Network (RNN)? Where is the simple RNN lacking? (3+2)

ii) How can you convert a simple RNN layer to a Long-Short Term Memory (LSTM) layer? Explain with a block diagram. (5)

c) i) Draw the block diagram of a Transformer encoder with the functional definition of each component. (5)

ii) How can you extend the architecture of Transformer encoder to a sequence-to-sequence learning? Show with a block diagram. (5)

TT#02	Course: Information and Network Security (SWE 429)	Marks: 20	Time: 40 mi

1. Write down the details of the following security principles: Separation of Privilege, Least Privilege, and Compromise Recording. **(4.**

2. I) Find an inverse for 43 modulo 600 that lies between 1 and 600, i.e., find an integer $1 \le t \le 600$ such that $43 \cdot t \equiv 1 \pmod{600}$. **[3.5]** **(5.5**

   II) Find $3^{100} \pmod{101} = ?$ **[2]** $a^{p-1} \equiv 1 \pmod{p}$

3. P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then **(10)**
   I) What will be cipher text value according to RSA algorithm? **[4]**
   II) Again, calculate plain text value from cipher text. **[4]**
   III) Prove the correctness of the RSA algorithm with the help of mathematical notation. **[2]**

TT#01	Course: Information and Network Security (SWE 429)	Marks: 20	Time: 35 mins

1. Define the following terms: Repudiation, Uniticity distance, Pretexting attack, DDoS **(6**

2. Explain how the key exchange happens between two parties who are using the Symmetric Cryptosystem. **(6**

3. "Cryptographic digest of a message(with just hashing the plaintext while generating a digital signature) from the sender ensures the integrity and authenticity of the message from MITM." - Is the statement true or false? Justify your answer with a proper explanation. **(8)**

TT#02(L)	Course: Information and Network Security (SWE 429)	Marks: 20	Time: 30 mins

1. Write down the details of the following security terms: Chosen-plaintext attack, Security by obscurity, and Compromise recording. **(4.5)**

2. I) What is the CFB(Cipher Feedback) mode of operation in cryptography? Write down the pros and cons of it. Illustrate how it works. **[4]** **(8)**
   II) Write down a short note on the RSA security mechanism. **[4]** 212 $7.5+4+4=15.5$

3. P and Q are two prime numbers. P=3, and Q=11. Take public key E=3. If the original message is 00111011 in binary format, then **(7.5)**
   I) What will be the cipher text value(in decimal) according to the RSA algorithm? **[4]**
   II) Again, calculate the decryption key for the given context. **[3.5]**

SPM; TT#1; 2024; Time: 30 min; Marks: 10

1. What is contract management? 1
2. What is a Product Breakdown Structure (PBS)? Show the hierarchical diagram of a sample PBS. 4
3. What are the activities covered by project management? Explain. 3
4. What are called "free floats" and "interfering floats"? How are they calculated? 2

SPM; Marks: 10; Time: 30 Minutes; Ct#3

1. Discuss leadership styles in software project management. How do different leadership approaches affect project success?
2. Discuss in the detail challenges of managing people in software projects. How can stress and conflict be effectively managed?

Course: SWE 431 **Course Title: Human Computer Interaction**

Time: 40 minutes **Total Marks:20**

1. ***Answer the following questions***

a) Mention two ways your design can match users' expectations (mental models). Give an example for any one of them. 2.5

b) List two pitfalls to avoid during ideation sessions and explain why. 2.5

c) Give one example of a UI metaphor and justify how it aids learnability. 2.5

d) With one example for each, define the *gulf of execution* and the *gulf of evaluation*. Mention one design principle that can help to reduce each of these gulfs. 2.5

e) Nielsen's 10 usability heuristics are widely used principles for evaluating user interfaces. 10

I. Briefly list any six of Nielsen's heuristics. (6 marks)

II. Draw one real or hypothetical software interface (e.g., a mobile app, website, or desktop program) and analyze how it supports or violates two of the heuristics you listed. (4 marks)

1) Define HCI.
2) What are the principles of HCI?
3) What are the challenges of good HCI design? Explain with examples.
4) What is thematic analysis?
5) What is a mental model? How is it developed?
6) How do you create personas?
7) You are a **user of a task scheduling app**. You currently use an app to organize your daily tasks, but you've been struggling to stay on top of them because you forget or miss important reminders. You've heard about a new version of your app that includes an **improved task reminder feature**—so now, you want to explore the app's new functionality and see if it will help you stay more organized. Create a Customer Journey Map.

2 5 1 1 2 8