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

Deep Learning

TT #01

How Deep Learning works ? Give the Flow Diagram and Explain every step. (10).

TT #02

Draw the figure of Transformer's Encoder - Decoder Architecture. Shortly explain it. (10)

- তোদের জন্য প্রশ্ন লিখে রাখলাম, ভালোমতো পারিস,
- রঞ্জু স্যার ক্লাস নিলে TT জাস্ট Diagram আঁকতে দিবেন। Xm Hall এ এসে তোরা মেইন বডে আসবি ওইটাই লিখতে দিবে স্যার। কি আমানিল্লাহ!

- Mohammad Emran (Low CGian)