NOTE: we made 136 MCQ

The estimated time for each part is indicated by E.T.

# MCQ Write the letter of the most correct answer [E.T. =30] [40 marks]

Part A: Lec1&2 Product Quality & Measuring system complexity:

1. How does increasing integrity within a system affect efficiency?

|  |  |
| --- | --- |
| 1. It improves efficiency by reducing processing overhead. | 1. It improves efficiency by increasing data accessibility. |
| 1. It reduces efficiency by adding processing overhead. | 1. It reduces efficiency by increasing system complexity. |

1. What does a lower mean time to change (MTTC) indicate about a software product?

|  |  |
| --- | --- |
| A) It improves efficiency by reducing processing overhead. | B) It improves efficiency by increasing data accessibility. |
| C) Higher maintainability | D) It reduces efficiency by increasing system complexity. |

3) What type of attack is caused by failures of the product or its users?

|  |  |
| --- | --- |
| A) Denial of service. | B) Input attacks. |
| C) Man in the middle. | D) Accidental attacks. |

1. What is the purpose of using prototypes in the development process?

|  |  |
| --- | --- |
| A) To ensure consistent and complete deliverables | B) To facilitate understanding requirements |
| C) To reduce the cost of recovery | D) To speed up the development timeline |

1. Which type of testing occurs during both developmental testing and system maintenance?

|  |  |
| --- | --- |
| A) Usability testing | B) Unit testing |
| C) Regression testing | D) Requirements-based testing |

1. Which type of system testing checks the system's ability to be started in a working hardware/software configuration?

|  |  |
| --- | --- |
| A) Performance testing | B) Security testing |
| C) Start-up and initialization testing | D) Stress testing |

1. Which type of system testing ensures that the system does not offer opportunities to breach security?

|  |  |
| --- | --- |
| A) Performance testing | B) Security testing |
| C) Start-up and initialization testing | D) Stress testing |

1. Which of the following statements best describes a system test matrix?

|  |  |
| --- | --- |
| A) It is a document that defines the expected outcomes of system tests. | B) It is a graphical representation of the test coverage in a system. |
| C) It is a document that outlines the resources required for system testing | D) It is a document that relates classes/packages to be executed during system tests. |

1. What is the significance of acceptance testing in the software development process?

|  |  |
| --- | --- |
| A) It facilitates communication between the development team and the customer. | B) It provides assurance that the system meets all Non-functional requirements. |
| C) It determines whether the system is ready for production. | D) It validates the system against predefined acceptance criteria. |

10) When does regression testing typically occur?

|  |  |
| --- | --- |
| A) During acceptance testing | B) During unit testing |
| C) During system maintenance | D) During performance testing |

1. How does McCabe's cyclomatic-complexity metric measure complexity?

|  |  |
| --- | --- |
| A) By counting the number of lines in the code | B) By counting the number of decision points in a method |
| C) By analyzing the number of function calls in the code | D) By calculating the average nesting depth of loops |

1. What is the cyclomatic complexity of Code :

int n = 10;

int result = 0;

for (int i = 1; i <= n; i++) {

if (i % 2 == 0) {

for (int j = 1; j <= i; j++) {

if (j % 3 == 0) {

for (int k = 1; k <= j; k++) {

result += k;

}

} else {

result -= j;

}

}

} else {

for (int j = 1; j <= i; j++) {

if (j % 4 == 0) {

result \*= j;

} else {

result += j;

}

}

}

}

|  |  |
| --- | --- |
| A) 7 | B) 8 |
| C)5 | D) 10 |

1. What does a DIT value of 0 indicate?

|  |  |
| --- | --- |
| A) The class has no super classes | B) The class has one superclass |
| C) The class is at the top of the inheritance hierarchy | D) The class has reached the maximum level of inheritance depth |

14) The higher the value of the CBO metric, the:

|  |  |
| --- | --- |
| A) Easier it is to understand the use of the given class | B) More difficult it is to understand the use of the given class |
| C) More likely it is to have a high NOC value | D) None of the above |

15) How does the NOC metric help in software development?

|  |  |
| --- | --- |
| A) It measures the complexity of a class | B) It determines the number of methods to be tested |
| C) It identifies the classes that are most likely to be affected by changes to a parent class | d) Neither black box nor white box testing |

16 Which type of testing ensures that each aspect of the customer's requirements is handled correctly?

|  |  |
| --- | --- |
| A) White box testing | B) Black box testing |
| C) Both black box and white box testing | D) Neither black box nor white box testing |

17) In black box testing, test cases are designed based on:

|  |  |
| --- | --- |
| A) The details of the implementation | B) The specification and requirements |
| C) The high-level design | D) The system architecture |

18) Which type of testing is more concerned with external behavior?

|  |  |
| --- | --- |
| A) Black box testing | B) White box testing |
| C) Both black box and white box testing | D) Neither black box nor white box testing |

19) What is the purpose of basis-path testing technique?

|  |  |
| --- | --- |
| A) To determine the cyclomatic complexity of the flow | B) To count the number of independent paths |
| C) To ensure that all reachable statements in a method are tested at least once | D) To prepare test cases that force execution of each path in the basis set |

20) What metric is used in basis-path testing technique?

|  |  |
| --- | --- |
| A) Halstead complexity | B) Cyclomatic complexity |
| C) McCabe complexity | D) None of the above |

21) What is the main issue with relying solely on black-box testing?

|  |  |
| --- | --- |
| A) Dependency on the internal state of an object | B) Poor coverage levels |
| C) Inability to reveal customer requirements | D) Insufficient focus on implementation code |

22) What is the main problem with relying solely on white-box testing?

|  |  |
| --- | --- |
| A) Lack of coverage in testing | B) Failure to reveal omitted customer requirements |
| C) Inability to analyze the internal state of an object | D) Dependency on the internal state of an object |

23) What is the solution to the problems of black-box and white-box testing?

|  |  |
| --- | --- |
| A) Combine black-box and white-box testing | B) Increase the coverage levels in black-box testing |
| C) Improve the focus on implementation code in white-box testing | D) Analyze the internal state of an object in black-box testing |

24) What is the main benefit of combining black-box and white-box testing??

|  |  |
| --- | --- |
| A) Ability to reveal customer requirements | B) Increased focus on implementation code |
| C) Better understanding of the internal state of an object | D) Improved coverage levels |

Part B: Lec3&4 Securing architecture:

1. Integrity is a software quality factors that belongs to ….: [2 marks]

|  |  |
| --- | --- |
| 1. revision requirements | 1. transition requirements |
| 1. operation requirements | 1. security requirements |

……………………………………….  
……………………………………….  
Part c: Lecture 2,3 - Secure SDLC, Secure SDLC, Secure coding session vulnerabilities:

1. What is a session in cybersecurity?

|  |  |
| --- | --- |
| A) ) A technique used by hackers to gain unauthorized access to a system | B) A permanent connection between a client and a server |
| C) A session is defined as a series of related browser requests that come from the same client during a certain time period. | D) A type of malware that infects a computer system |

1. \_\_\_\_\_\_\_\_\_\_\_\_\_ attack is the exploitation of the web-session and its mechanism that is usually managed with a session token,   
   XSS is \_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| A) Session Hacking, Injection of Scripts | B) Session Cracking, Injection of commands |
| C)Session Hijacking, Injection of Scripts | D)Session Compromising, Injection Parameters |

1. The most common protection mechanism against CSRF exploit

|  |  |
| --- | --- |
| A) Authentication exchange | B) Digital Signature |
| C) Bit stuffing | D)Token |

1. What type of vulnerability is clicking on a link not from a legit source where imitate the original website?

|  |  |
| --- | --- |
| A) SQL inject | B) phishing |
| C)cross site scripting | D)monitoring |

1. Which of Types XSS involves the injection of malicious code into a website's input fields work when click on link so it does not be in database of website?

|  |  |
| --- | --- |
| A) Reflected XSS | B) Stored attack |
| C)Both A and b | D) Persistent attack |

1. Which of Types XSS is persistent on the server and executed every time the user visits the infected page?

|  |  |
| --- | --- |
| A) Reflected XSS | B) Stored attack |
| C)Both A and b | D) Persistent attack |

|  |  |
| --- | --- |
| A picture containing text, screenshot, font  Description automatically generatedA) | A screen shot of a computer code  Description automatically generated with low confidenceB) |
| C) Both A&B | D) None of these |

1. Which of the following codes snippets PREVENTS XSS?
2. Which of the following code snippets PREVENTS a

Command Injection attack?

|  |  |
| --- | --- |
| A) | B) |
| C) Both A&B | D) None of these |

1. Which of the following code snippets PREVENTS a Buffer Overflow vulnerability?

|  |  |
| --- | --- |
| A) | B) |
| C) Both A&B | D) None of these |

1. Which phase of the SDLC involves defining the system requirements and creating a detailed project plan?

|  |  |
| --- | --- |
| A) Design | B) Planning |
| C) Analysis | D) Implementation |

1. What is the purpose of the testing phase in SDLC?

|  |  |
| --- | --- |
| A) To deploy the software system | B) To identify and fix defects in the software system |
| C) To maintain the software system | D) To design the software system |

1. Which of the following is true about the 3-tier architecture in the SDLC?

|  |  |
| --- | --- |
| A) The application layer is responsible for managing the user interface. | B) The presentation layer is responsible for storing and retrieving data. |
| C) The data layer is responsible for processing business logic. | D) The 3-tier architecture is not suitable for large-scale applications. |

1. Which of the following statements is true about the role of SAST and DAST in the software development lifecycle (SDLC)?

|  |  |
| --- | --- |
| A) SAST is only used during the development phase of the SDLC, while DAST is used during the testing phase. | B) SAST and DAST are not typically used in the SDLC. |
| C) SAST is used during the development phase, while DAST is used during the production phase to continuously monitor the application for vulnerabilities. | D) SAST can help identify vulnerabilities related to code design, architecture, and coding practices, while DAST analyzes the application's behavior and can identify vulnerabilities related to input and output handling, authentication, authorization, and other runtime issues. |

1. Which of the following statements is true about the advantages of DAST and SAST?

|  |  |
| --- | --- |
| A) SAST Can identify security issues in the early stages of the SDLC while DAST Can detect vulnerabilities related to runtime behavior | B) SAST Can identify vulnerabilities related to user input handling while DAST Can simulate real-world attack scenarios |
| C) both A and B. | D) None of these. |

# Part D: Lecture 1 - Cyber Security Introduction

1. What is the relation between Risk, Threat, Vulnerability?

|  |  |
| --- | --- |
| A) Risk = Threat x Vulnerability | B) Vulnerability = Threat x Risk |
| C) Threat = Risk x Vulnerability | D) there is no relation. |

1. What is the Zero Trust concept in cybersecurity and Which stage of the Kill Chain framework involves the attacker gaining control of the victim's system?

|  |  |
| --- | --- |
| A) A security approach that trusts all users and devices within a network, Reconnaissance | B) A security approach that assumes all users and devices within a network are untrusted until proven otherwise, Installation |
| C) A security approach that only trusts users with administrative privileges, Exploitation | D) A security approach that only trusts devices with the latest security updates, Command and Control |

1. What is the Zero Trust concept in cybersecurity?

|  |  |
| --- | --- |
| A) A security approach that assumes all users and devices within a network are untrusted until proven otherwise | B) A security approach that trusts all users and devices within a network |
| C) A security approach that only trusts users with administrative privileges | D) A security approach that only trusts devices with the latest security updates |

1. What is the main principle of Zero Trust?

|  |  |
| --- | --- |
| A) Verify and validate all users and devices before granting access to resources | B) Block all network traffic unless explicitly allowed |
| C) Assume that all network traffic is safe | D) Trust all users and devices by default |

5) Which of the following is not a component of the Zero Trust model?

|  |  |
| --- | --- |
| A) Firewall configuration | B) Continuous monitoring and analysis |
| C) Network segmentation | D) Identity and access management |

6) Which of the following best describes the purpose of Zero Trust?

|  |  |
| --- | --- |
| A) To reduce the attack surface of a network | B) To eliminate all security risks in a network |
| C) To maximize the speed and efficiency of network traffic | D) To increase the number of users and devices with network access |

7) Which of the following is a benefit of implementing the Zero Trust model?

|  |  |
| --- | --- |
| A) Increased visibility and control over network activity | B) Increased user productivity and flexibility |
| C) Reduced complexity and cost of network security | D) Increased network speed and performance |

8) What is the Kill Chain in cybersecurity?

|  |  |
| --- | --- |
| A) A framework for identifying and preventing cyber attacks | B) A method for tracking and recording all system activities |
| C) A tool for encrypting sensitive data | D) A type of firewall |

9) How many stages are there in the Kill Chain framework?

|  |  |
| --- | --- |
| A) 5 | B) 3 |
| C) 10 | D) 7 |

10)Which of the following is not a stage of the Kill Chain framework?

|  |  |
| --- | --- |
| A) Evasion | B) Exploitation |
| C) Reconnaissance | D) Detection |

11) What is the first stage of the Kill Chain framework?

|  |  |
| --- | --- |
| A) Reconnaissance | B) Installation |
| C) Exploitation | D) Command and Control |

12) What is the final stage of the Kill Chain framework?

|  |  |
| --- | --- |
| A) Actions on Objectives | B) Installation |
| C) Exploitation | D) Command and Control |

13) What is the purpose of the Kill Chain framework?

|  |  |
| --- | --- |
| A) To detect and respond to cyber attacks | B) To help attackers carry out successful attacks |
| C) To prevent all cyber attacks from occurring | D) To track user activity on a system |

14) What is the Defense in Depth concept in cybersecurity?

|  |  |
| --- | --- |
| A) A security approach that uses multiple layers of security to protect a network | B) A security approach that only trusts users with administrative privileges |
| C) A security approach that assumes all users and devices within a network are untrusted until proven otherwis | D) A security approach that trusts all users and devices within a network |

1. Confidentiality is important in cybersecurity because:

|  |  |
| --- | --- |
| A) It protects sensitive information from unauthorized access. | B) It prevents data from being lost or corrupted. |
| C) It ensures that data is transmitted securely. | D) It ensures that data is available when it is needed. |

1. Which of the following is an example of a breach of data integrity?

|  |  |
| --- | --- |
| A) An attacker changes the contents of a database | B) An attacker intercepts and   reads an email |
| C) An attacker deletes a database | D) An attacker floods a   network with traffic |

1. What is the definition of "availability" in cybersecurity?

|  |  |
| --- | --- |
| A) The ability to protect sensitive information from unauthorized access | B) The ability to detect and respond to security incidents in a timely manner |
| C) The ability to ensure that data is accessible and usable by authorized users when needed | D) The ability to ensure the accuracy and completeness of data |

1. Which of the following is NOT a component of AAA?

|  |  |
| --- | --- |
| A) Authentication | B) Authorization |
| C) Accounting | D) Availability |

1. Which AAA component verifies the identity of a user

|  |  |
| --- | --- |
| A) Authentication | B) Authorization |
| C) Accounting | D) All of the above |

1. Which AAA component determines what resources a user can access?

|  |  |
| --- | --- |
| A) Authentication | B) Authorization |
| C) Accounting | D) All of the above |

1. Which AAA component tracks the actions of a user?

|  |  |
| --- | --- |
| A) Authentication | B) Authorization |
| C) Accounting | D) All of the above |

1. Which of the following principles refers to restricting users' access to only the resources necessary for them to perform their job functions?

|  |  |
| --- | --- |
| A) Least Privilege | B) Need to Know |
| C) Segregation of Duties | D) All of the above |

1. Which of the following principles refers to limiting access to sensitive information to only those who require it to perform their job functions?

|  |  |
| --- | --- |
| A) Least Privilege | B) Need to Know |
| C) Segregation of Duties | D) All of the above |

1. Which of the following principles refers to separating job functions in a way that prevents any one person from having too much control over a critical system or process?

|  |  |
| --- | --- |
| A) Least Privilege | B) Need to Know |
| C) Segregation of Duties | D) All of the above |

1. Which of the following is an example of implementing the principle of Least Privilege?

|  |  |
| --- | --- |
| A) Giving all employees access to all company files and systems | B) Giving employees access only to the files and systems they need to perform their job functions |
| C) Giving employees access to all files and systems except those designated as "sensitive" | D) Giving employees access only to files and systems that are not critical to the company's operations |

1. Which of the following is an example of implementing the principle of Segregation of Duties?

|  |  |
| --- | --- |
| A) Allowing a single employee to have access to all financial records and the ability to make financial transactions | B) Separating the duties of creating financial records and approving financial transactions between two different employees |
| C) Allowing all employees to have access to financial records and transactions, but requiring two-factor authentication for all financial transactions | D) Only allowing executives to have access to financial records and transactions, with no separation of duties |

Part E: Lecture 1,2 - Intro & Operators, Substitution Caeser and Vernam

1. What does computer security aim to protect in an automated information system?

|  |  |
| --- | --- |
| 1. Hardware | 1. Software |
| 1. Information/Data | 1. Integrity |

1. Where do the majority of threats to a computer system typically originate from?

|  |  |
| --- | --- |
| 1. Internal sources | 1. External sources |
| 1. Network | 1. Software |

1. What is a cipher?

|  |  |
| --- | --- |
| 1. A type of encryption and decryption algorithm | 1. A method for data compression |
| 1. A protocol for network communication | 1. A hardware device for data storage |

1. What are symmetric ciphers?

|  |  |
| --- | --- |
| 1. Cryptographic techniques using different keys | 1. Cryptographic techniques using the same key |
| 1. Cryptographic techniques without encryption | 1. Cryptographic techniques without decryption |

1. Which ingredient of symmetric ciphers is responsible for converting the original message into an encrypted form?

|  |  |
| --- | --- |
| 1. Plaintext | 1. Encryption algorithm |
| 1. Secret Key | 1. Ciphertext |

1. What is the purpose of the secret key in symmetric ciphers?

|  |  |
| --- | --- |
| 1. Generate the plaintext | 1. Store the ciphertext |
| 1. used for encryption and decryption | 1. used for other purposes |

1. Which ingredient of symmetric ciphers represents the encrypted message?

|  |  |
| --- | --- |
| 1. Plaintext | 1. Encryption algorithm |
| 1. Ciphertext | 1. Secret Key |

1. Which ingredient of symmetric ciphers is responsible for converting the encrypted message back into its original form?

|  |  |
| --- | --- |
| 1. Plaintext | 1. Encryption algorithm |
| 1. Decryption algorithm | 1. Secret Key |

1. How many ingredients are there in symmetric ciphers?

|  |  |
| --- | --- |
| 1. 1 | 1. 2 |
| 1. 5 | 1. 3 |

1. What is the purpose of plaintext in cryptography?

|  |  |
| --- | --- |
| 1. To produce a different output | 1. To store the secret key |
| 1. To be transformed into an unreadable form | 1. To represent the scrambled message |

1. Which process is responsible for transforming the plaintext into an unreadable form?

|  |  |
| --- | --- |
| 1. Plaintext | 1. Secret Key |
| 1. Encryption Algorithm | 1. Ciphertext |

1. What is the purpose of the secret key in cryptography?

|  |  |
| --- | --- |
| 1. To produce a different output | 1. To store the encrypted message |
| 1. To transform the plaintext into ciphertext | 1. To reverse the encryption process |

1. What does the ciphertext represent in cryptography?

|  |  |
| --- | --- |
| 1. The original message to be sent | 1. The encryption algorithm used |
| 1. The scrambled message produced from encryption process | 1. The secret key |

1. What is the purpose of the decryption algorithm in cryptography?

|  |  |
| --- | --- |
| 1. To generate a secret key | 1. To produce an unreadable form of the original message |
| 1. To transform the ciphertext into plaintext | 1. To generate the plaintext |

1. In which type of cryptosystem are encryption and decryption performed using the same key?

|  |  |
| --- | --- |
| 1. Asymmetric cipher | 1. Hash function |
| 1. Symmetric cipher | 1. Public key encryption |

1. Which technique replaces letters of plaintext with other letters, numbers, or symbols to produce ciphertext?

|  |  |
| --- | --- |
| 1. Transposition technique | 1. Permutation technique |
| 1. Substitution technique | 1. Encryption technique |

1. Which technique permutes the letters of plaintext in a certain order to produce ciphertext?

|  |  |
| --- | --- |
| 1. Substitution technique | 1. Permutation technique |
| 1. Transposition technique | 1. Encryption technique |

1. Which type of cipher uses either substitution or transposition techniques?

|  |  |
| --- | --- |
| 1. Asymmetric cipher | 1. Hash function |
| 1. Symmetric cipher | 1. Public key encryption |

1. What is another name for asymmetric ciphers?

|  |  |
| --- | --- |
| 1. symmetric cipher | 1. Hash function |
| 1. Public key cryptography | 1. Encryption algorithms |

1. Which key is used for encryption in asymmetric ciphers?

|  |  |
| --- | --- |
| 1. Private key | 1. Plaintext |
| 1. Public key | 1. Ciphertext |

1. Which key is used for decryption in asymmetric ciphers?

|  |  |
| --- | --- |
| 1. Public key | 1. Plaintext |
| 1. Private key | 1. Ciphertext |

1. How are the public and private keys related in asymmetric ciphers?

|  |  |
| --- | --- |
| 1. Public key | 1. Plaintext |
| 1. They are mathematically related and form a key pair | 1. Ciphertext |

1. What type of cipher is the Caesar cipher?

|  |  |
| --- | --- |
| 1. Transposition cipher | 1. Asymmetric cipher |
| 1. Substitution cipher | 1. Other type of cipher |

1. In the Caesar cipher, what does the key represent?

|  |  |
| --- | --- |
| 1. Original plaintext | 1. Ciphertext |
| 1. Number of shifts | 1. Decryption algorithm |

1. What is the encrypted message (ciphertext) when encrypting the plaintext "fox faster than dog" using a key value of 3 in the Caesar cipher?

|  |  |
| --- | --- |
| 1. grl idvwhu wkdq ira | 1. irx idvwhu wkhq grj |
| 1. ira idvwhu wkdq grj | 1. irx idvwhu wkdq gkd |

1. What is the original plaintext message when decrypting the ciphertext "ira idvwhu wkdq grj" using a key value of 3 in the Caesar cipher?

|  |  |
| --- | --- |
| 1. dog faster than cat | 1. cat faster than dog |
| 1. fox faster than dog | 1. rat faster than dog |

1. What is the encrypted message (ciphertext) when encrypting the plaintext "Is fox faster than dog?" using a key value of 5 and the ASCII code table in the Caesar cipher?

|  |  |
| --- | --- |
| 1. Fx%kt}%kfxyjw%ymfs%itlN | 1. Nx%gt}%kgxyjw%ymfs%itlD |
| 1. Nx%kt}%kfxyjw%ymfs%itlD | 1. Fx%gt}%kgxyjw%ymfs%itlN |

1. What is the original plaintext message when decrypting the ciphertext "Nx%kt}%kfxyjw%ymfs%itlD" using a key value of 5 and the ASCII code table in the Caesar cipher?

|  |  |
| --- | --- |
| 1. Is dog faster than fox? | 1. Is cat faster than dog? |
| 1. Is fox faster than dog? | 1. Is dog faster than cat? |

1. What type of operation does the Vernam cipher use to encrypt each bit of the plaintext with the corresponding bit in the key?

|  |  |
| --- | --- |
| 1. Bitwise AND | 1. Bitwise OR |
| 1. Bitwise XOR | 1. Bitwise NOT |

1. In the Vernam cipher, what is the requirement for the key length in relation to the plaintext length?

|  |  |
| --- | --- |
| 1. The key length should be twice the plaintext length | 1. The key length should be half the plaintext length |
| 1. The key length should be equal to the plaintext length | 1. The key length is not relevant in the Vernam cipher |

1. Which type of data does the Vernam cipher operate on?

|  |  |
| --- | --- |
| 1. Letters | 1. Numbers |
| 1. Binary data | 1. ASCII characters |

1. What is the ciphertext obtained when encrypting the plaintext "Hello" with the key "12345" using the Vernam cipher algorithm?

|  |  |
| --- | --- |
| 1. tSLPQ | 1. pEDCI |
| 1. yW\_XZ | 1. kZUFA |

1. What is the original plaintext message when decrypting the ciphertext "yW\_XZ" with the key "12345" using the Vernam cipher algorithm?

|  |  |
| --- | --- |
| 1. World | 1. Cipher |
| 1. Hello | 1. Message |

Part f: Lecture 3,4 – Securing the Architecture

1. Which of the following best describes software architecture?

|  |  |
| --- | --- |
| 1. The detailed implementation of a software system's components | 1. The process of writing code for a software system. |
| 1. The broad structure and organization of a software system | 1. The testing and debugging phase of software development |

1. Which of the following statements about architectural views is correct?

|  |  |
| --- | --- |
| A) The functional view describes the concurrent aspects of the system at runtime. | B) The process view describes the main basic services and responsibilities of the system. |
| C) The functional view addresses the startup and shutdown processes of the system. | D) The deployment view maps the software elements onto the runtime environment. |

1. Which of the following architectural views describes the main basic services/functional elements, their responsibilities, interfaces, and primary interactions of a software system?

|  |  |
| --- | --- |
| A) Functional view | B) Process view. |
| C) Deployment view | D) None of the above |

1. Which architectural view addresses the concurrent aspects of the system at runtime, including system processes, startup, and shutdown?

|  |  |
| --- | --- |
| A) Functional view | B) Process view. |
| C) Deployment view | D) None of the above |

1. When should the deployment view be used in software development?

|  |  |
| --- | --- |
| A) When developing small and simple systems | B) When the system requires decomposition and is large and complex |
| C) When focusing on the communication protocols between computers | D) When dealing with the physical layer of networking |

1. Which of the following is an advantage of using a layered architecture?

|  |  |
| --- | --- |
| A) High coupling between layers | B) Lack of separation of concerns. |
| C) Improved maintainability and flexibility | D Increased replication of information across layers |

1. Which of the following is a disadvantage of using a layered architecture?

|  |  |
| --- | --- |
| A) High coupling between layers | B) Increased reusability of services |
| C) Lack of separation of concerns | D) Extra transformations at each layer leading to reduced performance |

1. The Layers pattern includes three principal layers. Which of the following is NOT one of the principal layers in the Layers pattern?

|  |  |
| --- | --- |
| A) Presentation layer | B) Application layer |
| C) Domain layer | D) Data source layer |

1. Which layer in the Layers pattern handles the interaction between the users and the system, capturing user events and the system's user interface?

|  |  |
| --- | --- |
| A) Presentation layer | B) Application layer |
| C) Domain layer | D) Data source layer |

1. Which of the following protocols is typically used for conveying SOAP messages in a Web service?

|  |  |
| --- | --- |
| A) HTTP | B) FTP |
| C) SMTP | D) SMTP |

1. What is the primary purpose of a Web service?

|  |  |
| --- | --- |
| A) 11-To support user interaction with a website | B) To facilitate machine-to-machine interaction |
| C) To enhance network security protocols | D) To provide graphical user interface (GUI) components |

1. When should the Model-View-Controller (MVC) pattern be used in software development?

|  |  |
| --- | --- |
| A) When there is a need to separate presentation from the model | B) When there is a requirement for high coupling between components |
| C) When testing is not a concern | D) When maintainability is not a priority |

1. Which component of the Model-View-Controller (MVC) pattern is responsible for managing user interactions and updating the model accordingly?

|  |  |
| --- | --- |
| A) Model | B) View |
| C) Controller | D) None of the above |

1. What is the main characteristic of services within a service-oriented architecture (SOA)?

|  |  |
| --- | --- |
| A) They are tightly coupled with the consumer application. | B) They are built as monolithic applications. |
| C) They are discoverable and location-independent. | D) They cannot be reused in different business processes. |

1. Which of the following statements is true about service-oriented architectures (SOA)?

|  |  |
| --- | --- |
| A) SOA is primarily focused on building monolithic applications. | B) SOA does not support reusability of application components. |
| C) SOA does not allow for the discovery of services. | D) SOA enables loose coupling between service providers and consumers. |

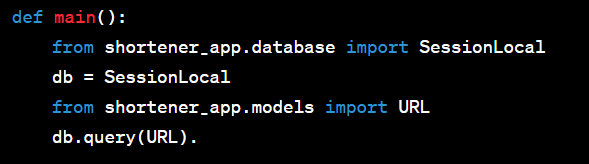
1. what is the purpose of using the route() decorator?

|  |  |
| --- | --- |
| A) To specify the URL that triggers a specific function. | B) To create an instance of the Flask application. |
| C) To import the Flask class. | D) To run the application on a local server. |

1. what is the purpose of creating an instance of the Flask application?

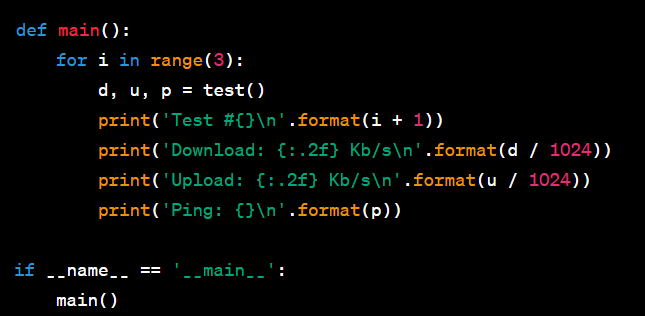
|  |  |
| --- | --- |
| A) To import the Flask class. | B) To define the name and package/module of the application. |
| C) To specify the URL that triggers a specific function | D) To run the application on a local server. |

1. What does the following code snippet accomplish?



|  |  |
| --- | --- |
| A) Defines a main() function that initializes a database session and imports the URL model, but does not execute any further code. | B) Imports the SessionLocal class from the shortener\_app.database module and assigns it to the db variable. |
| C) Imports the URL model from the shortener\_app.models module and assigns it to the db variable. | D) Establishes a connection to the database and performs a query on the URL model using the db session. |

1. What does the following Python code snippet accomplish?



|  |  |
| --- | --- |
| A) Defines a function named main() and calls the test() function three times to perform a speed test. | B) Executes a speed test three times and prints the results including download speed, upload speed, and ping time. |
| C) Formats the output of a speed test and saves it to a file using a pipe (>). | D) Reads the input from a file in a specific format and performs calculations based on the provided data. |

Part E: Lecture 3,6 – Cyber Security Part

1. The Rail Fence Cipher is a type of:

|  |  |
| --- | --- |
| A) Substitution Cipher | B) **Transposition Cipher** |
| C) Symmetric Cipher | D) Asymmetric Cipher |

1. How does the Rail Fence Cipher rearrange the letters of a message:

|  |  |
| --- | --- |
| A) By replacing each letter with a different letter | B) By swapping adjacent letters |
| C) By shifting the letters forward or backward in the alphabet | D) By writing the letters in a zigzag(diagonal) pattern along a set of numbers of rails or rows |

1. What is the purpose of Rail Fence cipher

|  |  |
| --- | --- |
| A) To compress the data | B) To authenticate messages |
| C) To ensure confidentiality of messages | D) To verify the integrity of messages |

1. Which of the following is true about the Rail Fence Cipher

|  |  |
| --- | --- |
| A) It is a highly secured encryption algorithm | B) It is resistant to attacks |
| C) It is considered manual encrypted algorithm | D) It can encrypt any messages without limitations |

1. How can message decryption occur when it is encrypted with the Rail Fence Cipher

|  |  |
| --- | --- |
| A) By reversing the steps of encryption exactly | B) By applying different transposition algorithm |
| C) By decrypting the ciphertext using a private key | D) By applying substitution cipher |

1. The number of rails in the Rail Fence cipher determines:

|  |  |
| --- | --- |
| A) The length of the ciphertext | B) The number of iterations in the encryption process |
| C) The size of the encryption key | D) The arrangement and reading order of the letters |

1. Which of the following is a disadvantage of Rail Fence Cipher:

|  |  |
| --- | --- |
| A) It is not compatible with the modern computer systems | B) It can be easily broken and decrypted easily |
| C) It requires a large memory resources to store the ciphertext | D)none of them |

1. The Columnar Transposition Cipher is a type of:

|  |  |
| --- | --- |
| A) Substitution Cipher | B) Transposition Cipher |
| C) Symmetric Cipher | D Asymmetric Cipher |

1. The order of the column in the Columnar Transposition cipher is determined by:

|  |  |
| --- | --- |
| A) The position of each letter in the plaintext | B) The order of the letter in the key |
| C) The number of times each letter appears in the plaintext | D)none of them |

1. In Columnar Transposition cipher, what is the purpose of the key in the columnar Transposition cipher:

|  |  |
| --- | --- |
| A) To authenticate messages | B) To ensure confidentially of messages |
| C) To determine the number of columns in the rearranged message | D)none of them |

11)The Rotor Machine is a cryptographic device used for:

|  |  |
| --- | --- |
| A) Data Compression | B) Authentication |
| C) Encryption and Decryption | D) Digital Signature |

12) How does the Rotor Machine achieve encryption\decryption:

|  |  |
| --- | --- |
| A) By using a complex set of mathematical algorithms | B) By applying a substitution cipher on the plaintext |
| C) By rotating the rotors to change the electrical connections | D) by swapping the adjacent letters in the plaintext |

13)What is the advantage of using a Rotor Machine for encryption compared to simple substitution ciphers:

|  |  |
| --- | --- |
| A) Increasing resistance to attacks | B) Faster encryption and decryption speed |
| C) Ability to encrypt messages of unlimited length | D) Simplicity in implementation and operation |

1. In a Rotor Machine, how does the rotor mechanism contribute to encryption:

|  |  |
| --- | --- |
| A) It generates random encryption keys | B) It performs mathematical calculations on the plaintext |
| C) It dynamically changes the encryption mapping | D) It encrypts each letter independently |

1. Stream ciphers and Block ciphers are two types of:

|  |  |
| --- | --- |
| A) Asymmetric encryption algorithms | B) Hashing algorithms |
| C) Symmetric encryption algorithm | D) Key change protocols |

1. The Feistel cipher structure is a symmetric encryption structure that:

|  |  |
| --- | --- |
| A) Uses different keys for encryption and decryption | B) Encrypts data in parallel across multiple rounds |
| C) Divides the plaintext into equal sized-blocks | D) none of them |

1. What does DES stand for:

|  |  |
| --- | --- |
| A) Data Encryption Standard | B) Data Encoding System |
| C) Digital Encryption System | D) Digital Encoding System |

1. Which cipher structure does DES use

|  |  |
| --- | --- |
| A) Feistel cipher | B) Stream cipher |
| C) Block cipher | D) Substitution cipher |

1. What is the purpose of S-boxes in DES

|  |  |
| --- | --- |
| A) To perform substitution operations | B) To generate round keys |
| C) To rotate the key bits | D)none of them |

1. What is the blocked size used by DES

|  |  |
| --- | --- |
| A) 32 bits | B) 64 bits |
| C) 56 bits | D) 48 bits |