|  |  |
| --- | --- |
| Names | IDs |
| Mohammed Mourad | 20196104 |
| Rawan AlShami | 20196097 |
| Mohammed Kelany | 20196085 |
| Catherine Maher | 20196038 |

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

# MCQ Write the letter of the most correct answer

# [E.T. =30][30 marks]

**Part 1**

**Lecture 1: Product Quality**

1. Which of the following software quality factors is affected by both product operation requirements and product transition requirements?

|  |  |
| --- | --- |
| A) Reliability | B) Maintainability |
| C) Usability | D) Portability |

1. In the context of software quality, what does the term "integrity" refer to?

|  |
| --- |
| A) How well the software meets the customer's requirements |
| B) The ability of the software to handle different operating environments |
| C) The security and protection of data within the software |
| D) The efficiency and performance of the software on the customer's hardware |

1. Which of the following measures is used to assess maintainability of a software product?

|  |  |
| --- | --- |
| A) MTTC | B) Threat attack and security attack calculations |
| C) Defects per KLOC | D) Usability testing |

1. Which type of testing focuses on checking that a software system meets the customer's requirements?

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

1. Why is regression testing necessary even after acceptance testing?

|  |
| --- |
| A) Acceptance testing only verifies that the software meets the customer's requirements, not that there are no bugs. |
| B) Regression testing helps improve the efficiency and performance of the software on the customer's hardware. |
| C) Acceptance testing and regression testing serve the same purpose and are interchangeable. |
| D) Regression testing is not necessary after acceptance testing. |

**Lecture 2: Measuring System Complexity**

1. Which approach is used to measure complexity based on the number of lines in a piece of code?

|  |  |
| --- | --- |
| A) McCabe's cyclomatic complexity metric | B) LOC |
| C) DIT | D) CBO |

1. Which metric measures the complexity of a method by counting the number of independent paths?

|  |  |
| --- | --- |
| A) McCabe's cyclomatic complexity metric | B) LOC |
| C) DIT | D) CBO |

1. Which metric measures the number of relationships a class has with other classes in an object-oriented system?

|  |  |
| --- | --- |
| A) McCabe's cyclomatic complexity metric | B) LOC |
| C) DIT | D) CBO |

1. Which testing technique ensures that all reachable statements in a method are tested at least once?

|  |  |
| --- | --- |
| A) Loop testing technique | B) Basis-path testing technique |
| C) Black box testing technique | D) White box testing technique |

1. What is the recommended approach to testing that combines black-box and white-box testing?

|  |  |
| --- | --- |
| A) Sequential simple loop tests | B) Basis-path testing technique |
| C) Loop testing technique | D) Combined black-box and white-box testing |

**Lecture 3: Securing Architecture**

1. Which architectural view addresses the concurrent aspects of a system at run-time?

|  |  |
| --- | --- |
| A) Functional View | B) Process View |
| C) Deployment View | D) Data source view |

1. Which design pattern is used to solve specific code scenarios?

|  |  |
| --- | --- |
| A) Layers architecture | B) Model View Controller (MVC) |
| C) Observer behavioral pattern | D) Data source view |

1. The Layers pattern helps to structure the architecture of a system into groups of basic services/functionalities. Which advantage is NOT associated with the Layers pattern?

|  |  |
| --- | --- |
| A) Separation of concerns | B) Lowered coupling |
| C) Replication of information across layers | D) Reusability |

1. In the Layers pattern, which layer handles the interaction between users and the system?

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

1. What are the characteristics of a service in a service-oriented architecture (SOA)?

|  |
| --- |
| A) Tight coupling, proprietary communication, and static location |
| B) Loose coupling, message-based communication, and transparent location |
| C) High coupling, direct method invocation, and dynamic location |
| D) Closed system integration, manual communication, and fixed location |

**Lecture 4: Securing Architecture**

1. Which software entity allows the lookup of services, service providers, and their location in the SOA infrastructure?

|  |  |
| --- | --- |
| A) Service | B) Consumer |
| C) Provider | D) Registry (or locator) |

1. Which technology is used for passing values in the form of (key, value) pairs and allows recursive data structures?

|  |  |
| --- | --- |
| A) XML | B) JSON |
| C) SOAP | D) HTML |

1. In the Flask framework, which decorator is used to define the URL route for a function?

|  |  |
| --- | --- |
| A) @app.route('/') | B) @app.route('/employees') |
| C) @app.route('/helloAgain') | D) @app.route('/tracks') |

1. What is the purpose of the following code snippet?

query = conn.execute("select trackid, name, composer, unitprice from tracks;")

result = {'data': [dict(zip(tuple(query.keys()), i)) for i in query.cursor]}

|  |  |
| --- | --- |
| A) Connecting to a database | B) Executing a query and fetching results |
| C) Creating a Flask application | D) Defining a route in Flask |

1. What is the purpose of the following code snippet?

s = speedtest.Speedtest()

s.get\_servers()

s.get\_best\_server()

s.download()

s.upload()

res = s.results.dict()

|  |  |
| --- | --- |
| A) Installing the speedtest-cli library | B) Sending a GET request to a web API |
| C) Testing network speed | D) Parsing JSON data |

**Lecture 1: Cyber Security Introduction**

1. What is the primary goal of cybersecurity?

|  |  |
| --- | --- |
| A) Enhancing data availability | B) Preventing unauthorized access |
| C) Facilitating data sharing | D) Optimizing network speed |

1. What is a vulnerability in the context of cybersecurity?

|  |  |
| --- | --- |
| A) The consequence of a successful cyber attack | B) The measure of potential harm resulting from a threat |
| C) The process of securing a system or network from threats | D) A weakness in a system or network that can be exploited |

1. In the equation Risk = Threat x Vulnerability, which factor represents the potential harm or negative impact?

|  |  |
| --- | --- |
| A) Risk | B) Threat |
| C) Vulnerability |  |

1. What is the purpose of conducting reconnaissance in a cyber attack?

|  |  |
| --- | --- |
| A) To deliver malware to the target system | B) To identify vulnerabilities and potential targets |
| C) To exploit a vulnerability and gain unauthorized access | D) To establish communication with a command and control server |

1. What is the purpose of the accounting component in AAA?

|  |  |
| --- | --- |
| A) Granting or denying access to resources | B) Monitoring and recording user activities and resource usage |
| C) Verifying the integrity and confidentiality of data | D) Encrypting communication channels |

1. What is the main benefit of implementing a zero trust architecture?

|  |  |
| --- | --- |
| A) Simplified access management for users | B) Reduced network complexity |
| C) Elimination of security vulnerabilities | D) Improved detection and response to security incidents |

1. What is the main principle behind defense in depth in cybersecurity?

|  |  |
| --- | --- |
| A) Concentrating security measures at a single point of failure | B) Implementing multiple layers of defense to protect against various threats |
| C) Prioritizing speed and performance over security | D) Relying solely on user awareness and training |

1. Which of the following is NOT an example of a layer in defense in depth?

|  |  |
| --- | --- |
| A) Firewalls and network segmentation | B) Intrusion detection systems and antivirus software |
| C) User authentication and access controls | D) Network monitoring and incident response |

**Lecture 2: Secure SDLC**

1. What is the purpose of conducting security testing during the SDLC?

|  |  |
| --- | --- |
| A) To validate software functionality and features | B) To ensure compatibility with different operating systems |
| C) To assess and mitigate potential security risks and vulnerabilities | D) To optimize software performance and resource utilization |

1. When should security requirements be identified in the SDLC?

|  |  |
| --- | --- |
| A) During the planning and requirements gathering phase | B) During the testing and deployment phase |
| C) During the development and coding phase | D) During the design and architecture phase |

1. Which of the following is an example of a security requirement?

|  |  |
| --- | --- |
| A) The software should provide real-time updates and notifications | B) The software must use encryption to protect sensitive data |
| C) The software should be compatible with multiple devices | D) The software must have an intuitive user interface |

1. In a 2-tier architecture, how are the components typically divided in terms of security?

|  |  |
| --- | --- |
| A) Application tier and network tier | B) Front-end and back-end |
| C) Client-side and server-side | D) Presentation tier and data tier |

1. In a 3-tier architecture, where is the security architecture typically implemented?

|  |  |
| --- | --- |
| A) Network tier | B) Data tier |
| C) Application tier | D) Presentation tier |

1. Which of the following is a key consideration in security design?

|  |  |
| --- | --- |
| A) Third-party software integration | B) Encryption and data protection mechanisms |
| C) Performance optimization techniques | D) User interface design and aesthetics |

1. Which of the following practices should be implemented during security development?

|  |  |
| --- | --- |
| A) Deployment and release management strategies | B) User acceptance testing and feedback collection |
| C) Performance testing and optimization techniques | D) Use of secure coding guidelines and best practices |

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

|  |  |
| --- | --- |
| A) DAST is more suitable for identifying configuration-related vulnerabilities. | B) SAST requires the application to be in a running state for analysis. |
| C) DAST provides a comprehensive analysis of potential code-level security issues. | D) SAST is more effective for identifying vulnerabilities during runtime. |

**Lecture 3: Secure coding session vulnerabilities**

1. What is a session in the context of web applications?

|  |  |
| --- | --- |
| A) A unique identifier assigned to each web page for tracking purposes | B) The process of encrypting data transmitted between a web browser and a server |
| C) A series of related browser requests from the same client during a certain time period | D) The time it takes for a web page to load in a browser |

1. How is a session typically maintained between a client and a server?

|  |  |
| --- | --- |
| A) Through the installation of a secure web browser extension | B) By limiting the number of concurrent users on the server |
| C) By encrypting all data exchanged during the session | D) Through the use of cookies or URL parameters |

1. What is an important security consideration when dealing with web sessions?

|  |  |
| --- | --- |
| A) Storing session data in plain text on the client-side | B) Implementing session expiration and timeout mechanisms |
| C) Using complex session identifiers for added security | D) Ensuring fast response times for session requests |

1. How can session hijacking be mitigated?

|  |  |
| --- | --- |
| A) Implementing strong password policies | B) Encrypting session data using secure protocols |
| C) Regularly monitoring and auditing session activity | D) All of the above |

1. Which of the following is a common method used in session hijacking?

|  |  |
| --- | --- |
| A) Secure Sockets Layer (SSL) encryption | B) Distributed Denial of Service (DDoS) attacks |
| C) SQL Injection | D) Cross-Site Scripting (XSS) |

1. What is Cross-Site Scripting (XSS)?

|  |  |
| --- | --- |
| A) A protocol for securely transmitting sensitive information over the internet | B) A vulnerability that allows malicious scripts to be injected into web pages |
| C) A method for authenticating user sessions in web applications | D) A technique for encrypting data transmitted between a client and a server |

1. Which of the following is a preventive measure against XSS attacks?

|  |  |
| --- | --- |
| A) Regularly updating web application frameworks | B) Using secure coding practices |
| C) Implementing strong encryption algorithms | D) Input validation and sanitization |

1. What is the main difference between Stored XSS and Reflected XSS?

|  |  |
| --- | --- |
| A) Reflected XSS can impact multiple users, while Stored XSS is specific to a single user. | B) Stored XSS requires user interaction to execute the attack, while Reflected XSS does not. |
| C) Stored XSS is more difficult to detect and mitigate compared to Reflected XSS. | D) Stored XSS targets stored data on the server, while Reflected XSS targets user input. |

1. What is the main goal of a CSRF attack?

|  |  |
| --- | --- |
| A) Extracting sensitive information from a server. | B) Manipulating user actions and performing actions on their behalf. |
| C) Gaining unauthorized access to user accounts. | D) Injecting malicious scripts into a web application. |

1. Which of the following is an effective measure to prevent CSRF attacks?

|  |  |
| --- | --- |
| A) Including anti-CSRF tokens in form submissions. | B) Implementing CAPTCHA to verify user interactions. |
| C) Enforcing the use of HTTPS for secure communication. | D) Implementing strong input validation and sanitization. |

**Part 2**

**Lecture 1: Intro and Operators**

1. What is an asymmetric cipher technique?

|  |  |
| --- | --- |
| A) DES | B) Substitution |
| C) RSA public key | D) Transposition |

1. Symmetric ciphers are cryptographic techniques in which both encryption and decryption processes use a different key

|  |
| --- |
| A) True |
| B) False |

1. Technique is one in which the letters of plaintext are permuted in some order to produce the cipher text?

|  |  |
| --- | --- |
| A) DES | B) Substitution |
| C) RSA public key | D) Tranposition |

1. Asymmetric ciphers has \_\_\_\_\_\_ ingredients

|  |  |
| --- | --- |
| A) 8 | B) 7 |
| C) 6 | D) 5 |

1. Which ingredient does the asymmetric cipher have

|  |  |
| --- | --- |
| A) Encryption algorithm | B) Decryption algorithm |
| C) Secret Key | D) Private key |

1. What is the result of 11011011 XOR 01010101?

|  |  |
| --- | --- |
| A) 10001110 | B) 10000110 |
| C) 10001111 | D) 11001110 |

**Lecture 2: Substitution Ceaser and Vernam**

A screenshot of a computer

Description automatically generated with medium confidence

1. If the key value in the Caesar cipher is 3, what is the decryption key?

|  |  |
| --- | --- |
| A) 24 | B) 3 |
| C) 23 | D) 5 |

1. In the Caesar cipher, what type of encryption algorithm is used?

|  |  |
| --- | --- |
| A) Symmetric encryption | B) Asymmetric encryption |
| C) Hashing algorithm | D) Digital signature algorithm |

1. If the plaintext is "HELLO" and the key value is 5, what is the cipher text in the Caesar cipher?

|  |  |
| --- | --- |
| A) HEOOL | B) MJQQT |
| C) HEPPO | D) JGNNQ |

1. You receive the following ciphertext using the Caesar cipher: "VSDFULQH WR WKH ZRUOG." If the key value is 3, what is the decrypted plaintext?

|  |  |
| --- | --- |
| A) REASONING IN THE WORLD. | B) SCULPTING IN THE WORLD. |
| C) SCENARIOS OF THE WORLD. | D) RECENTLY IN THE WORLD. |

1. The Caesar cipher is a type of \_\_\_\_\_\_\_\_\_\_ cipher.

|  |  |
| --- | --- |
| A) Transposition | B) Polyalphabetic |
| C) Substitution | D) Stream |

A picture containing text, number, screenshot, font

Description automatically generated

1. In the Vernam cipher, the process of encrypting plaintext with the key is done through

|  |  |
| --- | --- |
| A) Bitwise AND | B) Bitwise OR |
| C) Bitwise XOR | D) Modular arithmetic |

1. The key used in the Vernam cipher must have which of the following characteristics?

|  |  |
| --- | --- |
| 1. Longer than the plaintext | 1. Random and as long as the plaintext |
| 1. Derived from the plaintext | 1. Repeated periodically |

1. Encrypt the word "HELLO" using the Vernam cipher with the key "WORLD". What is the ciphertext?

|  |  |
| --- | --- |
| A) OLSSV | B) RFMMP |
| C) JGNNQ | D) KHOOR |

1. Decrypt the ciphertext "UMZOP" using the Vernam cipher with the key "FLOWER". What is the plaintext?

|  |  |
| --- | --- |
| A) MUSIC | B) RIVER |
| C) TIGER | D) WINGS |

**Lecture 6: DES Algorithm**

1. DES is a type of modern encryption scheme that uses \_\_\_\_\_\_\_ encryption where both the sender and receiver use the same \_\_\_\_\_\_\_ key to encrypt and decrypt messages

|  |  |
| --- | --- |
| A) Symmetric, Secret | B) Symmetric, Public |
| C) Asymmetric, Public | D) Asymmetric, Secret |

|  |
| --- |
| A) Expansion Permutation -> Compression Permutation -> S-box Substitution -> P-box Permutation |
| B) Expansion Permutation -> S-box Substitution -> P-box Permutation -> Compression Permutation |
| C) Expansion Permutation -> Compression Permutation -> P-box Permutation -> S-box Substitution |
| D) None of the above |

1. Which of the following is the correct order of execution during the 16 round encryption process?
2. Final permutation is the inverse of the initial permutation

|  |
| --- |
| A) True |
| B) False |

1. In the DES algorithm the round input is \_\_\_\_\_\_ and the key is \_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| A) Compressed, Expanded | B) Compressed, Compressed |
| C) Expanded, Compressed | D) None of the above |

1. During which rounds are key bits shifted two bits to the left?

|  |  |
| --- | --- |
| A) All 16 rounds | B) All rounds except 1, 2, 9, 16 |
| C) 1, 2, 9, 16 | D) None of the above |

1. In the DES algorithm, although the key size is 64 bits only 48 bits are used for the encryption procedure, the rest are parity bits.

|  |
| --- |
| A) True |
| B) False |

1. In the DES algorithm the key input is shortened by

|  |  |
| --- | --- |
| A) ignoring every 1st bit | B) ignoring every 8th bit |
| C) ignoring every 4th bit | D) none of the above |

1. Which stage is not part of the encryption process performed on the 32bit RPT?

|  |  |
| --- | --- |
| A) Final Permutation | B) Compression Permutation |
| C) Expansion Permutation | D) A & B |

1. Which stage is part of the encryption process performed on the 64bit PT?

|  |  |
| --- | --- |
| A) Initial Permutation | B) P-box Permutation |
| C) S-box Substitution | D) A & B |

1. Which stage is not part of the encryption process performed on the 32bit LPT?

|  |  |
| --- | --- |
| A) Final Permutation | B) Compression Permutation |
| C) Expansion Permutation | D) All of the above |

1. Compute expansion permutation on the following RPT: “1111 0000 1010 1010 1111 0000 1010 1010”

|  |
| --- |
| A) 111110 111000 010010 000111 100000 001000 010010 001001 |
| B) 011110 100001 010101 010101 011110 100001 010101 010101 |
| C) 011111 011110 110011 011011 100010 110111 001111 011111 |
| D) none of the above |

1. Suppose the output of the Expansion Permutation and Compression Permutation is as follows:

E (R0) = 011110 100001 010101 010101 011110 100001 010101 010101

K1 = 000110 110000 001011 101111 111111 000111 000001 110010

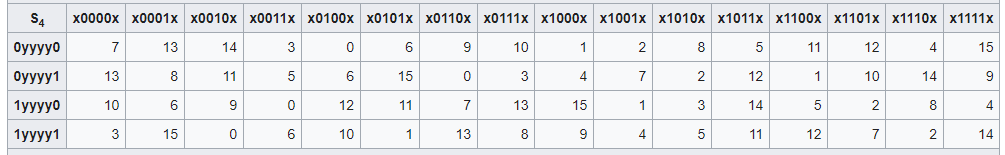
What would be the input to S-box Substitution?

|  |
| --- |
| A) 000110 100000 000001 000100 011110 000000 000001 010000 |
| B) 011110 110001 011111 111111 111111 100111 010101 110111 |
| C) 011000 010001 011110 111010 100001 100110 010100 100111 |
| D) none of the above |

1. The number of unique substitution boxes in DES are

|  |  |
| --- | --- |
| A) 6 | C) 4 |
| B) 12 | D) 8 |

1. Given the following DES S-box, and the input “100100”. What is the output produced?



|  |  |
| --- | --- |
| A) 1001 | B) 0010 |
| C) 1011 | D) 1111 |