**Software Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.** | **Process of checking that the developer is building the ‘right’ product.** | | | |
| **A** | Verification | **B** | **Validation** |
| **C** | Testing | **D** | Maintenance |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2.** | **Process of ensuring that the product being built ‘right’.** | | | |
| **A** | **Verification** | **B** | Validation |
| **C** | Testing | **D** | Maintenance |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3.** | **Software Quality Factors (SQFs) Includes** | | | |
| **A** | Product operation requirements | **B** | Product revision requirements |
| **C** | Product transition requirements | **D** | **All the mentioned** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **4.** | **Determines how well the software does what the customer wants** | | | |
| **A** | **Correctness** | **B** | Reliability |
| **C** | Efficiency | **D** | Integrity |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5.** | **Determines how well the software does what it is supposed to do** | | | |
| **A** | Correctness | **B** | **Reliability** |
| **C** | Efficiency | **D** | Integrity |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6.** | **Determines how well the system runs on the customer’s hardware** | | | |
| **A** | Correctness | **B** | Reliability |
| **C** | **Efficiency** | **D** | Integrity |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **7.** | **Determines how well the data is secured** | | | |
| **A** | Correctness | **B** | Reliability |
| **C** | Efficiency | **D** | **Integrity** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8.** | **Determines how easy the system is to use** | | | |
| **A** | Correctness | **B** | Reliability |
| **C** | Efficiency | **D** | **Usability** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **9.** | **Determines how easily bugs can be found and ﬁxed** | | | |
| **A** | **Maintainability** | **B** | Testability |
| **C** | Flexibility | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **10.** | **Determines how easily the system can be changed while in service** | | | |
| **A** | Maintainability | **B** | Testability |
| **C** | **Flexibility** | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **11.** | **Determines how easily the system can be tested to show that the customer’s requirements have been met** | | | |
| **A** | Maintainability | **B** | **Testability** |
| **C** | Flexibility | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **12.** | **Test unit of functionality of an application** | | | |
| **A** | **Unit Testing** | **B** | Integration Testing |
| **C** | Regression Testing | **D** | System Testing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **13.** | **Test units are tested together** | | | |
| **A** | Unit Testing | **B** | **Integration Testing** |
| **C** | Regression Testing | **D** | System Testing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **14.** | **It checks that fixing one bug has not introduced others.** | | | |
| **A** | Unit Testing | **B** | Integration Testing |
| **C** | **Regression Testing** | **D** | System Testing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **15.** | **Test system against the customer’s requirements.** | | | |
| **A** | Unit Testing | **B** | Integration Testing |
| **C** | Regression Testing | **D** | **System Testing** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **16.** | **Determines how easy it is to interface the system with another system** | | | |
| **A** | **Interoperability** | **B** | Maintainability |
| **C** | Reusability | **D** | Flexibility |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **17.** | **It refers to number of relationships the class has with other classes** | | | |
| **A** | **Coupling-between-objects (CBO) metric** | **B** | Number of Children (NOC) metric |
| **C** | All of the above | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **18.** | **Singletons Creational pattern is a** | | | |
| **A** | Microservice Pattern | **B** | Testing Pattern |
| **C** | **Design Pattern** | **D** | Architecture Pattern |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **19.** | **JSON stands for** | | | |
| **A** | **JavaScript Object Notation** | **B** | JavaScript Object Normalization |
| **C** | Java Object Notation | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **20.** | **Used to sign session cookies for protection against cookie data tampering** | | | |
| **A** | Public Key | **B** | OTP Key |
| **C** | **Private Key** | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **21.** | **It refers to the broad structure of a software system, it describes its major parts, and how they are put together and interact** | | | |
| **A** | Software Requirements | **B** | Software Testing |
| **C** | Software Maintainability | **D** | **Software Architecture** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **22.** | **Software architectural views are** | | | |
| **A** | Logical | **B** | Process |
| **C** | Deployment | **D** | **All the mentioned** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **23.** | **is an approach to build enterprise systems that deliver application functionality either as services to end-user applications or to build other services.** | | | |
| **A** | **Service-oriented architecture** | **B** | Web Service architecture |
| **C** | Microservice architecture | **D** | MVC architecture |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **24.** | **software module designed to support interoperable machine-to-machine interaction over a network** | | | |
| **A** | Service-oriented architecture | **B** | **Web Service** |
| **C** | Microservice architecture | **D** | MVC architecture |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **25.** | **{**  **"Name": "Sanad",**  **"Author": "Khaled Shawki",**  **"mail": "khalid@gamil.com"**  **}**  **The Previous code is an example of the format:** | | | |
| **A** | **JSON** | **B** | JSX |
| **C** | XML | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **26.** | **<employees>   <employee>     <firstName>Khaled</firstName>**  **<lastName>Shawki</lastName>   </employee> </employees>**  **The Previous code is an example of the format:** | | | |
| **A** | JSON | **B** | JSX |
| **C** | **XML** | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **27.** | **It refers to the exploitation of a valid session assigned to a user.** | | | |
| **A** | **Session Hijacking** | **B** | Cross-site scripting |
| **C** | Authentication | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **28.** | **Used for static analysis will take your code as input and analyze each line for any insecure functions or coding practices** | | | |
| **A** | **SAST** | **B** | DAST |
| **C** | NAST | **D** | KAHA |

**Use the following code to answer questions 29 to 39**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42 | **from** **flask** **import** Flask, jsonify, request  app = Flask(\_\_name\_\_)  # Sample data  books = [  {'id': **1**, 'title': 'Book 1'},  {'id': **2**, 'title': 'Book 2'}  ]    **@app**.route('/books', methods=['GET'])  **def** **get\_books**():  **return** jsonify(books)    **@app**.route('/books/<int:book\_id>', methods=['GET'])  **def** **get\_book**(book\_id):  book = next((book **for** book **in** books **if** book['id'] == book\_id), **None**)  **if** book:  **return** jsonify(book)  **else**:  **return** jsonify({'error': 'Book not found'}), **404**  **@app**.route('/books', methods=['POST'])  **def** **create\_book**():  new\_book = {'id': len(books) + **1**, 'title': request.json['title']}  books.append(new\_book)  **return** jsonify(new\_book), **201**  **@app**.route('/books/<int:book\_id>', methods=['DELETE'])  **def** **delete\_book**(book\_id):  book = next((book **for** book **in** books **if** book['id'] == book\_id), **None**)  **if** book:  books.remove(book)  **return** jsonify({'message': 'Book deleted'})  **else**:  **return** jsonify({'error': 'Book not found'}), **404**  **if** \_\_name\_\_ == '\_\_main\_\_':  app.run() |

|  |  |  |
| --- | --- | --- |
| **1.** | **What is the purpose of the Flask library in this code?** | |
| **A** | **To handle HTTP requests and responses** |
| **B** | To store and retrieve data |
| **C** | To perform database operations |
| **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2.** | **What HTTP status code will be returned if a requested book is not found?** | | | |
| **A** | 200 OK | **B** | 201 Created |
| **C** | 400 Bad Request | **D** | **404 Not Found** |

|  |  |  |
| --- | --- | --- |
| **29.** | **What does the “/books” route with the GET method do?** | |
| **A** | **Retrieves all books from the database** |
| **B** | Creates a new book in the database |
| C | Deletes a specific book from the database |
| **D** | Updates a specific book in the database |

|  |  |  |
| --- | --- | --- |
| **30.** | **What does the “/books/<int:book\_id>” route with the GET method do?** | |
| **A** | Retrieves all books from the database |
| **B** | Creates a new book in the database |
| **C** | Deletes a specific book from the database |
| **D** | **Get a specific book in the database** |

|  |  |  |
| --- | --- | --- |
| **31.** | **What does the “/books” route with the POST method do?** | |
| **A** | Retrieves all books from the database |
| **B** | **Creates a new book in the database** |
| **C** | Deletes a specific book from the database |
| **D** | Updates a specific book in the database |

|  |  |  |
| --- | --- | --- |
| **32.** | **What is the purpose of the “Jsonify” function in this code?** | |
| **A** | Converts JSON data to Python objects |
| **B** | **Converts Python objects to JSON data** |
| **C** | Converts JSON data to HTML format |
| **D** | Converts HTML format to JSON data |

|  |  |  |
| --- | --- | --- |
| **33.** | **How are new books added to the books list?** | |
| **A** | By using the GET method on the ‘/books’ route |
| **B** | **By using the POST method on the ‘/books’ route** |
| **C** | By using the DELETE method on the ‘/books’ route |
| **D** | By using the PUT method on the ‘/books/<int:book\_id>’ route |

|  |  |  |
| --- | --- | --- |
| **34.** | **What is the purpose of the if \_\_name\_\_ == '\_\_main\_\_': condition at the end of the code?** | |
| **A** | **It ensures the code is only executed if the script is run directly** |
| **B** | It checks if the server is running in the main thread |
| **C** | It defines the main function for the Flask application |
| **D** | It imports the necessary modules for the Flask application |

|  |  |  |
| --- | --- | --- |
| **35.** | **What is the purpose of the 404 status code in this code?** | |
| **A** | Indicates a successful request |
| **B** | Indicates a resource was created successfully |
| **C** | Indicates a client error |
| **D** | **Indicates a server error** (resource not found) |

|  |  |  |
| --- | --- | --- |
| **36.** | **How are the book objects stored in memory in this code?** | |
| **A** | In a local file on the server |
| **B** | In a remote database |
| **C** | **In a list called books** |
| **D** | In a text file |

|  |  |  |
| --- | --- | --- |
| **37.** | **What is the endpoint to retrieve all books?** | |
| **A** | **‘http://127.0.0.1/books’** |
| **B** | ‘http://127.0.0.1/books/int:book\_id’ |
| **C** | ‘http://127.0.0.1/str:book\_title’ |
| **D** | ‘http://127.0.0.1/books/all’ |

|  |  |  |
| --- | --- | --- |
| **38.** | **What is the response code when a book is successfully deleted?** | |
| **A** | **204** |
| **B** | 200 |
| **C** | 201 |
| **D** | 400 |

|  |  |  |
| --- | --- | --- |
| **39.** | **Which library is imported to handle HTTP requests and responses in the code?** | |
| **A** | Flask |
| **B** | Jsonify |
| **C** | Request |
| **D** | Python |

|  |  |  |
| --- | --- | --- |
| **40.** | **Which of the following best describes a threat in software security?** | |
| **A** | A weakness or flaw in software code |
| **B** | **An event or circumstance that has the potential to cause harm to software** |
| **C** | The likelihood of a software system being attacked |
| **D** | The impact or consequence of a security breach |

|  |  |  |
| --- | --- | --- |
| **41.** | **What is a vulnerability in software security?** | |
| **A** | The likelihood of a security incident occurring |
| **B** | **A weakness or flaw in software that can be exploited** |
| **C** | The potential harm caused by a security incident |
| **D** | The level of risk associated with a software system |

|  |  |  |
| --- | --- | --- |
| **42.** | **Risk in software security is defined as:** | |
| **A** | The combination of threats and vulnerabilities |
| **B** | The likelihood of a security incident occurring |
| **C** | **The potential impact or consequence of a security incident** |
| **D** | The measures in place to protect against threats and vulnerabilities |

|  |  |  |
| --- | --- | --- |
| **43.** | **Which of the following best defines confidentiality?** | |
| **A** | **Protecting information from unauthorized disclosure** |
| **B** | Ensuring that information is accurate and reliable |
| **C** | Making information available when needed |
| **D** | Ensuring that information is not altered or tampered with |

|  |  |  |
| --- | --- | --- |
| **44.** | **What does the integrity principle of the CIA triad in security refer to?** | |
| **A** | Keeping information confidential and preventing unauthorized access |
| **B** | **Ensuring that information is accurate, complete, and trustworthy** |
| **C** | Making sure that information is available and accessible |
| **D** | Safeguarding information against loss or destruction |

|  |  |  |
| --- | --- | --- |
| **45.** | **Availability, as a principle of the CIA triad, means:** | |
| **A** | **Ensuring that information is accessible to authorized individuals** |
| **B** | Protecting information from unauthorized modification or deletion |
| **C** | Maintaining the privacy and secrecy of sensitive information |
| **D** | Verifying the accuracy and consistency of information |

|  |  |  |
| --- | --- | --- |
| **46.** | **What is the primary purpose of authentication in cybersecurity?** | |
| **A** | Ensuring data confidentiality |
| **B** | **Verifying the identity of users or entities** |
| **C** | Controlling access to resources |
| **D** | Monitoring and logging user activities |

|  |  |  |
| --- | --- | --- |
| **47.** | **What does authorization refer to in the context of AAA?** | |
| **A** | Verifying the integrity of data |
| **B** | Ensuring data availability |
| **C** | **Granting or denying access to specific resources** |
| **D** | Recording and tracking user actions |

|  |  |  |
| --- | --- | --- |
| **48.** | **What is the role of accounting in AAA?** | |
| **A** | Authenticating users and entities |
| **B** | Authorizing access to resources |
| **C** | **Recording and tracking user activities and resource usage** |
| **D** | Encrypting data to protect its confidentiality |

|  |  |  |
| --- | --- | --- |
| **49.** | **What is the purpose of Segregation of Duties in cybersecurity?** | |
| **A** | **Preventing conflicts of interest and reducing the risk of fraud or unauthorized activities** |
| **B** | Ensuring that all users have the same level of access to resources |
| **C** | Granting users access to resources based on their job titles |
| **D** | Sharing administrative privileges among all users |

|  |  |  |
| --- | --- | --- |
| **50.** | **What does the principle of Need to Know in cybersecurity entail?** | |
| **A** | Providing users with access to all available information |
| **B** | **Restricting access to sensitive information to only those who require it for their job responsibilities** |
| **C** | Giving all users the same level of access to data and resources |
| **D** | Sharing sensitive information with anyone who asks for it |

|  |  |  |
| --- | --- | --- |
| **51.** | **What is the principle of Least Privilege in cybersecurity?** | |
| **A** | **Providing users with the minimum level of access necessary to perform their job functions** |
| **B** | Sharing all available information with every user |
| **C** | Granting administrative privileges to all users for convenience |
| **D** | Assigning the highest level of access to all users by default |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **52.** | **XSS (Cross-Site Scripting) is a vulnerability that primarily affects:** | | | |
| **A** | **Web browsers** | **B** | Database systems |
| **C** | Network Infrastructure | **D** | Network infrastructure |

|  |  |  |
| --- | --- | --- |
| **53.** | **Which of the following best describes SQL Injection?** | |
| **A** | A technique used to inject malicious scripts into web pages viewed by users |
| **B** | **A method of gaining unauthorized access to a database by manipulating SQL queries** |
| **C** | A type of malware that spreads through SQL databases |
| **D** | A method of intercepting network traffic to obtain sensitive information |

|  |  |  |
| --- | --- | --- |
| **54.** | **What is the main goal of an attacker in an XSS or SQL Injection attack?** | |
| **A** | To gain administrative access to the target system |
| **B** | **To extract sensitive information from the target system** |
| **C** | To disrupt the availability of the target system |
| **D** | To install malware on the target system |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **55.** | **process of transforming the plaintext into an unreadable form** | | | |
| **A** | **Encryption** | **B** | Decryption |
| **C** | Transposition | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **56.** | **It is a substitution technique that shifts each letter of the plaintext by number of places which is the key to produce the ciphertext** | | | |
| **A** | **Caesar cipher** | **B** | Vernam cipher |
| **C** | Encryption | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **57.** | **It is a substitution technique that shifts each letter of the plaintext by number of places which is the key to produce the ciphertext** | | | |
| **A** | **Caesar cipher** | **B** | Vernam cipher |
| **C** | Encryption | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **58.** | **It is a substitution technique that implements exclusive or operation (^) on each bit of plaintext with the corresponding bit in key, thus the key length must equal to the plaintext length.** | | | |
| **A** | Caesar cipher | **B** | **Vernam cipher** |
| **C** | Transposition ciphers | **D** | Rail fence cipher |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **59.** | **It is written as a sequence of diagonals with any depth and then read off as a sequence of rows.** | | | |
| **A** | Caesar cipher | **B** | Vernam cipher |
| **C** | Transposition ciphers | **D** | **Rail fence cipher** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **60.** | **Write letters of message out in rows over a specified number of columns. Then reorder the columns according to some key before reading off the rows.** | | | |
| **A** | Caesar cipher | **B** | Vernam cipher |
| **C** | **Transposition ciphers** | **D** | Rail fence cipher |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **61.** | **Which of the following is not an example of a block cipher?** | | | |
| **A** | DES | **B** | **Caesar cipher** |
| **C** | IDEA | **D** | Twofish |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **62.** | **This helps in identifying the origin of information and authentic user. This referred to here as** | | | |
| **A** | **Authenticity** | **B** | Availability |
| **C** | Integrity | **D** | Confidentiality |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **63.** | **\_\_\_\_ of information means, only authorised users are capable of accessing the information.** | | | |
| **A** | Availability | **B** | Integrity |
| **C** | **Confidentiality** | **D** | Non-repudiation |

|  |  |  |
| --- | --- | --- |
| **64.** | **CIA triad is also known as** | |
| **A** | NIC (Non-repudiation, Integrity, Confidentiality) |
| **B** | AIN (Availability, Integrity, Non-repudiation) |
| **C** | AIC (Authenticity, Integrity, Confidentiality) |
| **D** | **AIC (Availability, Integrity, Confidentiality)** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **65.** | **Which number of independent paths of the following adds 1 to cyclomatic complexity, start counting from 1:** | | | |
| **A** | **(while, do while, for) loops** | **B** | Variable initialization |
| **C** | Assign operation | **D** | None of the above |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **66.** | **What is the purpose of the route() decorator in Flask?** | | | |
| **A** | To create instance of the Flask application | **B** | To import the Flask class |
| **C** | **To trigger a specific URL for a function** | **D** | To generate URLs for a particular function |

|  |  |  |  |
| --- | --- | --- | --- |
| **67.** | **What is the DIT for class C11** | | A picture containing diagram, plan, sketch, technical drawing  Description automatically generated |
| **A** | 1 |
| **B** | 2 |
| **C** | 3 |
| **D** | 4 |
| **68.** | **What is the DIT for class C213, C2** | |
| **A** | 3,1 |
| **B** | 2,0 |
| **C** | 3,0 |
| **D** | 1,0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **69.** | **If (Condition 1)**  **Statement 1**  **Else**  **Statement 2**  **If (Condition 2)**  **Statement 3**  **Else**  **Statement 4**  **Cyclomatic Complexity for this program will be** | | | |
| **A** | **3** | **B** | 2 |
| **C** | 1 | **D** | 4 |

**Use the following problem to answer questions 70 to 72**

A web server has been running for a month. From the log ﬁles for that month we see that, of 2500 accesses, 120 attacks were made. Of these, 60 were denial-of-service attacks, of which 10 were successful, 35 were password guessing (of which none were successful) and 25 were accidental attacks (caused by errors on the part of the user), of which 25 were successful

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **70.** | **Denial of service threat, security** | | | |
| **A** | 10/2500, 10/60 | **B** | 10/2500, 10/50 |
| **C** | **60/2500, 50/60** | **D** | 60/2500, 50/50 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **71.** | **Password guessing threat, security** | | | |
| **A** | 35/2500, 0/35 | **B** | 0/2500, 0/35 |
| **C** | **35/2500, 35/35** | **D** | 0/2500, 35/35 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **72.** | **Accidental threat, security** | | | |
| **A** | 25/2000, 0/25 | **B** | **25/2500, 0/25** |
| **C** | 0/2500, 0/25 | **D** | 25/2500, 25/25 |

**Part 2: Use the following problem to answer questions 73 to 83**

You intercepted the following encrypted message: "Ymj vznhp gwtbs ktc ozruji tajw ymj qfed itl". It appears to be encrypted using a Caesar Cipher with a certain key. Decrypt the message and find the original plaintext.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **73.** | **What encryption technique is likely used to encrypt the intercepted message?** | | | |
| **A** | Substitution Cipher | **B** | Vernam Cipher |
| **C** | Caesar Cipher | **D** | S-box |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **74.** | **In a Caesar Cipher, what is the key?** | | | |
| **A** | A random sequence of letters | **B** | A matrix of substitution letters |
| **C** | **A numerical value indicating the shift** | **D** | A combination of numbers and symbols |

|  |  |  |
| --- | --- | --- |
| **75.** | **If the key for the Caesar Cipher used to encrypt the intercepted message is 5, what is the decrypted message?** | |
| **A** | **"The quick brown fox jumps over the lazy dog"** |
| **B** | "Xli szivw gwtbs lazmr qefp ymj rkdu mxp" |
| **C** | "Sgd pthbj aqnvm cnu htslq zmcv sgd kxwv bmf" |
| **D** | "Rfc ocrfg xliji wjmf ufybnsl nyhts qfsg" |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **76.** | **If the key for the Caesar Cipher used to encrypt the intercepted message is 5, what is the decrypted message?** | | | |
| **A** | Shift Cipher | **B** | One-Time Pad |
| **C** | Substitution Cipher | **D** | Transposition Cipher |

|  |  |  |
| --- | --- | --- |
| **77.** | **In a Substitution Cipher, how is the substitution determined?** | |
| **A** | By applying a matrix transformation |
| **B** | By using bitwise XOR operations |
| **C** | By shifting the letters of the alphabet |
| **D** | By using a pre-defined table of letter mappings |

|  |  |  |
| --- | --- | --- |
| **78.** | **The S-boxes are commonly used in which encryption algorithm?** | |
| **A** | They perform substitution operations on plaintext or ciphertext |
| **B** | They generate random keys for each encryption session |
| **C** | They perform transposition operations on plaintext or ciphertext |
| **D** | They combine multiple encryption techniques |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **79.** | **Which cipher uses a fixed substitution table known as the Caesar box?** | | | |
| **A** | Caesar Cipher | **B** | Rail Fence Cipher |
| **C** | Vernam Cipher | **D** | Playfair Cipher |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **80.** | **Which encryption technique guarantees perfect secrecy if used correctly?** | | | |
| **A** | Vernam Cipher | **B** | Substitution Cipher |
| **C** | S-box | **D** | Caesar Cipher |

|  |  |  |
| --- | --- | --- |
| **81.** | **If a Vernam Cipher is used with a truly random key of the same length as the plaintext, what can be said about the security of the encrypted message?** | |
| **A** | It is unbreakable and provides perfect secrecy. |
| **B** | It can be easily decrypted using frequency analysis. |
| **C** | The security depends on the strength of the key. |
| **D** | The encryption is vulnerable to brute-force attacks. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **82.** | **The S-boxes are commonly used in which encryption algorithm?** | | | |
| **A** | AES | **B** | RSA |
| **C** | DES | **D** | Diffie-Hellman |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **83.** | **Which of the following encryption techniques is based on the concept of bitwise XOR operations?** | | | |
| **A** | Substitution Cipher | **B** | Vernam Cipher |
| **C** | Caesar Cipher | **D** | S-box |

**PART 3: True & False**

|  |  |  |
| --- | --- | --- |
| **1.** | **Risk and vulnerabilities are the same things.** | F |
| **2.** | **SQL Injection is a one of Common Software Vulnerabilities.** | T |
| **3.** | **Cross-site Scripting is not a one of Common Software Vulnerabilities.** | F |
| **4.** | **Passive attack related to message modification.** | F |
| **5.** | **Active attack related to message reading only.** | F |
| **6.** | **Palin text is not a component of block cipher model.** | F |
| **7.** | **All users must have the same privilege.** | F |
| **8.** | **No need for input validation** | F |
| **9.** | **Validation is occurring on client-side only** | F |
| **10.** | **You must check for input validity at the server** | T |
| **11.** | **block cipher using key with length 128 bits is more secure than 64 bits.** | T |
| **12.** | **Security steps begin after software design.** | F |
| **13.** | **For Critical data you must not use http request rather than https** | T |
| **14.** | **DES is a asymmetric block cipher** | F |
| **15.** | **DES used in digital signature** | F |
| **16.** | **Phishing attacks can exploit any user even if they refuse to give information or have awareness.** | F |