|  |  |
| --- | --- |
| Name | ID |
| Mohammed Khaled | 20196068 |
| Mariam Mohamed | 20196052 |
| Mahmoud Mostafa | 20196009 |
| Hamdi Hossam | 20196019 |
| Ahmed Ashraf | 20196065 |
| Farah Ahmed | 20196088 |
| Ahmed Khaled | 20196005 |

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 Intro & Operators:

1. What is Cipher? [2 marks]

|  |  |
| --- | --- |
| 1. A programming language | 1. A type of computer virus |
| 1. algorithm for performing encryption or decryption | 1. A hardware component in a computer system |

1. Why is a Cipher used? [2 marks]

|  |  |
| --- | --- |
| 1. To enhance computer performance | 1. To improve data storage efficiency |
| 1. To enable faster data transmission | 1. To protect against attacks |

1. How do asymmetric ciphers differ from symmetric ciphers? [2 marks]

|  |  |
| --- | --- |
| 1. Asymmetric ciphers use the same key for encryption and decryption | 1. Asymmetric ciphers use different keys for encryption and decryption |
| 1. Asymmetric ciphers are more vulnerable to brute-force attacks | 1. Asymmetric ciphers are faster in terms of encryption speed |

1. In a symmetric cipher, which technique involves permuting the letters of plaintext to generate the ciphertext? [2 marks]

|  |  |
| --- | --- |
| 1. Substitution technique | 1. Transposition technique |
| 1. Hybrid technique | 1. Exclusive OR technique |

1. Which of the following processes involves transforming ciphertext back into plaintext using a specific algorithm or key? [2 marks]

|  |  |
| --- | --- |
| 1. Encryption | 1. Encoding |
| 1. Decoding | 1. Decryption |

1. What is the result of performing a bitwise OR operation between these two binary values?

11001011

10110110 [2 marks]

|  |  |
| --- | --- |
| 1. 11111111 | 1. 00000010 |
| 1. 11111101 | 1. 10101001 |

Part B: Lec 2 (Substitution Ceaser and Vernam):

1. What is the meaning of cipher in cryptography? [2 marks]

|  |  |
| --- | --- |
| 1. an algorithm that performs encryption | 1. an algorithm that generates a secret code |
| 1. a secret code | 1. an algorithm that performs encryption or decryption |

1. Encrypt the word ***alphabet*** using a Caesar cipher with a shift of 3: [2 marks]

|  |  |
| --- | --- |
| 1. dvsdulqv | 1. doofohdu |
| 1. doskdehw | 1. dorqhbhv |

1. A Caesar cipher is an example of a …..: [2 marks]

|  |  |
| --- | --- |
| 1. transposition cipher | 1. substitution cipher |
| 1. substantial cipher | 1. bimodal cipher |

1. What is cryptanalysis? [2 marks]

|  |  |
| --- | --- |
| 1. process of ciphering plain text messages. | 1. None of the answers |
| 1. process of deciphering coded messages with being told the key. | 1. process of deciphering coded messages without being told the key. |

1. A Vernam cipher is an example of a …..: [2 marks]

|  |  |
| --- | --- |
| 1. substitution cipher | 1. mono-alphabetic cipher |
| 1. transposition cipher | 1. additive cipher |

1. In which of the following cipher the plain text and the ciphered text does not have a same number of letters? [2 marks]

|  |  |
| --- | --- |
| 1. Vernam cipher | 1. affine cipher |
| 1. columnar cipher | 1. keyword cipher |

1. For each character in ciphertext c

if (c - k) < 0 then

p = c – k + alphabet\_count

else

p = c – k

End for

What does the above code do? [2 marks]

|  |  |
| --- | --- |
| 1. encrypt with Caesar algorithm | 1. encrypt with Vernam algorithm |
| 1. decrypt Caesar cipher | 1. decrypt Vernam cipher |

1. Use Caesar’s Cipher to decipher the following

HQFUBSWHG WHAW [2 marks]

|  |  |
| --- | --- |
| 1. ABANDONED LOCK | 1. ENCRYPTED TEXT |
| 1. ABANDONED TEXT | 1. ENCRYPTED LOCK |

1. You are required to use Caesar algorithm to encrypt a message and key = 4, what equation should be used? p stands for plaintext and c stands for ciphertext [2 marks]

|  |  |
| --- | --- |
| 1. c = (p+4) mod 26 | 1. p = (c+4) mod 26 |
| 1. c = (p+26) mod 4 | 1. p = (c+26) mod 4 |

1. What logical operator does Vernam algorithm use? [2 marks]

|  |  |
| --- | --- |
| 1. XOR | 1. OR |
| 1. AND | 1. XNOR |

1. Vernam algorithm works on …: [2 marks]

|  |  |
| --- | --- |
| 1. Binary Data | 1. Character Data |
| 1. Binary and character data | 1. None of the above |

1. In Caesar algorithm, the cipher text is ….: [2 marks]

|  |  |
| --- | --- |
| 1. Numbers and letters | 1. Numbers, symbols and letters |
| 1. Letters only | 1. Symbols and letters |

Part C: Lec3 Transposition & Rotor Machine:

1. In a particular encryption scheme, the plaintext is written as a sequence of diagonals with any depth, and then read off as a sequence of rows. What encryption technique is being used? [2 marks]

|  |  |
| --- | --- |
| 1. Substitution cipher | 1. Transposition cipher |
| 1. Rail fence cipher | 1. Columnar transposition cipher |

1. Encrypt the plaintext “we love Dr Hussein” with depth (rails) = 3, what will be the ciphertext sequence when read off as a sequence of rows? [2 marks]

|  |  |
| --- | --- |
| 1. woDue evrsi lehsn | 1. we Dri oseve nulH |
| 1. wvHse eerui loDsn | 1. wuol nHeeDvris leo |

1. what is the Rail fence decryption parameters? [2 marks]

|  |  |
| --- | --- |
| 1. Depth (d), Ciphertext (c) | 1. Plaintext (p), Ciphertext (c) |
| 1. Depth (d), Plaintext (p) | 1. Only Depth (d) |

1. What is a key characteristic of a Rotor Machine, a class of systems known for its application of multiple stages of encryption? [2 marks]

|  |  |
| --- | --- |
| 1. It employs a network of interconnected nodes to perform complex mathematical calculations. | 1. It relies on a series of substitution tables to replace plaintext characters with ciphertext characters. |
| 1. It utilizes a combination of transposition and substitution techniques to encrypt messages. | 1. It utilizes a set of rotating discs with electrical connections between input and output pins. |

1. Rotor Machines are known for their strength in encryption. What makes them particularly difficult to break? [2 marks]

|  |  |
| --- | --- |
| 1. Because of the complex internal wiring connections. | 1. Because one plain letter has many ciphered letters. |
| 1. Because It eliminates any patterns that can be exploited by cryptanalysts. | 1. Because each plaintext letter has multiple corresponding ciphertext letters. |

1. When comparing a rotor machine with a single cylinder to a rotor machine with multiple cylinders, which configuration is generally considered better in terms of encryption strength and security? [2 marks]

|  |  |
| --- | --- |
| 1. The rotor machine with a single cylinder. | 1. The rotor machine with multiple cylinders. |
| 1. Both configurations provide similar levels of encryption strength. | 1. It depends on the specific requirements and context of the encryption application. |

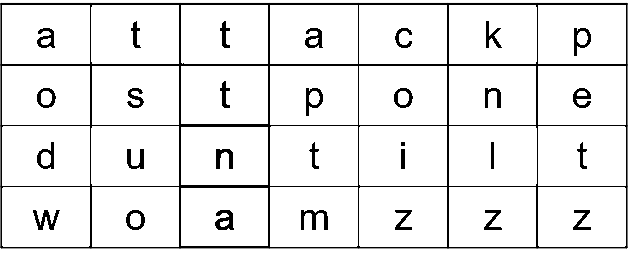
1. In a particular encryption scheme, the letters of a message are written out in rows over a specified number of columns. Then, the columns are reordered according to a specific key before reading off the rows. What is the name of this encryption technique? [2 marks]

|  |  |
| --- | --- |
| 1. Substitution cipher | 1. Rail Fence cipher |
| 1. Columnar Transposition cipher | 1. Rotor Machine cipher |

1. What is the Columnar Transposition encryption parameters? [2 marks]

|  |  |
| --- | --- |
| 1. Key (k), Plaintext (p) | 1. Key (k), Ciphertext (c) |
| 1. Depth (d), Plaintext (p) | 1. Plaintext (p), Ciphertext (c) |

1. What will be the ciphertext if we used the key '4312567'?

 [2 marks]

|  |  |
| --- | --- |
| 1. aptm coiz tsuo petz aodw knlz ttna | 1. petz knlz coiz aodw tsuo aptm ttna |
| 1. ttna tsuo knlz aodw coiz petz aptm | 1. ttna aptm tsuo aodw coiz knlz petz |

1. What happens in a three-rotor machine model after every complete rotation of the inner cylinder? [2 marks]

|  |  |
| --- | --- |
| 1. the middle cylinder rotates one pin position. | 1. the outer cylinder rotates one pin position. |
| 1. the inner cylinder rotates one pin position | 1. Nothing happens |

Part D: Lec4&5 Software Engineering & Secure Coding:

1. which of the following is not a type of injection attacks:

|  |  |
| --- | --- |
| 1. SQL injection | 1. cross-site scripting (XSS) |
| 1. CSRF | 1. Command injection |

1. Which of the following is the type of sql injection attack?

| 1. It inserts the data | 1. It updates the data |
| --- | --- |
| 1. It deletes the data | 1. All of the above |

1. Select the correct statement which will return all the rows from the Table and then also deletes the Table\_Add table

|  |  |
| --- | --- |
| 1. SELECT \* FROM Table; DROP TABLE Table\_Add | 1. SELECT \* WHERE Table; DROP TABLE Table\_Add |
| 1. SELECT \* FROM Table; DELETE TABLE Table\_Add | 1. SELECT \* WHERE Table; DELETE TABLE Table\_Add |

1. Which of the following statements is TRUE about SQL Injection?

|  |  |
| --- | --- |
| 1. SQL Injection is an Object Penetration Technique | 1. SQL Injection is a Function Penetration Technique |
| 1. SQL Injection is a Code Penetration Technique | 1. SQL Injection is a Database Penetration Technique |

1. All of the above are techniques used to mitigate SQL injection attacks except

|  |  |
| --- | --- |
| 1. mysqli\_real\_escape\_string() | 1. str\_replace() |
| 1. Prepared statements | 1. sqli\_replace() |

1. Which type of XSS attack is the most simple

|  |  |
| --- | --- |
| 1. Reflected XSS | 1. DOM-based XSS |
| 1. Stored XSS |  |

1. A type of XSS that stores malicious code on the application server

|  |  |
| --- | --- |
| 1. Reflected XSS | 1. Stored XSS |
| 1. DOM-based XSS | 1. Virtual XSS |

1. Involves injecting malicious executable code into an HTTP response.

|  |  |
| --- | --- |
| 1. Stored XSS | 1. DOM-based XSS |
| 1. Reflected XSS | 1. Virtual XSS |

1. Where the vulnerability exists in client-side code rather than server-side code.

|  |  |
| --- | --- |
| 1. Stored XSS | 1. DOM-based XSS |
| 1. Reflected XSS | 1. Persistent XSS |

1. What defense will best help stop Cross Site Scripting (XSS)

|  |  |
| --- | --- |
| 1. Input Validation | 1. Cryptographic Tokens |
| 1. Output Encoding | 1. Rate Throttling |

1. Which of those types of cookies are called Temporary cookies and are deleted after the user closes their web browser or logout?

|  |  |
| --- | --- |
| 1. Session cookies | 1. Browser cookies |
| 1. Persistent cookies | 1. Third-party cookies |

1. Which of the following session cookies is protected against XSS attacks

| 1. Set-cookie: sessionid=Qmww | 1. Set-cookie: sessionid=Qmww ; Http |
| --- | --- |
| 1. Set-cookie: sessionid=Qmww ; HttpOnly | 1. Set-cookie: sessionid=Qmww; HttpSession |

1. Which of the following is not a security flag to protect cookies

|  |  |
| --- | --- |
| 1. Secure flag | 1. HttpOnly flag |
| 1. SameSite flag | 1. ProtectCookie flag |

1. The only effective way to protect against XSS

|  |  |
| --- | --- |
| 1. Manual penetration testing | 1. Security Scanning |
| 1. Risk Assessment | 1. smoke testing |

1. States that a document from one unique origin may only load resources from the origin from which the document was loaded.

|  |  |
| --- | --- |
| 1. Remote work policy | 1. Local work policy |
| 1. Same Origin policy | 1. Cross site policy |

1. Which of the following is considered a same origin request

|  |  |
| --- | --- |
| 1. the JS code is on the page https://website.com/apple, is a request to https://subdomain.website.com | 1. if the JS code is on the webpage http://website.com/apple, is a request to http://website.com/banana |
| 1. if the JS code is on the webpage http://website.com/apple, is a request to http://SameOrigin.com/banana | 1. if the JS code is on the webpage http://subdomain.website.com/apple, is a request to http://website.com/banana |

1. Which of the following script is an example of SQL injection attack?

|  |  |
| --- | --- |
| 1. var Shipcity;   ShipCity = Request.form ("ShipCity");  var **SQL** = "select \* from OrdersTable where ShipCity = '" + ShipCity + "'"; | 1. var Shipcity;   ShipCity = Request.form ("ShipCity"); |
| 1. var Shipcity;   var **SQL** = "select \* from OrdersTable where ShipCity = '" + ShipCity + "'"; | 1. All of the mentioned |

1. Are tiny files which get downloaded to your system when you visit a website

|  |  |
| --- | --- |
| 1. Caches | 1. Cookies |
| 1. Crawlers | 1. Bots |

1. Which of the following explains cookies nature

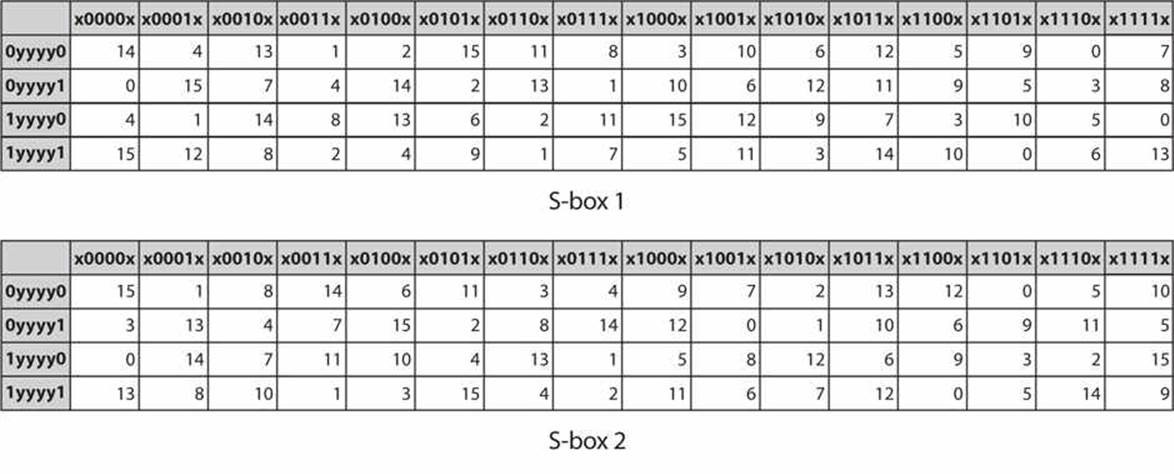
|  |  |
| --- | --- |
| 1. Volatile | 1. Non-Volatile |
| 1. Transient | 1. Non-Transient |

1. Which of the following should be stored in the cookie?

|  |  |
| --- | --- |
| 1. Session ID | 1. Account Privileges |
| 1. Username | 1. Password |

Part E: Lec6 DES Algorithm:

Given the S-Boxes, Answer questions from 49 to 52:



1. For input block B1 = 110101, then S1(B1) = . . .: [2 marks]

|  |  |
| --- | --- |
| 1. 11 | 1. 3 |
| 1. 1011 | 1. 0011 |

1. For input block B1 = 110101, then S2(B1) = . . .: [2 marks]

|  |  |
| --- | --- |
| 1. 8 | 1. 7 |
| 1. 0111 | 1. 1000 |

1. For input block B2 = 101100, then S1(B2) = ….: [2 marks]

|  |  |
| --- | --- |
| 1. 13 | 1. 2 |
| 1. 0010 | 1. 1001 |

1. For input block B2 = 101100, then S2(B2) = ….: [2 marks]

|  |  |
| --- | --- |
| 1. 13 | 1. 4 |
| 1. 1101 | 1. 0100 |

1. The DES algorithm has a key length of ….: [2 marks]

|  |  |
| --- | --- |
| 1. 64 | 1. 48 |
| 1. 32 | 1. 8 |

1. In the DES algorithm, the parity bits of the key are ….: [2 marks]

|  |  |
| --- | --- |
| 1. 28 | 1. 56 |
| 1. 16 | 1. 8 |

1. DES follows ….: [2 marks]

|  |  |
| --- | --- |
| 1. Vernam Cipher | 1. Feistel Cipher Structure |
| 1. Caeser Cipher | 1. SP Networks |

1. The DES Algorithm consists of … rounds each with a round key ….: [2 marks]

|  |  |
| --- | --- |
| 1. 16 | 1. 28 |
| 1. 48 | 1. 56 |

1. In the DES Algorithm, the sub keys are … long.: [2 marks]

|  |  |
| --- | --- |
| 1. 28 | 1. 32 |
| 1. 48 | 1. 56 |

1. The number of unique substitution boxes in DES is ….: [2 marks]

|  |  |
| --- | --- |
| 1. 4 |  |
| 1. 12 | 1. 16 |

1. In the DES Algorithm, the substitution box takes \_\_ input bits, and transforms them into \_\_ output bits.: [2 marks]

|  |  |
| --- | --- |
| 1. 8, 4 | 1. 6, 4 |
| 1. 4, 8 | 1. 4, 6 |

1. DES stands for ….: [2 marks]

|  |  |
| --- | --- |
| 1. Data Encryption Substitution | 1. Data Encryption Subscription |
| 1. Data Encryption Solutions | 1. Data Encryption Standard |

Part F: Before midterm:

1. The characteristics of a software that make it ﬁt for its purpose :

|  |  |
| --- | --- |
| 1. software elements | 1. software testing |
| 1. software quality | 1. security requirements |

1. Determines how easily bugs can be found and ﬁxed

|  |  |
| --- | --- |
| 1. Maintainability | 1. Testability |
| 1. Flexibilty | 1. Reusability |

1. Determines how easy it is to interface the system with another system.

|  |  |
| --- | --- |
| 1. Maintainability | 1. Portability |
| 1. Interoperability | 1. Reusability |

1. SQFs are affected by

|  |  |
| --- | --- |
| 1. Product operation requirements | 1. Product revision requirements |
| 1. Product transition requirements | 1. all of the above |

1. Which of these pairs of SQFs are not independent

|  |  |
| --- | --- |
| 1. Usability and flexibility | 1. Testability and reusability |
| 1. Usability and portability | 1. Maintainability and portability |

1. is the number of relationships the class has with other classes.

|  |  |
| --- | --- |
| 1. Number-of-children (NOC) metric | 1. Coupling-between-objects (CBO) metric |
| 1. Depth-of-inheritance-tree (DIT) metric | 1. none of the above |

1. Is used to check that the details of an implementation are correct.

|  |  |
| --- | --- |
| 1. Black box testing | 1. Gray box testing |
| 1. system testing | 1. White box testing |

1. What is Cyclomatic complexity?

|  |  |
| --- | --- |
| 1. Black box testing | 1. White-box testing |
| 1. Yellow box testing | 1. Green box testing |

1. Which of the following is incorrect?

|  |  |
| --- | --- |
| 1. A Layered-style program is divided into an array of modules or layers | 1. Each layer provides services to the layer “below” and makes use of services provided by the layer “above” |
| 1. ) All of the mentioned | 1. None of the mentioned |

1. What are the main issues addressed by the Layers pattern?

|  |  |
| --- | --- |
| 1. Achieving low coupling between   functionalities | 1. Separating concerns |
| 1. Achieving high coupling between functionalities | 1. Both A & B |

1. Which of the following is one of the two styles/flavors of Layers pattern

|  |  |
| --- | --- |
| 1. One-layer pattern | 1. Two-layer pattern |
| 1. Three-layer pattern | 1. Four-layer pattern |

1. Which of the following is correct about MVC

|  |  |
| --- | --- |
| 1. The view and controller are both dependent on the model | 1. The view and controller are both independent on the model |
| 1. Only the view is dependent on the model | 1. Only the controller is dependent on the model |

1. Is a lightweight web application framework

|  |  |
| --- | --- |
| 1. Selenium | 1. JavaScript |
| 1. XML | 1. Flask |

1. Flask is a web development framework created in\_\_\_\_\_\_\_\_\_\_\_ language.

|  |  |
| --- | --- |
| 1. C | 1. Python |
| 1. Java | 1. JavaScript |

1. Which of the following lines connect to Database

|  |  |
| --- | --- |
| 1. db\_connect = create\_engine('sqlite:///chinook.db') | 1. query = conn.execute() |
| 1. conn=db\_connect.connect() | 1. db = SessionLocal() |

1. JSON stands for

|  |  |
| --- | --- |
| 1. JavaScript Object Notation | 1. Java Object Notation |
| 1. JavaScript Object Normalization | 1. JavaScript Object-Oriented Notation |

1. XSS is :

|  |  |
| --- | --- |
| 1. Injection of commands | 1. Injection of Scripts |
| 1. Injection Prameters | 1. All of the above |

1. In which side does validation occur :

|  |  |
| --- | --- |
| 1. Server side | 1. Client side |
| 1. Both client and server side | 1. User side |

1. Attack which forces a user(end user)to execute unwanted actions on a web application in which he/she is currently authenticated…

|  |  |
| --- | --- |
| 1. Cross-site scoring scripting | 1. Cross-site request forgery |
| 1. Cross-site scripting | 1. None of these |

1. The most common protection mechanism against CSRF exploit

|  |  |
| --- | --- |
| 1. Authentication exchange | 1. Digital Signature |
| 1. Bit stuffing | 1. Token |