IT 8761 Security Laboratory

Batch: 2017-21 **Academic year: 2020-21**

Semester Lab Questions

December, 2020

1. University exam Quiz for 15 marks will be posted (either as google quiz or in LMS)

2. Each one of you will be given a question

3. You are asked to create a Repl.it login and asked to share the link in a google form earlier.

4. Code the answer for the lab question in Repl.it

5. At the end of the session after showing the output download the code and capture the snapshots.

6. Convert the code and output snapshots into a single pdf.

7. Send it as email to Internal examiner and external examiner

8. You will be monitored during the entire session via Zoom video and breakout rooms

Refer University Instructions:

1. The laboratory course examination shall be conducted online through any suitable popular online video communication services.
2. The laboratory examination shall be conducted using the usual procedure of appointing internal and external examiners prescribed by the University.
3. The duration of the examination shall be 3 Hrs.
4. The college principals shall create necessary weblink for the conduct of the online laboratory course examination and publish/post the same in the university web portal along with other necessary details such as list of students' registered, internal examiner appointed, session and date.
5. The college principal shall coordinate with the internal examiners of the laboratory course and communicate the weblink to all the eligible students who have registered for the laboratory examinations.
6. The examination shall be conducted using any suitable open source platform/ scientific software packages/ Simulation software/Modelling tools/ Design software/ IoT enabled/ IoT assisted/ Comprehensive Assessment Method in the online mode.
7. Any suitable open source platform/ scientific software packages/ simulation software/Modelling tools/ Design software can be used for IT/CSE/ Design/ Programming laboratory courses.

10. Objective type (MCQ) questions shall be set by the external examiner based on the syllabus of the laboratory course. The MCQ test may be conducted for all the students of the class/college using any open source platform such as Google forms/ Microsoft teams, etc. and the copies of the responses of the same must be forwarded to the concerned Zonal Office.
11. The external examiner shall set the questions based on the prescribed university syllabus jointly with internal examiner for the conduct of the laboratory examinations. The relevant and the usual procedure of the University is to be followed for the conduction of the exams.
12. Students shall use plain A4 sheets for answering the lab examinations questions posed to them.

13. At the end of the laboratory examination, each student has to send the scanned copies of the lab course write-up-answer-sheet to the email IDs of the external examiner and internal examiners. The write-up answer shall contain the Aim, equipment / apparatus/ software / software suites/ hardware/ tools/ components/ accessories required to carry out the experiments, theory/concepts/ laws/procedure/design steps/ methods/ techniques/ Algorithms/ methodologies /calculations, circuit diagrams/ schematic diagrams/ flow chart/ process diagrams, graph/plot/ model plot/ model graph, tables/model tables, inference/observation and results.

. The external examiner shall evaluate the scanned copies of the answer sheet of the individual students and award the marks based on the prescribed mark split up given in point 17. The consolidated mark statement of the laboratory course, bearing the details of all the students' those who have attended the online lab examinations must be prepared and signed by the external examiner. The scanned copy of the same must be communicated to the internal examiner. The internal examiner shall enter the marks of the students in the university web portal strictly based on the consolidated mark statement given by the external examiner. Usual procedures are to be followed for Mark entry and for other examination related activities.

(The email ids will be shared during the exam session)

Mark split-up

1	Online test (MCQ with 4 options / Objective type questions - 15 Questions- for all the students)	15 marks
2.	Aim, equipment / apparatus/ software / software suites/hardware/tools/ components/ accessories required for carrying out the experiments, theory/concepts/ laws/ procedure/ design steps/methods/techniques/ Algorithms/ methodologies/calculations, circuit diagrams/schematic diagrams/ flow chart/ process diagrams, graph/plot/ model plot/ model graph, tables/model tables, Record/observation books	65 marks
3.	Results/inference /observations	10 marks
4.	Viva-voce	10 marks
		100 marks

For any program below, if you need matrices it is already available in the LMS.

Sample questions:

1. Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the shift cipher text EVIRE. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar?
2. Develop a java program to implement the Playfair Cipher
3. Develop a java program to find the multiplicative inverse of a given number with respect to a modulus
4. Develop a java program to find the inverse of the given matrix and encrypt the message using Hill Cipher. (Key will be a numerical matrix)
5. Develop a java program to find the inverse of the given matrix and decrypt the message

using Hill Cipher. (Key will be a numerical matrix)

6. Develop a java program to display the Vigenere matrix and implement the Vigenere encryption.
7. Develop a java program to display the Vigenere matrix and implement the Vigenere decryption.
8. Develop a java program to implement the Rail fence Cipher with depth 5 and reapply the same algorithm with depth 3 on the intermediate cipher and generate the final cipher text.
9. Develop a java program to implement the Row & Column Transformation cipher twice to generate the cipher text.
10. Develop a java program to implement the RSA Algorithm with a module to check the p and q as prime numbers using Miller Rabin primality checking algorithm.
11. Develop a java program to implement the MD5 Algorithm
12. Develop a java program to implement the Diffie-Hellman Key exchange algorithm. Implement the Miller Rabin primality checking algorithm to check the primality of the input prime number for DH key exchange algorithm.
13. Develop a java program to implement the SHA-1 Algorithm
14. Develop a java program to implement the DES encryption. Keys in numeric/ hexadecimal/ binary will be given. Input plaintext message will be an English statement / phrase, encrypted message should be in hexadecimal.
15. Develop a java program to implement the DES decryption. Keys in numeric/ hexadecimal/ binary will be given. Input will be an encrypted message in hexadecimal and the output should be an intelligible English statement.
16. Develop a java program to implement the DES Key generation. Input should be an integer string, output expected can be in hexadecimal/ binary string.
17. Develop a java program to implement the AES algorithm.

18. Develop a java program to implement the Digital Signature Standard.
19. Develop a java program to implement the Miller Rabin primality checking algorithm to check the primality of a given number.

------All The Very Best------