Department of Computer Science (New Campus)
University of Engineering & Technology, Lahore

Subject: **Information Security**   (6th Semester, 2021 Session)   **Total Marks: 10**

Due Date: **27-04-2024**   **Assignment**

CLOs	Questions	Marks
4	Apply Data Encryption Standard (DES) to encrypt and decrypt the given plain text as per the following criteria. 1. The plain text is: **LAHORE IS A BIG CITY** 2. Key: Get the first <u>8 characters</u> of your full name. For example, my full name is Abdul Wahab, the key will be Abdul Wah. 3. Block size: 64 bits 4. Number of Rounds: 2 5. Apply DES key scheduling algorithm to generate 2 round keys. 6. Mode of Operation: Cipher Block Chaining (CBC) **Instructions to upload the project:** 1. You can use MS Word for this project and then convert it to a PDF file. The name of the PDF file should be your registration number in the format 2021SExxx. 2. A link will be shared to upload the PDF file to DropBox.	5+5

Department of Computer Science (New Campus)
University of Engineering & Technology, Lahore

Subject: **Information Security**   (6th Semester, 2021 Session)   **Total Marks: 10**

Due Date: **27-04-2024**   **Assignment**

CLOs	Questions	Marks
4	Apply Advanced Encryption Standard (AES) to encrypt and decrypt the given plain text as per the following criteria. 1. The plain text is: **ISLAMABAD IS THE CAPITAL OF PAKISTAN.** 2. Key: Get the first <u>8 characters</u> of your full name. For example, for the full name Abdul Wahab, the first 8 characters are Abdul Wah**.** Now append them to MY NAME IS to get the key **MY NAME IS A**bdul Wah. 3. Block size: 128 bits 4. Number of Rounds: 2 5. Apply AES key scheduling algorithm to generate 2 round keys. 6. Mode of Operation: Cipher Block Chaining (CBC) **Instructions to upload the project:** 1. You can use MS Word for this project and then convert it to a PDF file. The name of the PDF file should be your registration number in the format 2021SExxx. 2. A link will be shared to upload the PDF file to DropBox.	5+5