****

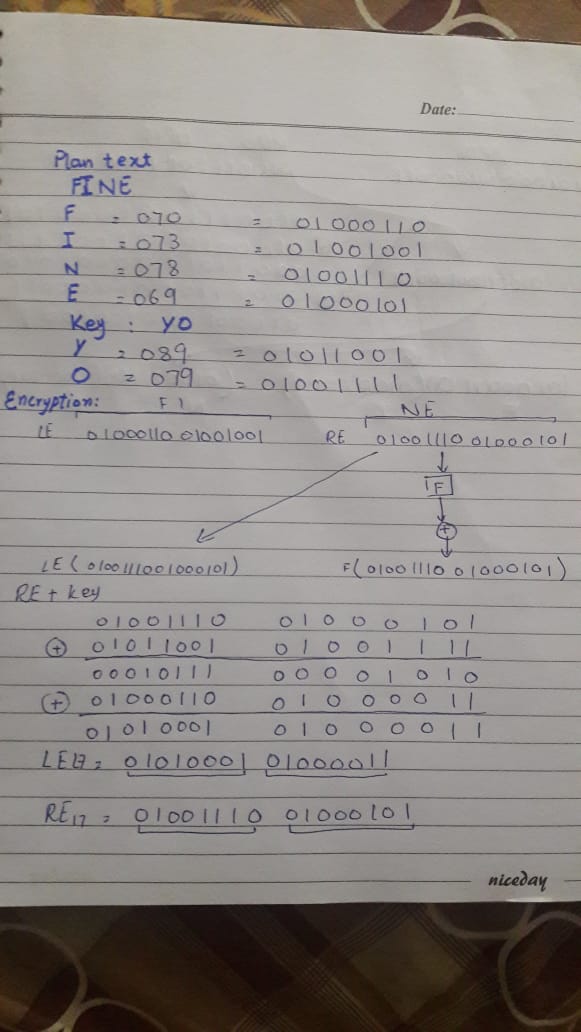
**COMSATS University Islamabad, Lahore**

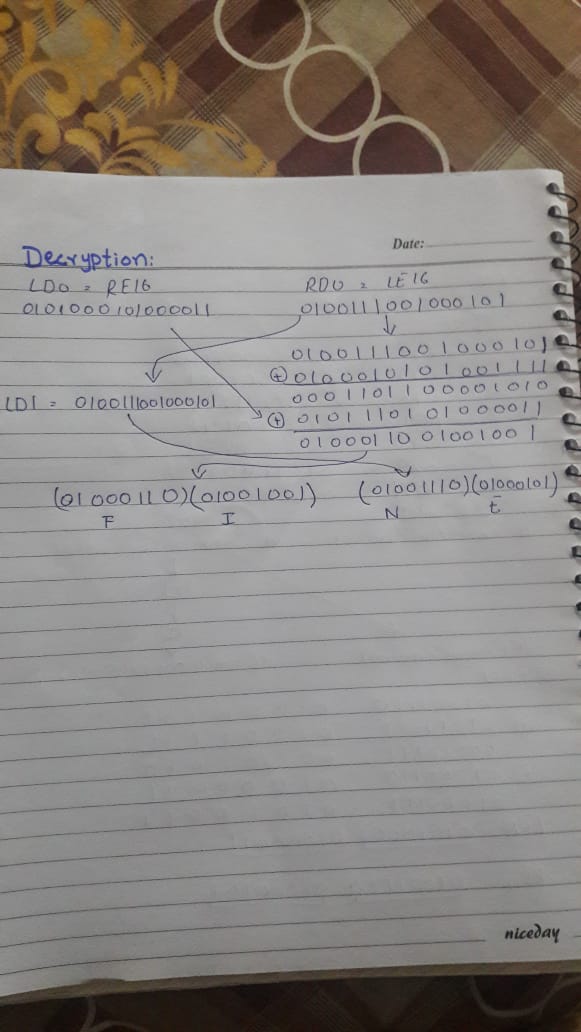
**Assignment 2**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Course Title: | Data Security and Encryption | | | | Course Code: | | CSE348 | Credit Hours: |  |
| Course Instructor/s: | Dr. M. Tayyab Chaudhry | | | | Programme Name: | | BSE | | |
| Semester: |  | Batch: |  | Section: | A | | Date: |  | |
| **Deadline:** | **Friday 27th March 12:00 AM** | | | | **Maximum Marks:** | | | **5** | |
| Student’s Name: | **Zinneera Waheed** | | | | Reg. No. | FA16-BSE-229 | | | |
| **Important Instructions / Guidelines:**   * Submit the assignment through email to [tayyabch@cuilahore.edu.pk](mailto:tayyabch@cuilahore.edu.pk) through CUI email address only. * You must use the submission email title as: “<reg. no.> <section> Assignment 2 DSE Spring 2020” * Please submit with in deadline. 50% marks will be deducted for late submissions. * One student per assignment. * No plagiarism is allowed. * Assignments submitted without the prescribed title and/or CUI email address may not be marked. | | | | | | | | | |

**Question: Solve the example of Figure 3.3 in book with the 32-bit input data of encryption round 15 and subkey K15 other than given in example i.e., use new data and subkey. Show that the corresponding decryption round 2 generates the correct corresponding block.**

**Answer:**

****

****

**This page is intentionally left blank for rough work.**

**Good Luck**