# National University
## of Computer & Emerging Sciences

Program: BS (CS/SE)
Semester: Fall 2022
Course: CS3002 - Information Security

Assignment#01
Due Date: 21-10-2022
Instructor: Waqas Ali

1. You have to launch a successful meet-in-the-middle attack on double DES (using two keys). Since this process requires you to generate all possible combinations of the first key (i.e. $k_1$), you need to report the number of keys used for $k_2$ to find the key pair i.e. ($k_1$, $k_2$). Report the time taken for finding the key pair.

   **Note**

   1. You can use any implementation of DES (use built-in functions (if available) or pick any valid implementation from the internet).
   2. This assignment must be implemented in python.
   3. You can generate a number of plain-text, cipher-text pairs to use for the attack. One pair can be used to launch the attack, the rest can be used to verify that the keys found are valid.