# Information Assurance and Security (IT352) Laboratory Program - 4

Implement Electronic Code Book (ECB) mode of operation using DES. It should consider the plaintext of any type (alphanumeric/integer/strings) as one of the inputs and key of any type (alphanumeric/integer/strings) as another input. Maximum size of the plaintext is restricted to 40 bytes and program should consider the given key input only if its size is 8 bytes. Further, these should the supplied during program run-time. Display output of every round and output of final permutation as ciphertext on terminal and also store all results including intermediate results into a file with a name "Output-of-Program-4.txt".

**Steps:**

1. Read the plaintext, if its size of the plaintext is greater than 40 bytes, quit the program execution else check whether the input size is greater than 8 bytes. If so, divide into blocks of size 8 bytes. If the last block is lesser than 8 bytes, make the size of the last block equals to 8 bytes by adding required number of padding bytes "space".
2. Read the given key value, check its size to continue or to the quit the program execution.
3. Encrypt each plaintext block independently using given key and display as well as store the results on terminal and output, respectively.
4. Consider the space between the work as input character and its ASCII value for further computation.

**Sample Text Case**

Plaintext : Information Assurance and Security 2018
Round Keys : CRYPTOGR

Submit program as well as screenshot of the output to it35215b@gmail.com before the deadline.

Subject of the email is : IT352-Lab-Program4-with-Results

File name of the program : RegisterNo_IT352_P4
(P2 indicates Program Number-2)

File name of the screenshot : RegisterNo_IT352_P4_S1
(S1 indicates screenshot for the first test case, similarly, for other test cases S2, S3, S4, S5)

Date of Laboratory : 6th February 2019
Date of submission-cum-evaluation : 6th February 2019

**Note:** Kindly clarify the doubt(s) (if any related to the said program) before commencement of the laboratory. **If student(s) absent for the 6th February 2019 laboratory for program-4 submission-cum-evaluation, such student(s) program-4 submission will not be considered for evaluation.**