# CS-364: Introduction to Cryptography and Network Security LAB

## LAB Assignment II

Course Instructor: Dr. Dibyendu Roy Due: Feb 27, 2022, 11:59 pm

Instructions: Code must be written in C and well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. The file name of the code will be YOUR ROLL NO.c. Write Your Name and Roll Number on the top of your code. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks.

Implement the encryption as well as the decryption of full round (16 rounds) DES algorithm.

1. Your code will take 64 bit plaintext block $P$ as input.
2. Your code will take 56 bit secret key $K$ as input. We are not considering the parity check bits.
3. Code will output the 64 bit ciphertext $C$.

If the code is correct then the decryption on ciphertext $C$ using the secret key $K$ should return the same plaintext $P$. Your code will be verified using existing test vectors.