ISEC 2000 Fundamental Concepts of Cryptography
Laboratory 4
@ Computing, Curtin University

Notes:

- Make sure you complete prac questions. Assignments are highly related to them. In fact, programming questions are building blocks for the assignments.
- Group discussion is encouraged but make sure you complete questions individually.
- Ask questions not just answers. There is no answer of prac questions documented or provided for computing units.
- You can use your preferred programming language, C/C++, Java, or Python. Do NOT rely on libraries excessively.

1. It is important for a cipher to contain both confusion and diffusion. Briefly discuss what is confusion and diffusion.

2. Prove that DES works, i.e., the decryption can indeed recover the plaintext.

3. Please write a program that converts standard keyboard characters ($a, b, 3, !, =$, #) to binary and hexadecimal numbers.