Laboratory I2: Data Encryption Algorithm

1 Objective

Objective of the lab: The objective of this lab is to give the student some practical exposure to the DES concepts and algorithm presented in class.

2 Requirements

Note: This lab requires some preparation, in terms of theoretical background as well as the use of the tools (use of the D-Lab, Matlab, the m-files, etc.). Students who are unable to do the lab because they have not prepared will be asked to leave.

Instructions, source material and preparation required:

- You are required to do all the preparation needed to implement the algorithms beforehand. You need to have access to all the permutation tables (Initial Permutation, Inverse Initial Permutation, S-boxes, E-boxes, P-boxes, Key Permutations, etc.) as well as all the detailed workings of each step.
- Lab partners must operate in groups of two (and no larger) and may help each other during the lab but each should use his/her own sample text in all the exercises and write his/her own lab report.

Report: The report will take the form of the following group of files which should all be attached to a single email:

- An answer sheet (in Word or PDF format) with your name and your lab partner's name and student numbers, the date and experiment number, and your results for Question 2, 3 and 4.
- All the m-files used in the lab.

3 Outcomes

1. Implement a function that will generate the specific subkey K_i when the following parameters are passed as inputs to the function: a 56 bit key and the index i.
2. Calculate the number of unique subkeys for the following 64-bit keys (ignore the parity bits in your calculations) and classify the keys:
   - $1F1F\ 1F1F\ 0E0E\ 0E0E$,
   - $1FFE\ 1FFE\ 0EFE\ 0EFE$,
   - $1FFE\ FE1F\ 0EFE\ FE0E$.
3. Implement a function that will produce two 32-bit output blocks, given a 64-bit input block, the index of the round ($i \in \{1, 2, ..., 16\}$) and the 48-bit subkey K_i. (The whole round must be implemented.)

4. Using the functions of 1 and 3, implement the Data Encryption Algorithm (DEA).

For question 3, a 64-bit input block, a sub-key and the result will be provided. For Question 4, a plaintext, key and ciphertext will be provided. This is to test if your implementation is working correctly.

For your answer sheet, each one of you will be assigned a unique set of parameters for Question 3 and Question 4.