CS 153 Problem Set 1.
Due 19 March 2015, 5:00 p.m.

1. You can work on this problem set as an individual or in pairs. There is at most one group of three that will be allowed in class.
2. All source code should be committed to a git repository. I suggest you use either github.com or bitbucket.com. You should give me (spfestin@dcs.upd.edu.ph) access to your git repository so I can clone your project.
3. The answers to the questions should be submitted in PDF format, via e-mail, no later than 5:00 p.m. of 19 March 2015. Email submission should be to spfestin@dcs.upd.edu.ph with Subject Line: CS 153 Problem Set 1 Submission.

Summary of Deliverables:
1. Submit by e-mail
   a. Link to git repository
   b. Attach as PDF, answer to the question posted below. Make sure that your name(s) are included in the PDF submission.

You can use any of the ff: languages: Python, Java, C, C++.
You cannot use canned crypto libraries (e.g., Java Cryptographic Extension (JCE)).

Implement DES. In your implementation, display the subkey (round key) generated for each round.

Use the following four (4) DES keys (in hexadecimal) and characterize the output of your DES implementation.

(a) `0101010101010101`
(b) `fefefefefefefefe`
(c) `1f1f1f1f1f1f1f1f`
(d) `e0e0e0e0e0e0e0e0`