Homework Assignment #1A

Note

This assignment is due 2:10PM Tuesday, October 11, 2016. Please write or type your answers on A4 (or similar size) paper. Drop your homework by the due time in Yih-Kuen Tsay's mail box on the first floor of Management Building 2. Late submission will be penalized by 20% for each working day overdue. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

1. Solve the following exercise problems in Stallings' book (6th edition): 1.1 (10 points), 2.1 (10 points), 2.18 (10 points), 3.1(b) (5 points), 3.4 (10 points), 3.8 (TD_i is the transformation defined by the i-th iteration of decryption; 10 points), 4.14 (5 points), 4.19(a)(b) (10 points), 4.26 (10 points), 4.27 (multiplicative inverse of $x^3 + x$; 10 points).

2. A permutation operation on n (≥ 1) distinct objects (arranged in some order so that each object is uniquely identifiable by a number in $\{1, 2, \cdots, n\}$) can be represented by a table listing a permutation of the numbers from $\{1, 2, \cdots, n\}$ in the following sense: if the i-th entry of the table is p_i, then the new i-th object will be the original p_i-th object.

   For example, the following P is a permutation operation on 8 objects:

   $$P = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{matrix} \\ \left[\begin{matrix} 4 & 2 & 7 & 3 & 8 & 6 & 1 & 5 \end{matrix}\right] \end{array}$$

   Given the input $M = \langle M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8 \rangle$, P produces the output $P(M) = \langle M_4, M_2, M_7, M_3, M_8, M_6, M_1, M_5 \rangle$.

   (a) Give the inverse permutation of the above P using the same representation. (5 points)

   (b) Let $[r_1 r_2 \cdots r_{n-1} r_n]$ be the inverse of a given permutation $[p_1 p_2 \cdots p_{n-1} p_n]$. Describe in precise terms the relation between r_i's and p_i's. (5 points)