Assignment 2 (CS558)

Due: 11:59pm March. 11 (Sunday)

This assignment is done by a group of 2
Each group should submit only ONE copy of the assignment (i.e., only ONE group member should submit the assignment)

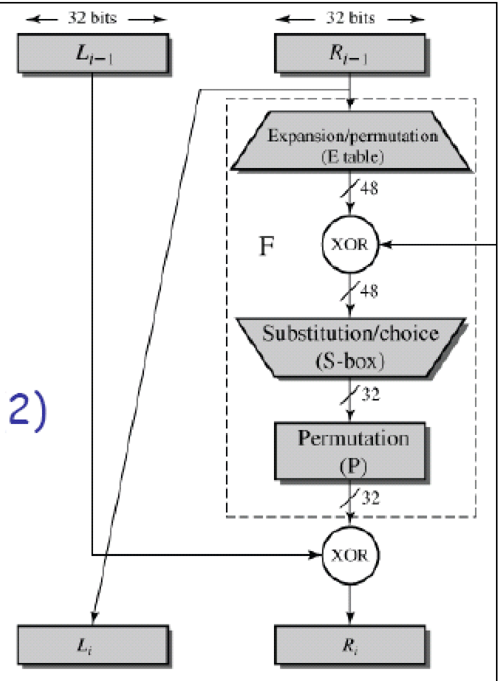
The following Figures are used for Questions 3, 4, and 5.

Permutation (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

E table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1



1. **[15 points] Decrypt** the message "**dfsfhoisgosidh**" using **rail fence cipher** with depth **4** (give detailed steps)
2. **[15 points] Decrypt** the message **"dhdplakshgiskfnhgd**" using **row transposition cipher** and **key: 351462 (**give detailed steps)
3. **[25 points]** Use **s-box S2** to show that s-box has the property: the four output bits from each S-box affect six different S-boxes on the next round.

4. [30 points] consider the 1-round DES given below, in which (Li-1, Ri-1) is the plaintext and (Li, Ri) is the ciphertext.

Assume that the attacker knows the following two plaintext-ciphertext pairs
(Pi-1=0000000000000000
0000000000000000
0010000000000000
0000000000000000,

```
 Ci=0010000000000000
       0000000000000000
       0011000000000000
       0000000000000000)
and
(Pi-1'= 0110000010000000
       1000000000000000
       0100000000000000
       0000000000000000
 Ci'=0100000000000000
       0000000000000000
       0110000000000000
       0000000000000000.
```

Discover the first 6 bits of key Ki using attacks studied in the class.

5. **[15 points]** Using Fermat's theorem to compute 3^{302} mod 11.

Submission guideline

You need to hand in your assignment through mycourses, which contains: 1) Names and email addresses of group members; and 2) Solution to the problems. Your assignment must be in **.pdf** format. If you use word, please convert .doc to .pdf using **print** command.

Academic Honesty:

All students should follow Watson School Student Academic Honesty Code. All forms of cheating will be treated with utmost seriousness. You may discuss the problems with students in another groups, however, you must write your OWN solutions. Discussing solutions to the problem with students in another group is NOT acceptable. Copying an assignment from students in another group or allowing students in another group to copy your assignment may lead to a 0 in the assignment or an **F** for this course. You need ensure that your code and documentation are protected and not accessible to other students. Use **chmod 700** command to change the permissions of your working directories before you start working on the assignments. If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please consult the instructor before you collaborate.