# Assignment 2 (CS558)

***Due: 11:59pm, Oct. 8 (Sunday)***

**This assignment is done individually or by a group of 2 students.**

**Each group should submit only ONE copy of the assignment (i.e., only ONE group member should submit the assignment).**

1. [14 points] **Decrypt** the ciphertext **"dpualy"** using the **caesar cipher** (the plaintext is an English word; give detailed decryption steps).

2. **[14 points] Decrypt** the ciphertext "**cdefghijklmnop**" using the **rail fence cipher** with depth **4** (the plaintext is not an English word; give detailed steps).

**3. [14 points] Decrypt** the ciphertext "**cdefghijklmnopqrst"** using the **row transposition cipher** and the **key 315264 (**give detailed steps).

4. [14 points] **Encrypt** the plaintext "**heecggs"** using the **playfair cipher** and the keyword **helol (**give detailed steps). Use "x" as plaintext fillers if needed.

5. [8 points] Consider the following S-box.
(1) (6') Assume that the output of the S-box is 6. What are the 4 possible inputs to the S-box?
(2) (2') Assume that the input to the S-box is 100101. What is the output of the S-box?

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

6. [8 points] Given the following permutation table (P table).
**(1)** (4') If the **output** of the P table is 01000000 00100000 00000000 00000000, which bits of the **input to** the P table is 1 (No explanation is needed)?
**(2)** (4') If the **input** to the P table is 01000000 00100000 00000000 00000000, which bits of the **output** of the P table is 1 (No explanation is needed)?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |

**7.[10 points]** Using Fermat's theorem to compute $3^{503}$ mod 11.

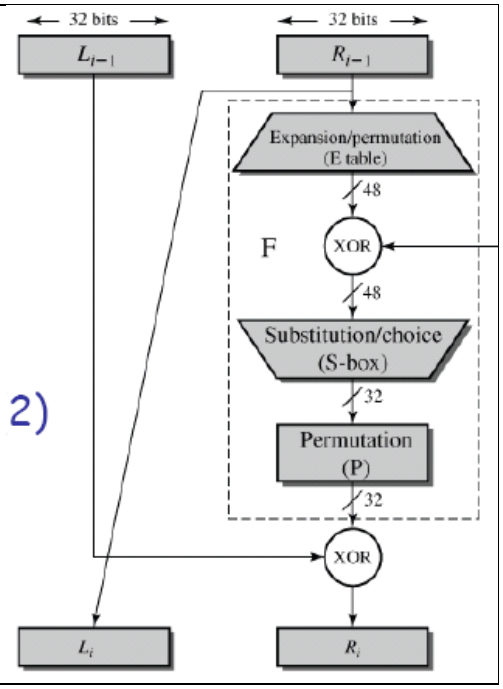
8. **[12 points]** Use **S-box S3** and the following figures/tables to show that s-box has the property: the four output bits from each S-box affect six different S-boxes on the next round.

**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 |




9. (6 points) Provide two reasons suggesting that https://inventoryliquidationshop.com/ is likely a scam website.

***Submission guideline***

You need to submit your assignment as one .pdf file through brightspace.binghamton.edu, which contains: 1) the name and email addresse of group members and 2) the solution to the problems. If you use word, please convert .doc to .pdf using **print** command. You can also write down your answers, take pictures, and convert the pictures into one .pdf file.

***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 other students, however, you must write your OWN solutions. Discussing solutions to the problem 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.