Assignment 2

Due: 11:59pm June 19 (Sunday)

This assignment is done individually.

1. **(6 points)** which of the following attacks are passive attacks (one or more answers may be correct)?

   A. Traffic analysis   B. Denial of service   C. Replay attack   D. Masquerade

2. **(12 points)** Let **Pu**$_A$ and **Pr**$_A$ be Alice's public and private keys, respectively, and **Pu**$_B$ and **Pr**$_B$ be Bob's public and private keys, respectively. Assume that Alice sends Bob a message M.

   a) If Alice wants to protect the confidentiality of M, then what key should Alice use to encrypt M?

   b) If Alice wants to provide digital signature, then what key should Alice use to create the digital signature?

   c) If Alice wants to protect the data integrity of M, then what key should Alice use to encrypt M?

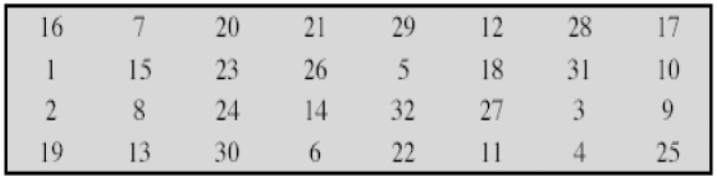
3. **(8 points)** Suppose 4 people want to communicate securely with each other such that the communication of none of the possible pairs of people can be eavesdropped by the remaining persons. Answer the following questions:
   (a) If they use a symmetric cipher, how many symmetric keys would they need in total?

   (b) If they use a public-key cipher, how many public and private keys would they need in total?

4. **[15 points] Encrypt** the message "**tomorrowfriday**" using **rail fence cipher** with depth **4**

5. **[15 points] Decrypt** the message "**rnoxitrzsunwinooagry**" using **row transposition cipher** and **key: 35214**

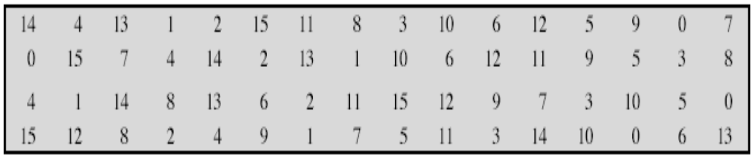
6. **[7 points] Given** the following permutation table (P table)



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

Assume that the **input of the P table is 11000000 00000000 00000000 00000000, which bits of the output** of the P table are **1?**

7. **[15 points]** Consider the following **S-box**. Assume that the output of this S-box is 2, What are the four possible inputs to 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

8. **[12 points]** Prove that the decryption process of the counter mode is correct. The counter mode can be formalized using the following two equations. Here, E represents the encryption algorithm, Ci is the ciphertext of the ith block, and Pi is the plaintext of the ith block.
   Encryption: $Ci = E(Counter + i - 1) \oplus Pi$
   Decryption: $Pi = E(Counter + i - 1) \oplus Ci$

9. **[10 points]** Compute $\Phi(55)$, where Φ is Euler totient function.

Submission guideline

You need to hand in your assignment (one .pdf file) through brightspace.binghamton.edu, which contains: 1) Your name and email address; and 2) Solution to the problems. Your assignment must be in the **.pdf** format. You can write down the solution in a paper, take a picture of the solution, and then upload the solution to brightspace.

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 another student, however, you must write your OWN solutions. Discussing solutions to the problem with another student is NOT acceptable. Copying an assignment from another student or allowing another student to copy your assignment may lead to a 0 in the assignment or an **F** for this course. If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please consult the instructor before you collaborate.