CS 462: Assignment 6

1. What is the difference between block and stream cipher? 2
2. What is the difference between diffusion and confusion? 2
3. What are the parameters that define a simple Feistel cipher? 2
4. Why is DES considered less secure nowadays? 2
5. Why is the AES algorithm considered better than the DES? 2
6. Explain the avalanche effect in a crypto system. 2
7. What makes breaking the RSA algorithm so difficult by brute force? 2
8. What is the fundamental difference between Hash values generated using digital signatures and ciphertext generated using encryption techniques like RSA and DES? 2
9. How do Certification Authorities address limitations we find in Digital Signatures? 2
10. Explain the difference between Stateless and Stateful packet filtering. 2
11. What is the difference between Firewalls and Intrusion Detection Systems? 2
12. What is a Demilitarized Zone in a network? 2
13. Explain each step in a single round of DES algorithm. 4
14. Using the S-Box given below, explain what the output would be if the input is (ABC8E2193ACD)16. Given that in a sequence of 6 bits, the middle 4 bits represent column number and extreme two bits represent row number 4

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

15. Perform encryption and decryption using the RSA algorithm for the following terms. Show the steps for the process. 4
    a. p = 3; q = 11; e = 7; m = 5
    b. p = 5; q = 11; e = 3; m = 9

36 points