Arab Academy for Science Technology and Maritime Transport
College of Computing and Information Technology

Course	Computer System Security
Course Code	CS421
Lecturer	Prof. Dr Ayman Adel
TA	Maram Shouman, Menna Elmasry

Sheet 3

Review Questions: (2 marks per each question)

1. Draw the round of encryption for the Data Encryption Standard.
2. Draw the key schedule calculation.
3. What is the difference between block cipher and stream cipher?
4. What is the difference between diffusion and confusion?
5. Explain why the initial and final permutations of DES do not add to its security.
6. Why does the DES function need an expansion permutations?
7. Why must it be the case that the size of the cipher-text block is at least as big as the size of the plain-text block for any encryption algorithm?
8. What is an upper bound on the worst case number of attempts a brute force algorithm (one that sequentially tries all keys) must make to crack 3DES?
9. How many DES keys on average encrypt a particular plaintext block to a particular cipher text block?
10. What is double DES? What kind of attack on the double DES makes it useless?
11. Discuss the Brute force attack in DES and the alternatives of the double and triple DES.

Problems: (5 marks per each question)

1. Show the Cipher text after one round of DES for the following plaintext and key in hexadecimal numbers. Compare part *a* versus part *b* to verify the avalanche effect in DES.

   a) Plaintext: 0 1 2 3 4 5 6 7 8 9 A B C D E F, Key: 0 1 2 3 4 5 6 7 8 9 A B C D E E
   b) Plain-text: 0 1 2 3 4 5 6 7 8 9 A B C D E E, Key: 0 1 2 3 4 5 6 7 8 9 A B C D E F

2. What is the output of the first iteration of the DES algorithm when the both plain-text and the key are all zero?
3. Answer the following questions about S-boxes in DES:
   - show the result of passing 110111 through S-box 3
   - show the result of passing 001100 through S-box 4
   - show the result of passing 000000 through S-box 7
   - show the result of passing 111111 through S-box 2

4. Show the results of the following hexadecimal data after passing it through the final permutation box.

   AAAA BBBB CCCC DDDD

5. Show the results of the following hexadecimal data after passing it through the initial permutation box.

   0110 1023 4110 1023

6. If the key with parity bit (64 bits) is 0123 ABCD 2562 1456. Find the first round key.
7. Use Java to write an application that shows encryption and decryption using DES. Input is to be provided interactive from user and constrained to 1 block of text.