****

**BAHRIA UNIVERSITY (KARACHI CAMPUS**)

MIDTERM EXAMINATION –SPRING SEMESTER – 2020

**(Data Encryption and Security: CEN-451)**

Take Home Assignment

Class: **BS (CS)-7 (B,C) (Evening)**

Course Instructor: **BILAL MUHAMMAD IQBAL** Submission Deadline: **31-May-2020**

Max Marks: 20

**Note:**

Any form of plagiarism will result in receiving zero in the assignment

Any assignment submitted after the deadline will receive zero

1. **Hill Cipher Encrypt = “meet me at the usual place at then rather than eight o clock”**

K = [9 4]

[5 7]

(**3 marks)**

1. **(a) Define following terms with suitable examples or diagram:**
   1. Security Goals
   2. Security Attacks
   3. Security Services
   4. Security Mechanisms

(**2 marks)**

**(b) Find the general solutions to the equation by using Linear Diophantine Equation method.**

* 1. 21x+14y=35

(**1 mark)**

**(c)Find the modulo of the following operations:**

* 1. **-**19 mod 14
  2. -8 mod 10

(**1 mark)**

**(d) Find the multiplicative inverse of following:**

* 1. Find all multiplicate inverses Z26\* in Z26

Hint:

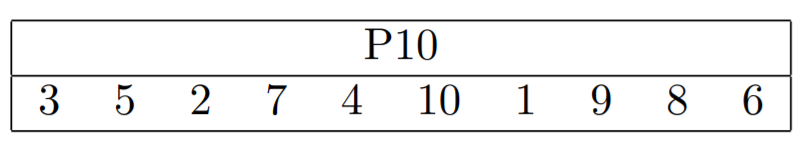
* gcd (a, b) = 1, we say that a and b are relatively prime.
* Two numbers are relatively prime if they have no common factors other than 1

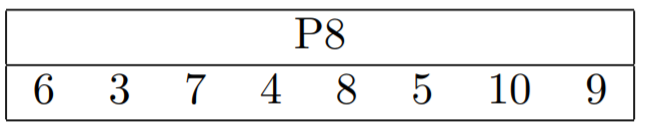
(**1 mark)**

1. **The S-DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of cipher text as output.**

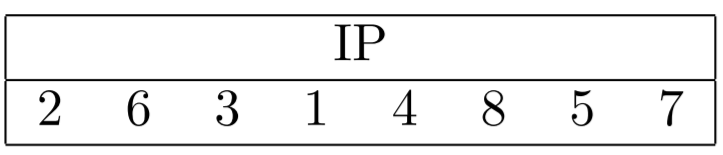
**Apply the S-DES to encrypt the plaintext (0010 1000), Let the 10-bit key is (1100011110).**

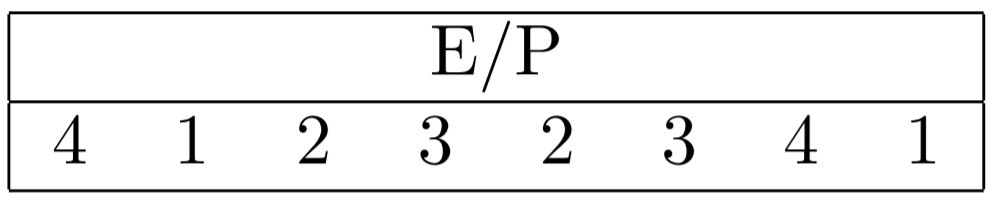
**The keys K1 and K2 derived using the given functions P10 and P8.**

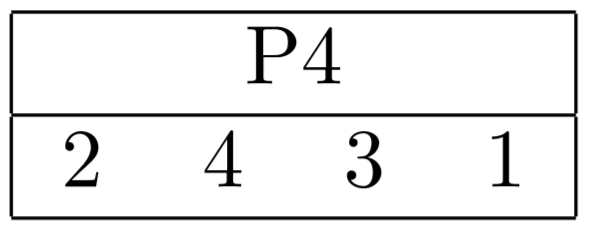


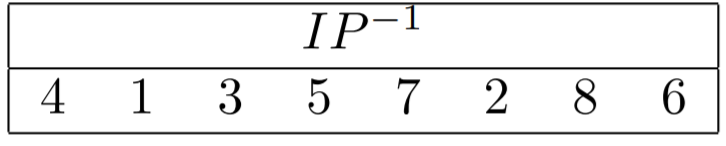


The functions IP, E/P, P4, IP−1 and S-Boxes are follows:



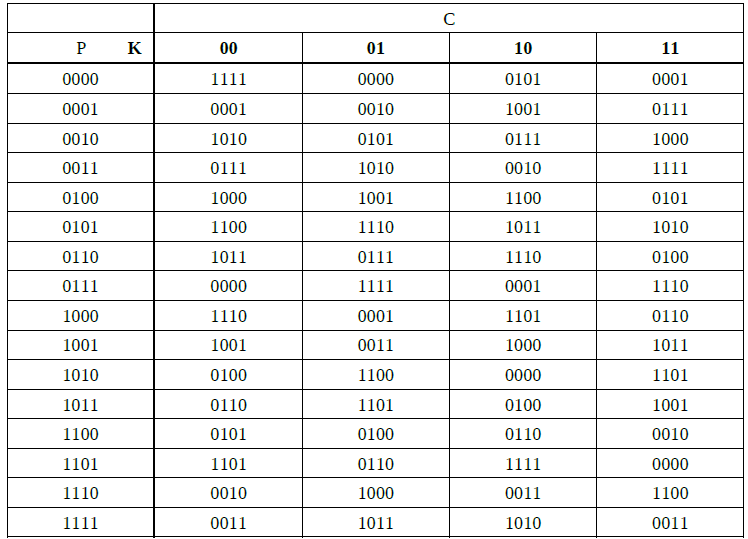




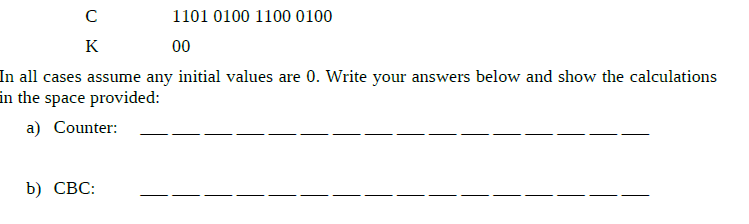


(**5 marks)**

1. **Consider a block cipher, called A, shown in the table below. The table gives the ciphertext C produced when encrypting the plaintext P with one of the four keys.**

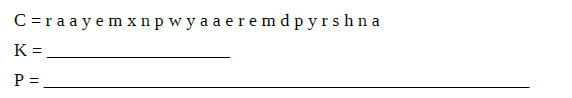


Using cipher A and one of the following modes of operation, decrypt the ciphertext C with key K:



(**5 marks)**

1. **The following ciphertext was obtained by encrypting the original plaintext P with a Rows/Column Transposition cipher using a key K. No padding was necessary. What is the original plaintext and key K? (Hint: the 5th character of the plaintext is y;**



(**2marks)**