Department of Information Systems
College of Computer and Information Sciences
King Saud University

IS493: Information Security

Summer Session: 2016 -2017

Section:

Student Name:

ID:

Assignment: 1

Deadline 4th December

TOTAL: 100

N.B: Submission after 4th December, it is considered as a **zero** mark. Softcopy will be sent to me and hard copy will be given to TA. (For your information: Prepare your submission with question and answer; if question is not available then mark will be deducted and it could be from 45% to 75 %. For your help you can download the doc file)

Question 1: (5 Marks)

Decrypt the following ciphertext using columnar transposition cipher with **keyword: YOURSELF**

Ciphertext: YARUEDCAUOADGRYHOBBNDERPUSTKNTTTGLORWUNGEFUOLNDRDEYGOOAOJRUCKESPY

Answer:

Question 2: (5 Marks)

If exists, calculate multiplicative inverse of 7, 12, 22, 23, 66, 93, and 129 in Z_{164}. If does not exists explain why?

Answer:

Question 3: (5 Marks)

Additive cipher technique is used to produce the following ciphertext. Find the key by brute force cryptanalysis and deduce the plaintext.

Ciphertext: il pu aol jshzz dpaopu jlyahpu wlyjluahnl

Answer:

Question 4: (5 Marks)

Using Affine cipher technique decrypt the following ciphertext: Where $K_1 = 11$ and $K_2 = 14$

Cipher Text: Y oq o epavgbp

Answer:

Question 5: (5 Marks)

If exists, find the determinant and the multiplicative inverse of the residue matrix M_1 and M_2 over $\mathbf{Z_{26}}$

$$M_1 = \begin{pmatrix} 21 & 6 & 22 \\ 5 & 23 & 25 \\ 7 & 3 & 9 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 23 & 6 & 3 \\ 25 & 21 & 22 \\ 9 & 5 & 7 \end{pmatrix}$$

Answer:

Question 6: (5 Marks)

If we want to use above matrices (M_1 and/ or M_2) of Question 5 as a key for constructing a Hill Cipher cryptosystem, then which one between M_1 and M_2 you recommend to use as a key, and why?

Using your recommended key decrypt the following ciphertext.

Ciphertext: **TJFKBSXXW**

Answer:

Question 7: (5 Marks)

A. Show the result of 3-bit circular left shift on word $(10011011)_2$.

B. Show the result of 3-bit circular right shift on the resulting from Part a.

C. Compare the result of Part b with the original word in Part a.

Answer:

Question 8: (5 Marks)

Find the result of the following operations:

A. $(01001101) \oplus (01001101)$

B. $(01001101) \oplus (10110010)$

C. $(01001101) \oplus (00000000)$

D. $(01001101) \oplus (11111111)$

Answer:

Question 9: (5 Marks)

A message has 2003 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.

Answer:

Question 10: (5 Marks)

Determine whether the P-box with the following permutation table is a straight P-box, a compression P-box, or an expansion P-box.

1	**3**	**5**	**6**	**7**

Answer:

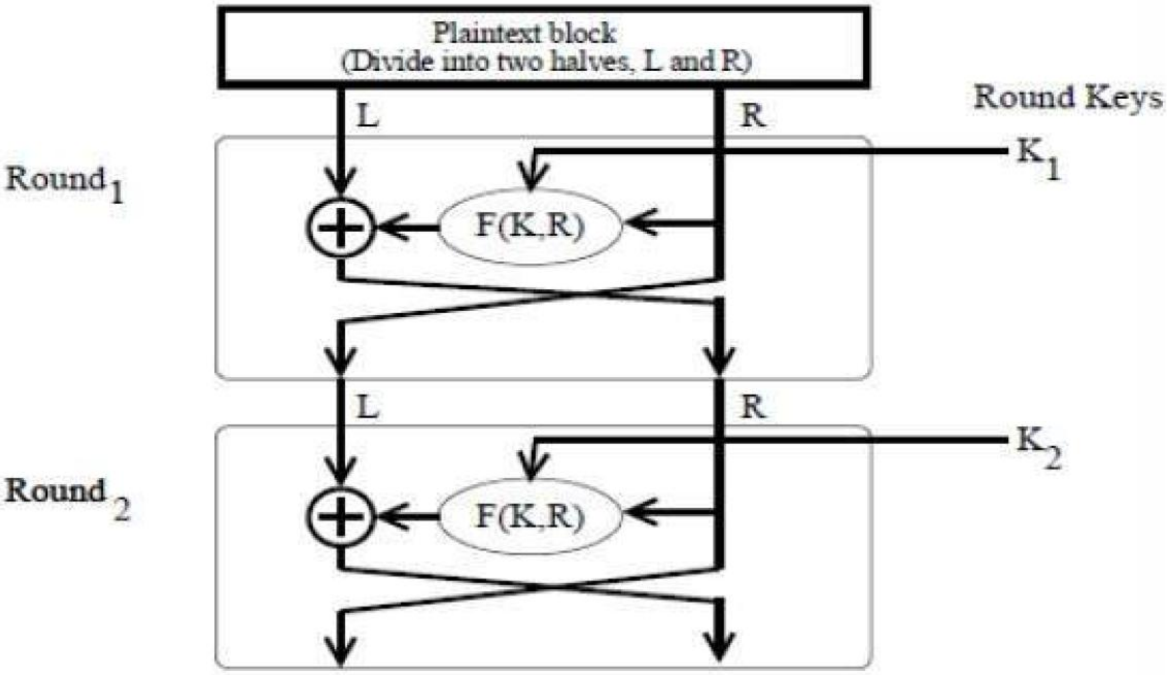
Question 11: (10 Marks)

Using Feistel Block Cipher Encryption technique with two rounds, encrypt the following plaintext .

Plaintext: be (01100010 01100101)

K_1 : 10101011

K_2 : 11001101



F is defined as follows:

$$F(K, R) = K \oplus \text{ [4-bit left circular shift of } R]$$

Answer:

Question 12: (5 Marks)

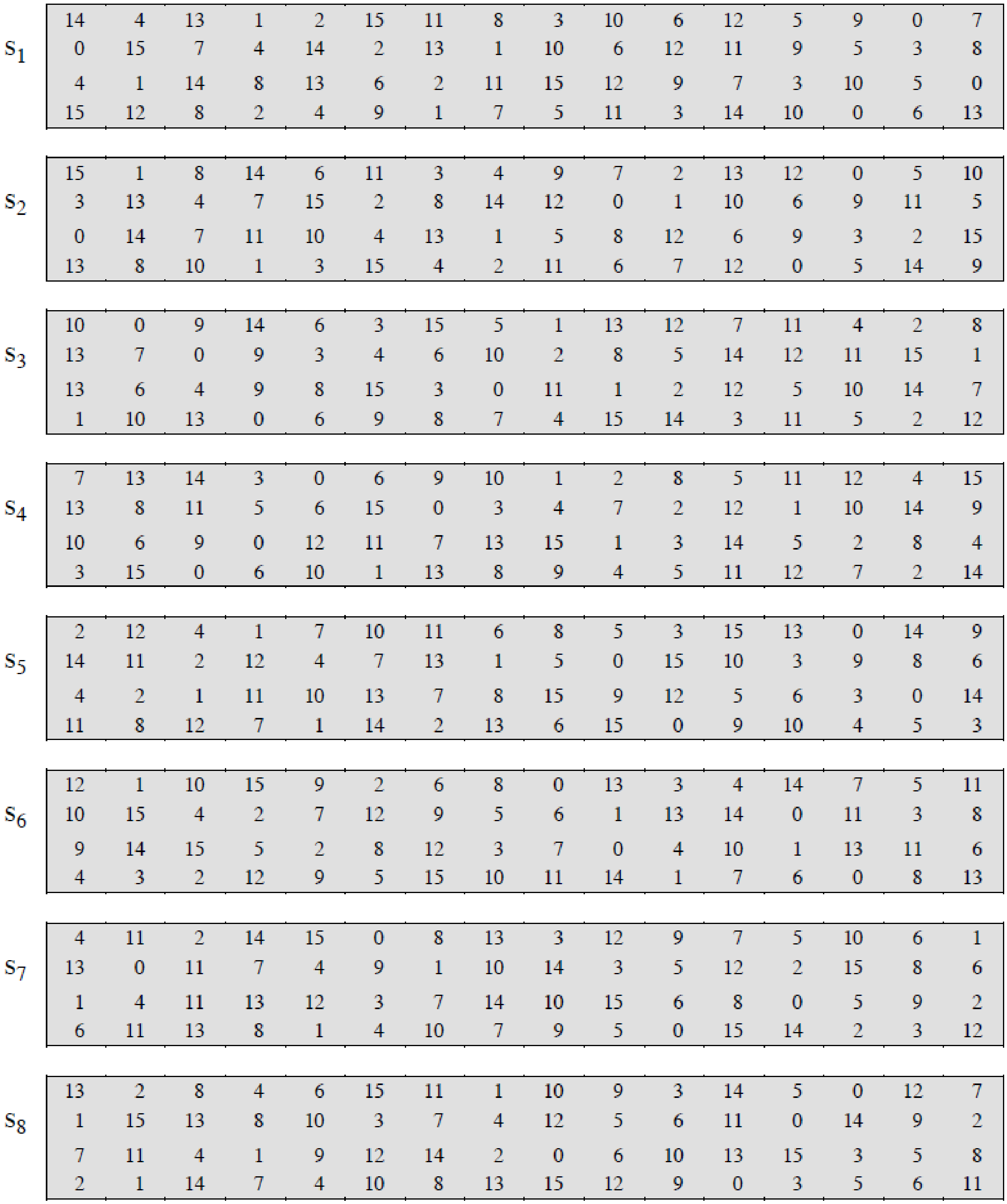
The Input/ Output relation in 2 x 2 a S-box is shown by the following table . Show the table for the inverse S-box.

		Input: right bit	
		0	1
Input: left bit	0	01	11
	1	10	00

Answer:

Question 13:

Definitions of DES S-Boxes are as follows:



S_1	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
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Answer the following questions about S-boxes in DES: **(5 Marks)**

A. Show the result of passing 110111 through S-box 3
B. Show the result of passing 001100 through S-box 4
C. Show the result of passing 000000 through S-box 7
D. Show the result of passing 111111 through S-box 2
E. Draw the table to sow the result of passing 111111 through all 8 S-boxes. Do you see a pattern in the outputs?

Answer:

Question 14: (10 Marks)

Ahmed is using RSA crypto-system with the following setup:

- p = 11 and q = 3
- n = pq = 11 × 3 = 33.
- Φ(n) = (p − 1)(q − 1) = 10 × 2 = 20.
- Ahmed publish his Public Key:
  (n, e) = (33, 3).

A. Calculate Ahmed's private key.
B. Charlie wants to send the message M = 13 to Ahmed. Using Ahmed's public and private keys, calculate the ciphertext C, and the value for Message R, when Alice recovers the message.
C. Dixit wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find his private and public keys.

Answer:

Question 15: (5 Marks)

In a RSA cryptanalysis , assume $n = 209$ and $\phi(n) = 180$. Calculate p and q.

Answer:

Question 16: (5 Marks)

In a RSA cryptanalysis, you intercept the ciphertext C = 10 sent to a user whose public key is (e = 7, n = 35). What is the plaintext M?

Answer:

Question 17: (5 Marks)

How many primitive roots are available for 43? Find all of them.

Answer:

Question 18: (5 Marks)

In a Deffie-Hellman key exchange setup, for simplicity, consider the large prime **P = 53** and the primitive root of ***P*** is ***a = 5.*** A sender generates his random secret $\boldsymbol{X_A}$ ***=12*** and the receiver generates his random secret $\boldsymbol{Y_B}$ ***= 18***. Calculate the session key.

Answer: