SP 24 INFO-231

Homework 5 Solutions - DES, Group Theory and Hill Cipher

Due Date: 11:59pm, Thursday, 02/22/2024

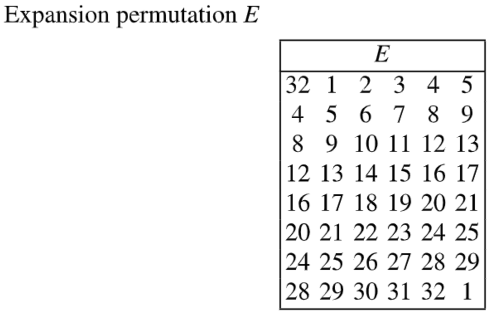
This homework contains 5 questions.

Grade Table (for grading use only)

Question	Points	Score
1	20	
2	25	
3	25	
4	15	
5	15	
Total:	100	

IU user name:____________________

1. (20 points) Given the input bits 11001100 10110101 00011111 01110010 and the expansion mapping shown below, what is the resulting output after Permutation?



Expansion permutation *E*

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

The given question is asking us to convert the following 32-bit input to a 48-bit input length. To do this, we have to understand the DES initial step which is the conversion of 32-bit input to 48-bit input using an Expansion Box (E).

A.The given input Bits are of length 32-bit:

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix}$$

B.By removing the first and last column of Expansion Box(E) and comparing the value which we wrote below, we can tell that following matches this way:

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \rightarrow \begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 \\ 29 & 30 & 31 & 32 \end{vmatrix}$$

C.Now bring the first and last row back and inserting the values based on the numbers, we can create the following :

$$\begin{vmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{vmatrix} \rightarrow \begin{vmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{vmatrix}$$

D.Final Answer is a 48-bit solution:

01100101 10010101 10101010 10001111 11101011 10100101

2. (25 points) In the previous homework you used the matrix below to encrypt the plaintext "RONALDO". Encrypted Text Result is: **FZXUWDOIP**

   Now calculate the inverse, and decrypt your message. Please review pages Chapter-6 Hill Cipher in the Rubinstein Salzedo textbook from week 5.

   Show your calculation of the determinant, its inverse with the multiplication of its inverse, and write out the decryption. You will not get points if you just provide the value.

$$\begin{pmatrix} 10 & 17 & 5 \\ 21 & 6 & 20 \\ 2 & 2 & 11 \end{pmatrix}$$

determinant $= -2837$
$-2837 \mod 26 = 23$

modular inverse of determinant $= 17$

$$adj \begin{pmatrix} 10 & 17 & 5 \\ 21 & 6 & 20 \\ 2 & 2 & 11 \end{pmatrix} = \begin{pmatrix} 26 & -177 & 310 \\ -191 & 100 & -95 \\ 30 & 14 & -297 \end{pmatrix} \mod 26 = \begin{pmatrix} 0 & 5 & 24 \\ 17 & 22 & 9 \\ 4 & 14 & 15 \end{pmatrix}$$

$$deteminant \times \begin{pmatrix} 0 & 5 & 24 \\ 17 & 22 & 9 \\ 4 & 14 & 15 \end{pmatrix} \mod 26 = \begin{pmatrix} 0 & 7 & 18 \\ 3 & 10 & 23 \\ 16 & 12 & 21 \end{pmatrix}$$

Multiply the indices of the encrypted text with the modular inverse of determinant and get the dencrypted text.

3. (25 points) In the previous homework you used the matrix below to encrypt the plaintext "PASSWORD". Encrypted Text Result is: **EZNQOMFGU**.

   Now calculate the inverse, and decrypt your message. Please review pages Chapter-6 Hill Cipher in the Rubinstein Salzedo textbook from week 5.

   Show your calculation of the determinant, its inverse with the multiplication of its inverse, and write out the decryption. You will not get points if you just provide the value.

   $$\begin{pmatrix} 6 & 20 & 1 \\ 17 & 16 & 19 \\ 21 & 14 & 15 \end{pmatrix}$$

   Similar steps but determinant is 0, so the calculating the decryption is not possible

4. (15 points) What is a group? From the readings or the slides, write a formula or alternatively state in clear words the meaning of the following modulo a natural number.

   For example, for *closure under addition*
   For all a, b which are element of the group is defined as the natural numbers mod(n):
   a+b is an element of that group, or a+b is an element of 0, 1, 2, ..., n-1
   If there are two positive integers that are less than n-1 then the sum of those elements can be reduced to an element in mod.

   - Associative under addition
   - Additive identity exists
   - Commutative under addition
   - Closure under multiplication
   - Associative under multiplication
   - Distributive
   - Commutative under multiplication

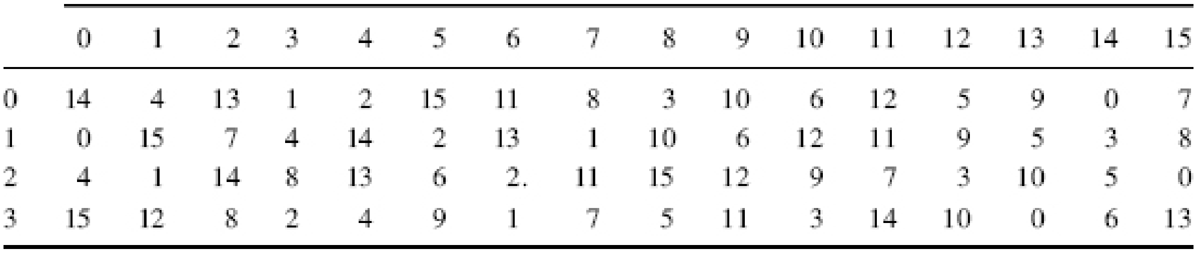
- Multiplicative identity

- Multiplicative inverse

A group, in the context of abstract algebra, is a set equipped with a binary operation that satisfies certain properties. Let's define these properties modulo a natural number n:

1. **Closure under addition**: For all a, b which are elements of the group defined as the natural numbers mod n, $a+b$ is an element of that group, or $a+b$ is an element of $0, 1, 2, \ldots, n-1$.
2. **Associative under addition**: For all a, b, c in the group defined as the natural numbers mod n, $(a+b)+c = a+(b+c)$.
3. **Additive identity exists**: There exists an element e in the group such that for all a in the group, $a+e = e+a = a$. Here, e is the additive identity, often denoted as 0.
4. **Commutative under addition**: For all a, b in the group defined as the natural numbers mod n, $a+b = b+a$.
5. **Closure under multiplication**: For all a, b in the group defined as the natural numbers mod n, $a \times b$ is an element of that group, or $a \times b$ is an element of $0, 1, 2, \ldots, n-1$.
6. **Associative under multiplication**: For all a, b, c in the group defined as the natural numbers mod n, $(a \times b) \times c = a \times (b \times c)$.

5. (15 points) Write the compressed output after the bits go through the following s box. Remember the activity we did in class to work on this problem. Go through the week's slides if needed.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2.	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

First two bits help us identify the row and the last 4 bits helps us identify the column

(a) 101101 - 10

(b) 110010 - 8

(c) 011110 - 3

(d) 100101 - 6

(e) 010111 - 1