SP 24 INFO-231
Homework 5 - 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 username: irmeyer

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

1 1 0 0 – matrix without outside rows of E
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

– use this matrix against E to solve for which numbers go in the outer rows

0 1 1 0 0 1 —-final matrix
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

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.

det(A) = a(ei-fh) - b(di-fg) + c(dh-eg)

det(A) = 10(6*11-20*2) - 17(21*11 - 20*2) + 5(21*2-6*2)

260	-	3247	+	150
		-2837 (mod 26)		
		det(A) = 23		

inverse calculation:

23x = 1 mod 26

23(17) = 391

26(15) = 390

391 - 390 = 1 mod 26

23(17) = 1 mod 26

	10 17 5		6*11-2*20	-(2*5-11*17)	17*20-5*6
adj	21 6 20	=	-(20*2-21*11)	11*10-5*2	-(5*21-20*10)
	2 2 11		21*2-6*2	-(2*17-2*10)	10*6-21*17

adj =	26 -177 310	mod 26	adj	=	0 5 24	mod 26
	-191 100 -95				17 22 9	
	30 14 -297				4 14 15	

decryption:

0 5 24			0 85 408		0 7 18
17 22 9	* 17	=	229 374 153 (mod 26)	=	3 10 23
4 14 15			68 238 255		16 4 21

0 7 18		5(f)		589			17 – R
3 10 23	*	25(z)	=	794	(mod 26)	=	14 – O
16 4 21		23(x)		663			13 – N
0 7 18		20(u)		208			0 – A
3 10 23	*	22(w)	=	349	(mod 26)	=	13 – L
16 4 21		3(d)		471			3 – D
0 7 18		14(o)		326			14 – O
3 10 23	*	8(i)	=	467	(mod 26)	=	25 – Z
16 4 21		15(p)		571			25 – Z

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 in verse, and write out the decryption. You will not get points if you just provide the value.

6 20 1
17 16 19
21 14 15

encrypted text:	as matrix:
E Z N	4 25 13
Q O M	16 14 12
F G U	5 6 20

determinant calculation:

4 25 13	4(14*20 - 12*6) - 25(16*20 - 12*5) + 13(16*6 - 14*5)
16 14 12	832 - 6500 + 338
5 6 20	-5330 mod 26

det(A) = 0

Since this determinant mathematically works out to equal zero we know that an inverse is not possible. This means that there are an infinite number of solutions.

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.

A group is a set of elements that are denoted by a number that associates to each ordered pair of the elements in the group.

- Associative under addition

  $[(x + y) + z] mod\, n = [x(y + z)] mod\, n$

  $a + (b + c) = (a + b) + c\ for\ all\ a,\ b,\ c\ in\ the\ group$

- Additive identity exists

  $(0 + x) mod\, n = x\ mod\, n$

  $There's\ an\ element\ e\ in\ G\ such\ that\ a + e = e + a = a\ for\ all\ a\ in\ G$

- Commutative under addition

  $(x + y) mod\, n = (y + x) mod\, n$

  $a * b = b * a\ for\ all\ a, b\ in\ G$

- Closure under multiplication

  $x\ mod\, n\ \&\ y\ mod\, n \Rightarrow xy\ mod\, n$

- Associative under multiplication

  $[(x * y) * z] mod\, n = [x * (y * z)] mod\, n$

  $a * (b * c) = (a * b) * c\ for\ all\ a,\ b,\ c\ in\ G$

- Distributive

  $[x(y + z)] mod\, n = [(x * y) + (x * z)] mod\, n$

- Commutative under multiplication

  $(x * y) mod\, n = (y * x) mod\, n$

  $a + b = b + a\ for\ all\ a, b\ in\ G$

- Multiplicative identity

  $(1 * x) mod\, n = x\ mod\, n$

- Multiplicative inverse

  $(x, y)\ where\ (x * y) mod\, n \equiv 1\ mod\, n$

  $for\ each\ x \in Zn,\ x > 0,\ there\ exists\ a\ y\ such\ that\ (x * y) \equiv 1\ mod\, n$

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

(a) 10|1101

where 2 crosses 13 = 10 – 1010

(b) 11|0010

where 3 crosses 2 = 8 – 1000

(c) 01|1110

where 1 crosses 14 = 3 – 0011

(d) 10|0101

where 2 crosses 5 = 6 – 0110

(e) 01|0111

where 1 crosses 7 = 1 – 0001