Assignment 4

rap180002 - CS 4389.501 - 10/1/21

Question 1

1.) (50 POINTS – 25 POINTS each) A ciphertext C given as follows: "TEBKFKQEBZLROPBLCERJXKBSBKQP" is known to be enciphered using the Caesar cipher.

1.A.) (25 POINTS) Decrypt the ciphertext C by using brute force attack. Please show your work.

Decrypted Text: WHENINTHECOURSEOFHUMANEVENTS

See Java Program decrypt.java for solve method and output. (use BF for Brute Force)

1.B.) (25 POINTS) Decrypt the ciphertext C by using the ϕ(i) correlation model explained in detail below.

Decrypted Text: WHENINTHECOURSEOFHUMANEVENTS

See Java Program decrypt.java for solve method and output. (use COR for Correlation Model)

Use another 3 x 3 matrix as a key K to encrypt the plaintext P = "heyeverybody". 2.A.) (20 POINTS) Based on the key matrix K you have chosen, find K-1, i.e. the multiplicative inverse of K. Please show your work.

Key

2	1	1
3	2	1
2	1	2

Augmented Matrix.

2	1	1	1	0	0
3	2	1	0	1	0
2	1	2	0	0	1

Row 1 Pivot + First Column

1	1/2	1/2	1/2	0	0
0	1/2	-1/2	-3/2	1	0
0	0	1	-1	0	1

Row 2 Pivot + Second Column.

1	0	1	2	-1	0
0	1	-1	-3	2	0
0	0	1	-1	0	1

Row 3 Pivot + Third Column (Inverted Matrix on Right)

1	0	0	3	-1	-1
0	1	0	-4	2	1
0	0	1	-1	0	1

Question 2 Cont.

Alphabet Index

0	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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Selected Key:

2	1	1
3	2	1
2	1	2

Key Inverse:

3	-1	-1
-4	2	1
-1	0	1

2.B.) (20 POINTS) Find the cipher-text C. Please show your work.

“heyeverybody” (4x3) * Key (3x3) =

7	4	24
4	21	4
17	24	1
14	3	24

2	1	1
3	2	1
2	1	2

74	39	59
79	50	33
108	66	43
85	44	65

Multiplied Matrix Mod 26:

74	39	59
79	50	33
108	66	43
85	44	65

22	13	7
1	24	7
4	14	17
7	18	13

Encrypted Text:

22	**13**	**7**	**1**	**24**	**7**	**4**	**14**	**17**	**7**	**18**	**13**
W	N	H	B	Y	H	E	O	R	H	S	N

2.C.) (10 POINTS) Verify that your hill cipher system works properly: Can you obtain plaintext P from the ciphertext C you have calculated in previous step? Please show your work.

Key:

2	1	1
3	2	1
2	1	2

Key Inverse:

3	-1	-1
-4	2	1
-1	0	1

Inverse Key Mod 26

3	-1	-1
-4	2	1
-1	0	1

3	25	25
22	2	1
25	0	1

Encrypted Matrix * Inverse Key

22	13	7
1	24	7
4	14	17
7	18	13

3	25	25
22	2	1
25	0	1

527	576	570
706	73	56
745	128	131
742	211	206

Result Mod 26

527	576	570
706	73	56
745	128	131
742	211	206

7	4	24
4	21	4
17	24	1
14	3	24

Decrypted Text:

7	**4**	**24**	**4**	**21**	**4**	**17**	**24**	**1**	**14**	**3**	**24**
H	E	Y	E	V	E	R	Y	B	O	D	Y