INTRODUCTION TO CRYPTOGRAPHY – QUIZ 7
B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of submission: 22/02/2022

Quiz

1. (4 points) Let S_1 and S_2 be the standard Vigenére and Permutation ciphers, respectively, with $P = (Z_{26})^5$ (so the block length of each is $m = 5$). Consider the product cipher $S_1 \times S_2$. Consider the keycode k_1 = latex in Vigenére Cipher, and the key k_2 in Permutation Cipher given by

1	2	3	4	5
4	5	2	1	3

Find the decryption $d_{(k_1,k_2)}$(IEAEDURMZXALZTM) in $S_1 \times S_2$. Write your plaintext with spaces.

➔ m=5

k_1=latex

k_2^{-1} :

1	2	3	4	5
4	3	5	1	2

$d_{(k_1,k_2)}$(IEAEDURMZXALZTM)

(Cyclic after sequency of 5)

I	E	A	E	D	U	R	M	Z	X	A	L	Z	T	M
E	A	D	I	E	Z	M	X	U	R	T	Z	M	A	L
L	A	T	E	X	L	A	T	E	X	L	A	T	E	X
4	0	3	8	4	25	12	23	20	17	19	25	12	0	11
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11	0	19	4	23	11	0	19	4	23	11	0	19	4	23
19	0	10	4	7	14	12	4	16	20	8	25	19	22	14
T	A	K	E	H	O	M	E	Q	U	I	Z	T	W	O

Plaintext: take home quiz two

2. (3 points) Find a Vigenére keycode k_1' such that $d_{(k_2,k_1')}$(IEAEDURMZXALZTM) in $S_2 \times S_1$ is the same plaintext you obtained in previous problem.

➔ k_1=latex

k_2:

1	2	3	4	5
4	5	2	1	3

$k_1' = k_2(k_1)$

k2(LATEX) = EXALT

Therefore, k_1'=exalt

3. (4 points) Let M be the Multiplicative Cipher and S be the Shift Cipher. For the encryption rule $e_{(9,15)}(x)$ in M × S, find the corresponding encryption rule $e_{(c,d)}(x)$ in S × M. In other words, find the value of c and d such that $e_{(c,d)}(x)$ in S × M is equal to $e_{(9,15)}(x)$ in M × S

➔ $e_{(9,15)}(x) = e^S_{(9)}(e^M_{(15)}(x)) = e^S_{(15)}(9x) = 9x + 15 \bmod 26$
$e_{(c,d)}(x) = e^M_{(d)}(e^S_{(c)}(x)) = e^M_{(d)}(x+c) = (x + c)d \bmod 26$

9x + 15 = dx + cd mod26
Therefore, d=9

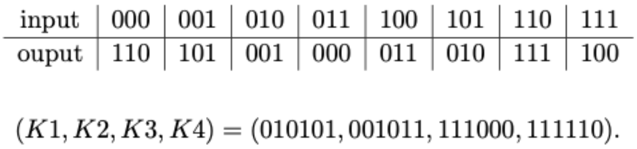
15=c9 mod 26

9x19=171 is equivalent to 15 in mod 26, therefore, c=19

Therefore, (c,d)=(19,9)

4. (9 points) Find the solution for problem 4 of the problem set 5. You should also write the intermediate results (i.e., the rows A, B, D, E, F, G, H, and J from Figure 1).

➔



input	000	001	010	011	100	101	110	111
ouput	110	101	001	000	011	010	111	100

$(K1, K2, K3, K4) = (010101, 001011, 111000, 111110).$

plaintext=100101

w0 = 1	0	0	1	0	1	Plaintext
k1 = 0	1	0	1	0	1	Key 1
u1 = 1	1	0	0	0	0	A
v1 = 1	1	1	1	1	0	B
w1 = 1	1	1	1	1	0	D
k2 = 0	0	1	0	1	1	Key 2
u2 = 1	1	0	1	0	1	E
v2 = 1	1	1	0	1	0	F
w2 = 1	0	1	1	1	0	G
k3 = 1	1	1	0	0	0	Key 3
u3 = 0	1	0	1	1	0	H

v3 = 0	0	1	1	1	1	J
k4 = 1	1	1	1	1	0	Key 4
u4 = 1	1	0	0	0	1	Ciphertext