1. (4 points) Let S_1 and S_2 be the standard Vigenére and Permutation ciphers, respectively, with $\mathcal{P} = (\mathbb{Z}_{26})^5$ (so the block length of each is $m = 5$). Consider the product cipher $S_1 \times S_2$. Consider the keycode $k_1 = \texttt{latex}$ 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 $d_{(k_1,k_2)}(\texttt{IEAEDURMZXALZTM})$ in $S_1 \times S_2$. Write your plaintext with spaces.

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

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

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).

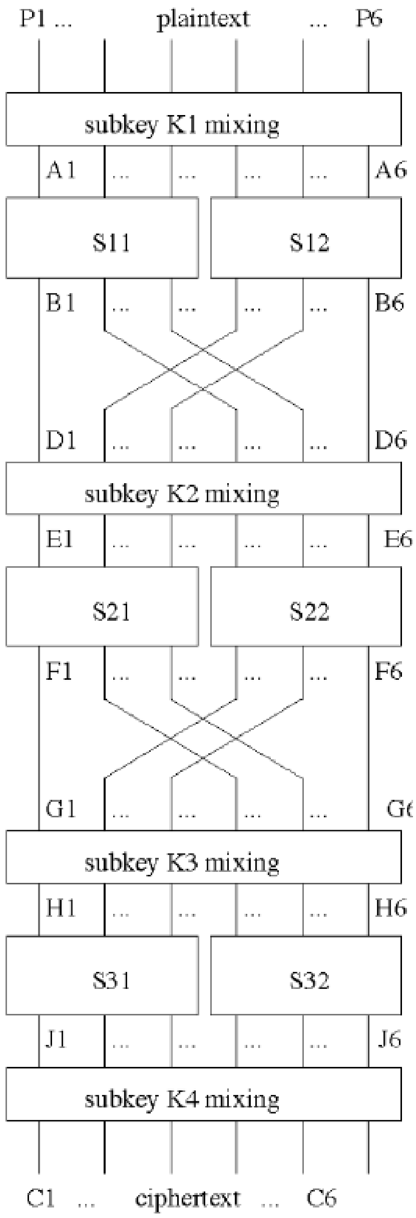
4. Consider a very simple substitution permutation network shown in Figure 1 on the next page at the end of this homework problems set. Assume that the S-box is as given below:

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

Find the encryption of the plaintext "100101", using the key

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

You should also show the intermediate results (i.e., the rows A, B, D, E, F, G, H, and J from Figure 1).



22-2-22

Quiz 7

A2.

Emil Pulickal
K046.

Q1. $m = 5$.

$S_1 \times S_2$

S_1: Vigenere, S_2: Permutation.

k_1 = latex.

k_2:

1	2	3	4	5
4	5	2	1	3

$k_2^{-1} \Rightarrow$

1	2	3	4	5
4	3	5	1	2

$d_{(k_1,k_2)}$(IEAED URMZX ALZTM)

$\Rightarrow d_{(k_1,k_2)}$(IEAED):

k_2^{-1}: I E A E D (1 2 3 4 5)

$\Rightarrow$ E A D I E

k_1: L A T E X

$\Rightarrow$ 11 0 19 4 23

$d_{(k_1,k_2)}$: E A D I E

4 0 3 8 4

$(c - k_2^{-1}) \bmod 26$: $-$(11 0 19 4 23)

19 0 10 4 7

T A K E H

$\therefore$ similarly: U R M Z X

k_1^{-1}: Z M X U R

25 12 23 20 17

$-$(11 0 19 4 23)

14 12 4 16 20

O M E Q U

A L Z T M

k_1^{-1}: T Z M A L

19 25 12 0 11

$-$(11 0 19 4 23)

8 25 -7 -4 -12

8 25 19 22 14

I Z T W O

Plaintext: TAKEHOMEQUIZTWO

$\Rightarrow$ take home quiz two

Q2. $k_1 =$ latex

$k_2 =$

1	2	3	4	5
4	5	2	1	3

(k_2, k_1') in $S_2 \times S_1$.

$\therefore$ First Vigenere then shift.

$\therefore$ Vigenere key k_1': $k_2(k_1)$

$\to k_2(LATEX)$: E X A L T

$\therefore k_1' =$ EXALT : <u>exalt</u>.

Q3. $e_{(9,15)}(x)$ in $M \times S$. equals →

$e_{(c,d)}(x)$ in $S \times M$

$\therefore e^{M \times S}_{(9,15)}(x) = e^S_{15}(e^M_9(x)) = e^S_{15}(9x) = \underline{9x+15 \mod 26}$

$e^{S \times M}_{(c,d)}(x) = e^M_d(e^S_c(x)) = e^M_d(x+c) = \underline{(x+c).d \mod 26}$

$\therefore 9x+15 = dx + cd \pmod{26}$

$\Rightarrow \therefore d = 9$

$9c = 15 \pmod{26}$

$\therefore 9 \times 19 = 171 \equiv 15 \pmod{26}$

$\therefore c = \underline{\underline{19}} \quad d = \underline{9}$

Q4. S box:

I/P.	000	001	010	011	100	101	110	111
O/P	110	101	001	000	011	010	111	100

plaintext: $w^0 = 100101$

$K^1 = 010101$

$u^1 = 110000 \longrightarrow A.$

$v^1 = 111110 \longrightarrow B.$

$w^1 = 111110 \longrightarrow D.$

$K^2 = 001011$

$u^2 = 110101 \longrightarrow E$

$v^2 = 111010 \longrightarrow F$

$w^2 = 101110 \longrightarrow G$

$K^3 = 111000$

$u^3 = 010110 \longrightarrow H$

$v^3 = 001111 \longrightarrow J$

$K^4 = 111110$

$u^4 = 110001 \longrightarrow$ ciphertext C.