USAMA SARWAR
FA17-BCS-090-B

Question # 01.

Additive Cipher

→ The most straightforward code is an additive cipher.
→ Each coded letter is essentially moved a specific number of spaces from the plaintext letter.
→ The case appeared below utilizes a key of 5. Utilizing the lowercase letter for plaintext and capital letters for cipher text.
→ In additive cipher lowercase can be used for plaintext and uppercase can be used for cipher text.
→ Suppose that a value of key is shifted to 5 then a will be shifted to position 5 that means it will be F and b will be G and so on.
→ Below is the complete table which shows the ciphes

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
q	r	s	t	u	v	w	x	y	z						
V	W	X	Y	Z	A	B	C	D	E						

⇒ As per given details, in order to send the messages Alice thinks about the double encryption with different keys in additive cipher the description is as follows

→ With the help of double encryption with different key will not work.

Proof

→ Suppose that the encryption with key $S1$ and followed by the encryption with key $S2$ that will be same like Encryption with key $S = (S1 + S2) \bmod 26$

→ Suppose that PT is a plain text and CT is a CipherText then;

$$\begin{aligned} CT &= [(PT + S1) \bmod 26 + S2] \bmod 26 \\ &= (PT \bmod 26 + S1 \bmod 26 + S2) \bmod 26 \\ &= (PT \bmod 26) \bmod 26 + (S1 \bmod 26) \bmod 26 + S2 \bmod 26 \\ &= PT \bmod 26 + S1 \bmod 26 + S2 \bmod 26 \\ &= (PT + S1 + S2) \bmod 26 \\ &= (PT + S) \bmod 26 \end{aligned}$$

where $S = (S1 + S2)$

Question # 02.

(a) Apply additive cipher key = 20 "this is an exercise."

Plain Text

	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e
P-Value	19	7	8	18	8	18	0	13	04	23	04	17	02	8	18	04
Key	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
C-Value	13	1	2	12	2	12	20	7	24	17	24	11	22	2	12	24
Cipher Text	N	B	C	M	C	M	U	H	Y	R	Y	L	W	B	M	Y

$$C = (P + K) \bmod 26$$

Ciphertext is

NBCMCMUHYRYLWBMY

Decrypt the message

	N	B	C	M	C	M	U	H	Y	R	Y	L	W	B	M	Y
C'-value	13	1	2	12	2	12	20	7	24	17	24	11	22	2	12	24
Key	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
P'-value	19	7	8	18	8	18	0	13	04	23	04	17	02	8	18	04
Plain Text	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e

$$\text{decrypt}\ (C - K) \bmod 26$$

Plaintext: this is an exercise

b) Multiplicative Cipher Key = 15

this is an exercise

Encrypt the message $C = (P \times K) \bmod 26$

	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e
P-Val	19	7	8	18	8	18	0	13	4	23	04	17	02	8	18	4
Key	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
C-Val	25	1	16	10	16	10	0	13	8	7	8	21	4	16	10	8
Cipher Text	Z	B	Q	K	Q	K	A	N	I	H	I	V	E	Q	K	I

Cipher Text is

ZBQKQKANIHIVEQKI

Decrypting the message

$P = (C \times K^{-1}) \bmod 26$

	Z	B	Q	K	Q	K	A	N	I	H	I	V	E	Q	K	I
C-Val	25	1	16	10	16	10	0	13	8	7	8	21	4	16	10	8
Key	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
K^{-1}	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
P-Val	19	7	8	18	8	18	0	13	4	23	04	17	02	8	18	4
Plain Text	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e

Original Plain Text

this is an exercise

(c) Affine Cipher with (15,20)

Encrypt $C = (P \times K_1 + K_2) \bmod 20$

By Calculating, we get

Cipher Text

TVKEKEUHCBCPYKEC

Decrypt $P = ((C - K_2) \times K_1^{-1}) \bmod 26$

By Calculating we get

Original Plain Text

this is an exercise

Usama Sarwar
FA17-BCS-090

Question # 03

Given Key = GUIDANCE

Constructing 5x5 Matrix

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

⇒ Text to be encrypted = "The key is hidden under the door pad".

⇒ Two letters repeating in words hidden & door
So, separating them with X

⇒ New Text

"The key is hidxden under the doxor pad.

⇒ Pairing

TH EK EY IS HI DX DE NU ND ER TH ED
OX OR PA DZ

↑ inserted to complete pair.

Converting into cipher text

Using P for Plain text & C for Cipher text

P	C	P	C
TH	PO	ND	BG
KK	CL	ER	LX
FRY	BX	TH	PO
IS	DR	ED	BI
HI	LG	OX	L2
DX	JY	OR	LT
DE	JB	PA	TG
NU	CG	DZ	AY

So, the cipher text is:

POCLBXDRLGJYJBCGBGLXPOBIL2LTTGAY

Question # 04

P_{10} = | 9 | 5 | 8 | 1 | 10 | 7 | 3 | 2 | 6 | 4 |

P_8 = | 6 | 8 | 5 | 7 | 2 | 1 | 3 | 4 |

Bits	1	2	3	4	5	6	7	8	9	10
key	0	0	0	1	0	1	0	1	0	0
P_{10}	0	0	1	0	0	0	0	0	1	1
Shift(P_{10})	0	1	0	0	0	0	0	1	1	0
P_8(Shift(P_{10}))	0	1	0	0	1	0	0			

Key 1 => 01001000

Bits	1	2	3	4	5	6	7	8	9	10
Key	0	0	0	1	0	1	0	1	0	0
P_{10}	0	0	1	0	0	0	0	0	1	1
$Shift^3(P_{10})$	0	0	0	0	1	1	1	0	0	0
$P_8(Shift^3(P_{10}))$	1	0	1	1	0	0	0	0		

Key 2 => 10110000

Question # 05.

$K_1 = 0100\ 1000$

$K_2 = 1011\ 0000$

$P = 0011\ 0110$

First Round

$IP(P) = \underbrace{0010}_{P_L}\ \underbrace{0111}_{P_R}$

$EP(P_R) = 1101\ 1011$

$K_1 = 0100\ 1000$

$K_1 \oplus EP(P_R) = \underline{1001}\ \underline{0011}$

S_0

1001

$R: 11 \rightarrow 3$

$C: 00 \rightarrow 0$ — 3 → 11

S_1

0011

$R: 01 \rightarrow 1$

$C: 01 \rightarrow 1$ — 0 → 00

After S Boxes

1100

$P4(1100) \rightarrow 0011$

$\boxed{F = 0011}$

$F \oplus IP(R_2)$

$F = 0011$

$IP(R_2) = 0010$

0001

$\boxed{00010111}$

$SW(00010111)$

$= 01110001$

Round 2

$\underbrace{0111}_{R_L}$ $\underbrace{0001}_{R_R}$

$EP(R_R) = 10000010$

$K_2 = 10110000$

$\oplus = 00110010$

S_0

0011

R: 01 → 1 \
C: 01 → 1 — 2 → 10

S_1

0010

R: 00 → 0 \
C: 01 → 1 — 1 → 01

After S Boxes

1001

$P_4(1001) = 0101$

$F = 0101$

$R_e = 0111$

$\oplus = 0010$

Before performing IP^{-1} $R_e = 0001$

00100001

$IP^{-1}(00100001) = ?$

Bit No.	1	2	3	4	5	6	7	8
	0	0	1	0	0	0	0	1
IP^{-1}	0	1	1	0	0	0	0	0

Cipher Text = 01100000