Question-1

GCD (56, 15) = 56x + 15y

$$15 \overline{)56}\ 3,\ 45,\ 11$$

Step-A

$a = qb + r$

① $56 = 3 * 15 + 11$

$$11 \overline{)15}\ 1,\ 11,\ 4$$

② $15 = 1 * 11 + 4$

$$4 \overline{)11}\ 2,\ 8,\ 3$$

③ $11 = 2 * 4 + 3$

$$3 \overline{)4}\ 1,\ 3,\ 1$$

④ $4 = 1 * 3 + 1$

$$1 \overline{)3}\ 3,\ 3,\ 0$$

⑤ $3 = 3 * 1 + 0$ ← remainder → 0

Step-B

Taking the 4th step

$1 \Rightarrow 4 - (1 * 3)$ ↙ From step-3

$\Rightarrow 4 - [1 * (11 - 2 * 4)]$

$\Rightarrow 4 - [11 - (2 * 4)]$

$\Rightarrow (1 * 4) - 11 + (2 * 4)$

$\Rightarrow (3 * 4) - 11$ ↙ From step-2

$\Rightarrow 3 * [15 - (1 * 11)] - 11$

$\Rightarrow (3 * 15) - (3 * 11) - (1 * 11)$

$\Rightarrow (3 * 15) - (4 * 11)$ ↙ From step-1

$\Rightarrow (3 * 15) - (4 * [56 - (3 * 15)])$

$\Rightarrow (3 * 15) - (4 * 56) + (12 * 15)$

$\Rightarrow (15 * 15) - (4 * 56)$

$\Rightarrow$

Therefore $1 \Rightarrow (15 * 15) - (4 * 56)$

~~$x \Rightarrow 15$~~
~~$y \Rightarrow -4$~~

$x \Rightarrow -4$
$y \Rightarrow 15$

$5 \mid 15$
$3 \mid 3$
1

$2 \mid 4$
$2 \mid 2 \quad 0$
1

LCM of 15 $\Rightarrow 5 \times 3 \times 1$

LCM of 56 $\Rightarrow 2 \times 2 \times 2 \times 7 \times 1$

$2 \mid 56$
$2 \mid 28$
$2 \mid 14$
$7 \mid 7$
1

$\therefore$ GCD of 15 and 56 $\Rightarrow 1$

Verification

$56x + 15y \Rightarrow$ ~~$56(15) + 15(-4)$~~

$\Rightarrow 56(-4) + 15(15)$

$56x + 15y \Rightarrow 1$

Hence proved.

plain text ⇒ "Hide diamond immediately"

key ⇒ "Occurrence"

Algorithm: Playfair cipher

Step-A (Key Matrix)

	1)	2)	3)	4)	5)
1)	o	c	u	r	e
2)	n	a	b	d	f
3)	g	h	i/j	k	l
4)	m	p	q	s	t
5)	v	w	x	y	z

Step-B (Splitting up the plain text)

hi de di am on di [illegible] mx me di at el gx

Step-C (Encryption)

*) Lies on the same row ⇒ immediate right

*) Lies on the same column ⇒ immediate low

*) Lies on the different row, different column ⇒ Diagonal

*) hi [same row] ⇒ ik | jk

g	h	i/j	k	l

*) de ⇒ fr

r	e
d	f

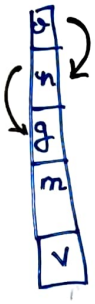
*) di ⇒ bk

b	d
i/j	k

*) am ⇒ np

n	a
g	h
m	p

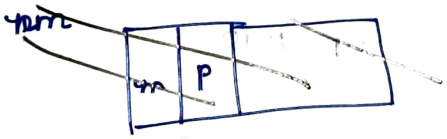
*) on ⇒ ng



di ⇒ bk

b	d
i/j	k

*) [illegible]



⇒ qv

*) mx

m	p	q
v	w	x

*) me

o	c	u	r	e
n	a	b	d	f
g	h	i/j	k	l
m	p	q	s	t

*) di ⇒ bk

*) at ⇒ fp

a	b	d	f
h	i/j	k	l
p	q	s	t

*) el ⇒ ft

⇒ to

*) yx ⇒ zy

v	w	x	y	z

Hence Cipher text

ik/ij fr bk np ng bk qv to bk fp ft to

DES algorithm

a) Given key K ⇒ 1AD33F34560 1071A

Generate 48 bit sub-key

*) Hexa-Decimal value for the key ⇒ 1AD33F345601071A

*) Decimal value for the key ⇒ 49 65 68 51 51 70 51 52 53 54 48 55

*) Binary Representation

1	A	D	3	3	F	3	4	5
0001	1010	1101	0011	0011	1111	0011	0100	0101

6	0	1	0	7	1	A
0110	0000	0001	0000	0111	0001	1010

*) Grouping into 8 bits

(1) 8 ≡ 00011010

(9) 8 ≡ 11010011

(17) 8 ≡ 00111111

(25) 8 ≡ 00110100

(33) 8 ≡ 01010110

(41) 00000001 8

(49) 00000111 8

(57) 00011010 8

Permuted choice-1

LK

0 0 0 0 0 0 1
0 0 0 0 1 0 0
1 0 0 0 0 0 1
1 0 0 1 0 0 1

RK

1 1 0 1 0 1 1
1 0 1 0 1 1 1
0 0 1 0 0 0 0
1 0 1 1 1 1 1

output ⇒ 56 bits

LCS

LK

0 0 0 0 0 1 0
0 0 0 1 0 0 0
0 0 0 0 0 1 1
0 0 1 0 0 1 1

RK

1 0 1 0 1 1 1
0 1 0 1 1 1 1
0 1 0 0 0 0 0
0 1 1 1 1 1 1

↓ 56 bits

Permuted choice-2

↓ 48 bits

XOR

6)

XOR

input ⇒ Expansion Matrix ⇒ 48 bits

output ⇒ 48 bits

same bit ans ⇒ 0

different bit ans ⇒ 1