Question-1

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

$$\begin{array}{r} 3 \\ 15\overline{)56} \\ 45 \\ \hline 11 \end{array}$$

$$\begin{array}{r} 1 \\ 11\overline{)15} \\ 11 \\ \hline 4 \end{array}$$

$$\begin{array}{r} 2 \\ 4\overline{)11} \\ 8 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 1 \\ 3\overline{)4} \\ 3 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 3 \\ 1\overline{)3} \\ 3 \\ \hline 0 \end{array}$$

Step-A

$\boxed{a = qb + r}$

① $56 = 3*\boxed{15 + 11}$

② $15 = 1*\boxed{11 + 4}$

③ $11 = 2*\boxed{4 + 3}$

④ $4 = 1*\boxed{3 + 1}$

⑤ $3 = 3*\boxed{1 + 0}$

↑ remainder => 0

Step-B

Taking the 4th step

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

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

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

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

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

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

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

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

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

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

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

Therefore 1 => (15 * 15) - (4 * 56)

~~x => 15~~
~~y => -4~~

$\boxed{\begin{array}{l} x \Rightarrow -4 \\ y \Rightarrow 15 \end{array}}$

$$\begin{array}{r|l} 5 & 15 \\ 3 & 3 \\ & 1 \end{array} \qquad \begin{array}{r|l|l} \cancel{2} & 4 & \\ 2 & \boxed{2} & 0 \\ & 1 & \cancel{0} \end{array}$$

LCM of 15 => 5 × 3 × 1

LCM of 56 => 2 × 2 × 2 × 7 × 1

$$\begin{array}{r|l} 2 & 56 \\ 2 & 28 \\ 2 & 14 \\ 7 & 7 \\ & 1 \end{array}$$

$\boxed{\therefore \text{ GCD of 15 and 56} \Rightarrow 1}$

Verification

56x + 15y => ~~56 (15) + 15 (-4)~~

=> 56 (-4) + 15 (15)

56x + 15y => 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 mx me di at el yx

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

*) an ⇒ np

n	a
g	h
m	p

*) on ⇒ ng

o
n
g
m
v

di ⇒ bk

b	d
i/j	k

*) ~~nm~~

~~m~~	~~p~~	

*) mx ⇒ qv

m	p	q
v	w	x

*) ne ⇒ to

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

e
f
l
t
z

*) 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 — 0 0011010

(9) 8 — 11010011

(17) 8 — 0011 1111

(25) 8 — 00110100

(33) 8 — 01010110

(41) 00 00 0001 — 8

(49) 00000111 — 8

(57) 0001010 — 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
49 0 0 1 0 0 0 0
65 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 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