Amit K. Nerurkar

VIT Vidyalankar Institute of Technology
(Accredited A+ by NAAC)
(Autonomous Institute Affiliated to University of Mumbai)

Mid Semester Examination

Branch	Date	Sem.	Roll No. / Exam Seat No.	Subject	Student's Signature	Junior Supervisor's Name and Sign
CMPN	11/3	5	-	CSS-2		

Question No.	A	B	C	D	E	F	G	H	Total	Total out of (20 /30 / 40)
1										
2										
3										
4										

Examiners Signature	Student's Sign (After receiving the assessed answer sheet)

Q1.a

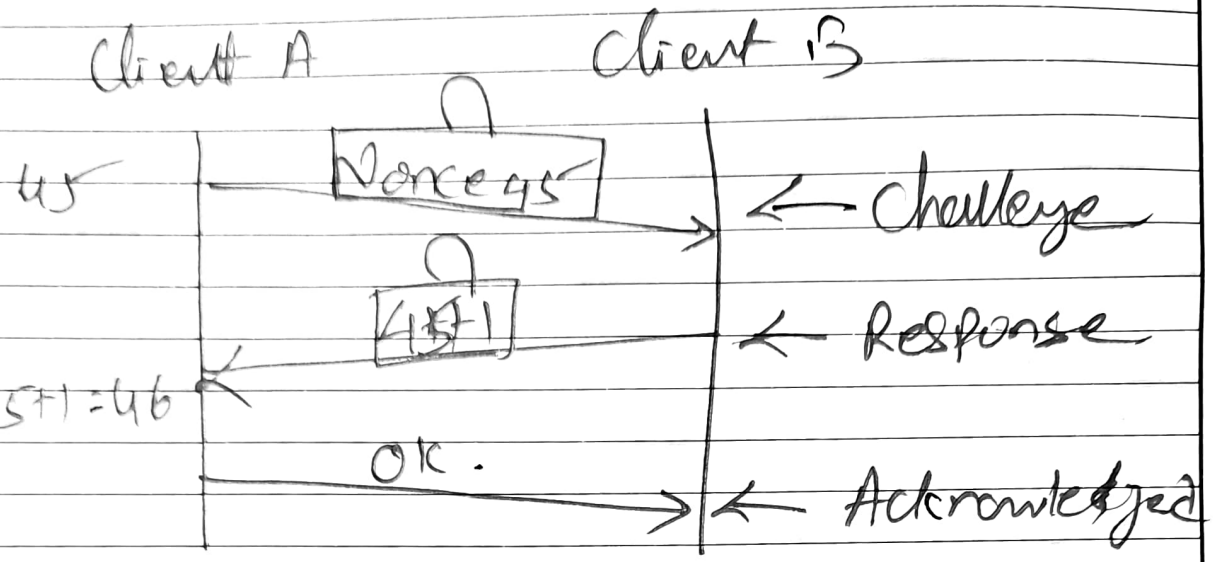
(1) TGS:

It is Ticket Granting Ticket which is used for authorizing the client

(2) TGT:

It is Ticket Granting Ticket which KDC uses to validate client & further give it to TGS for authorization.

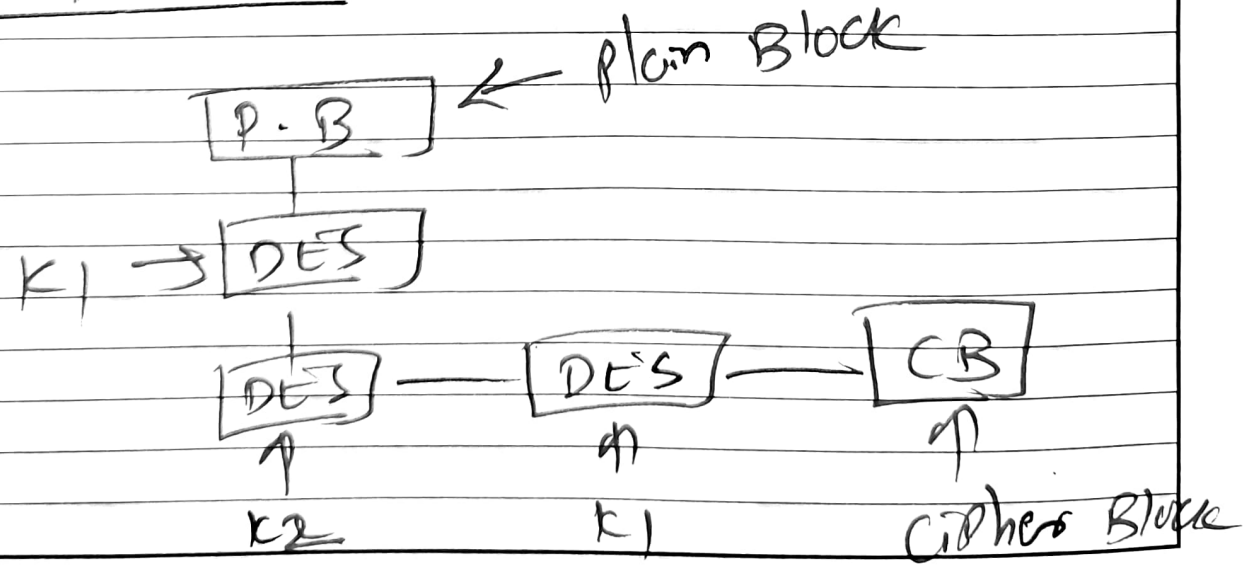
Q1
b



Q1
c

$$P = D(K_1, E(K_2, D(K_3, C)))$$

Q1
d. Triple DES



Q)

e. Key scheduling needs n iteration

n = size of S array

Key stream generation needs iteration equal to size of key(K) array.

Q)

f. RC4

P.T.(142, 90) ~~f~~ key(63, 57)

P.T.	128	64	32	16	8	4	2	1
142	1	0	0	0	1	1	1	0
90	0	1	0	1	1	0	1	0
63	0	0	1	1	1	1	1	1
57	0	0	1	1	1	0	0	1

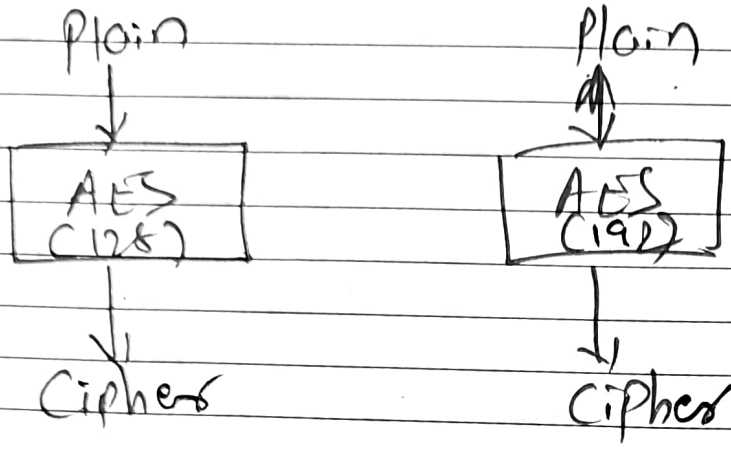
10001110 01011010 ∴CT(177, 99)

XOR

00111111 00111001

10110001 01100011

Q1 g.



10 Rounds

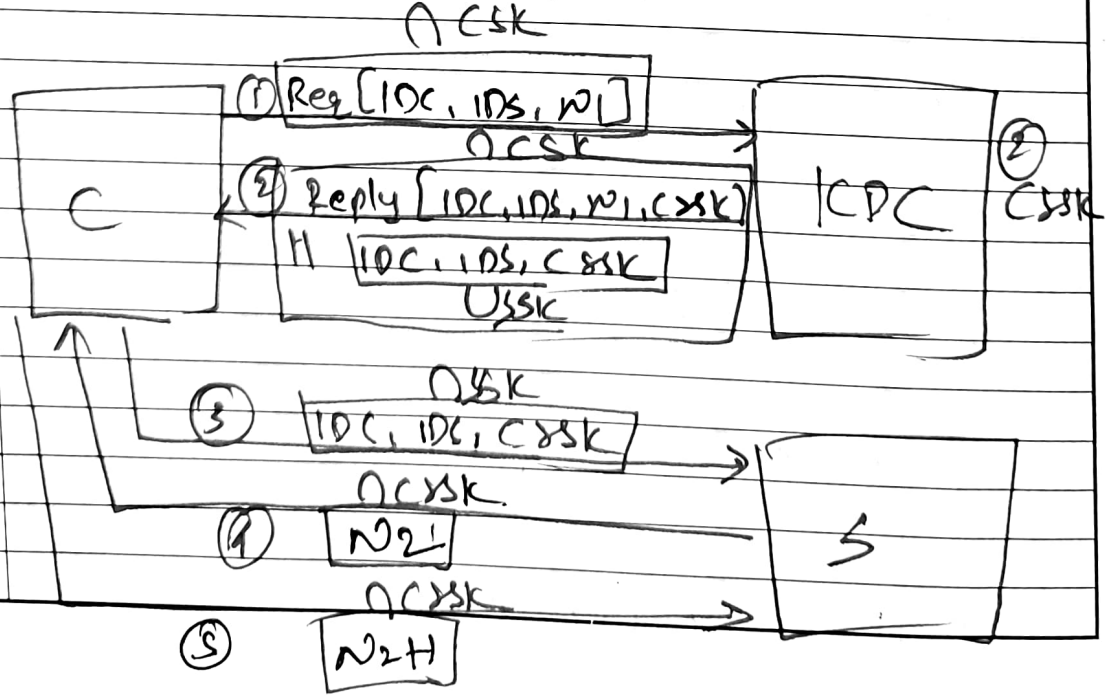
12 Rounds.

Q1 h

It shares CSK [Client Server Secret Key] ie the session key. KDC of the system creates & shares that.

KDC: Key distribution center.

Q2 a.



(1) Client sends Request to KDC [Key Distribution center] by encrypting using CSK [Client Server key]
session

(2) KDC decrypts that using client's session key & then generates session key for Client & Server CSSK. Sends it to client with appended Encrypted message to server.

(3) Client decrypts the message, keeps CSSK, & forwards encrypted message to Server.

(4) Server decrypts the message, takes CSSK & sends Nonce as Challenge (N1) encrypted using CSSK. & gives it to client

(5) Client solves challenge & responds using N2+1 encrypted using CSSK.

(6) Server checks the response & authenticates the client

Q) b.

Cipher text using Knapsack

| 0 | 1 | 1 | 0 | 0 | 1 | 1 |

*

| 1 | 4 | 6 | 9 | 30 | 50 | 70 | 90 |

1 + 0 + 6 + 9 + 0 + 0 + 70 + 90

$CT_1 = 176$

| 1 | 0 | 0 | 1 | 1 | 00 |

*

| 1 | 4 | 6 | 9 | 30 | 50 | 70 | 90 |

1 + 4 + 0 + 0 + 30 + 50 + 0 + 0

CT2 88

| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |

*

| 1 | 4 | 6 | 9 | 30 | 50 | 70 | 90 |

1 + 0 + 6 + 9 + 0 + 50 + 70 + 90

CT3 226

1 1 0 0 0 0 1 1

* 1 4 6 9 30 50 70 90

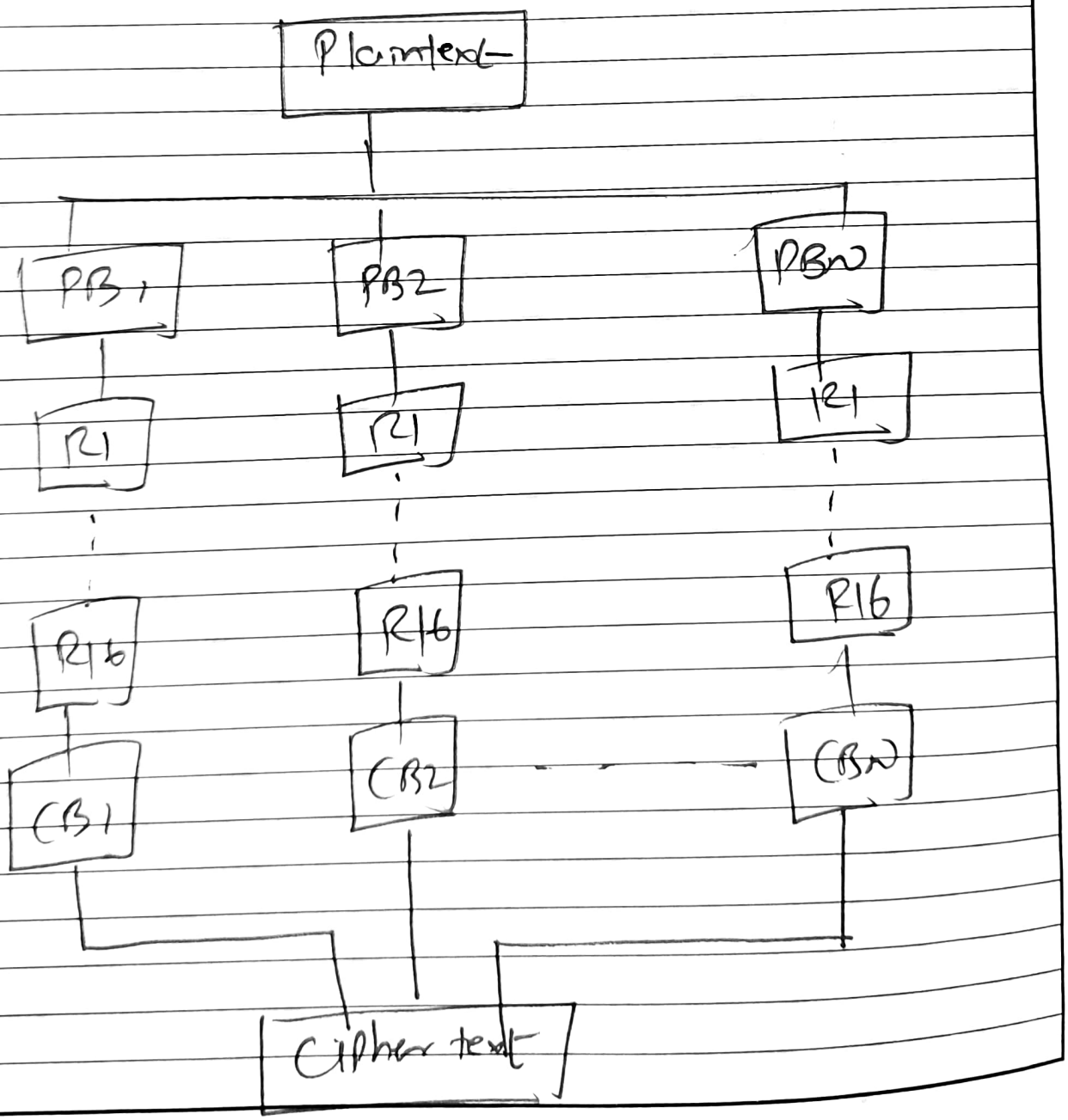
1 + 4 + 0 + 0 + 0 + 0 + 70 + 90

CT4 165

Q3

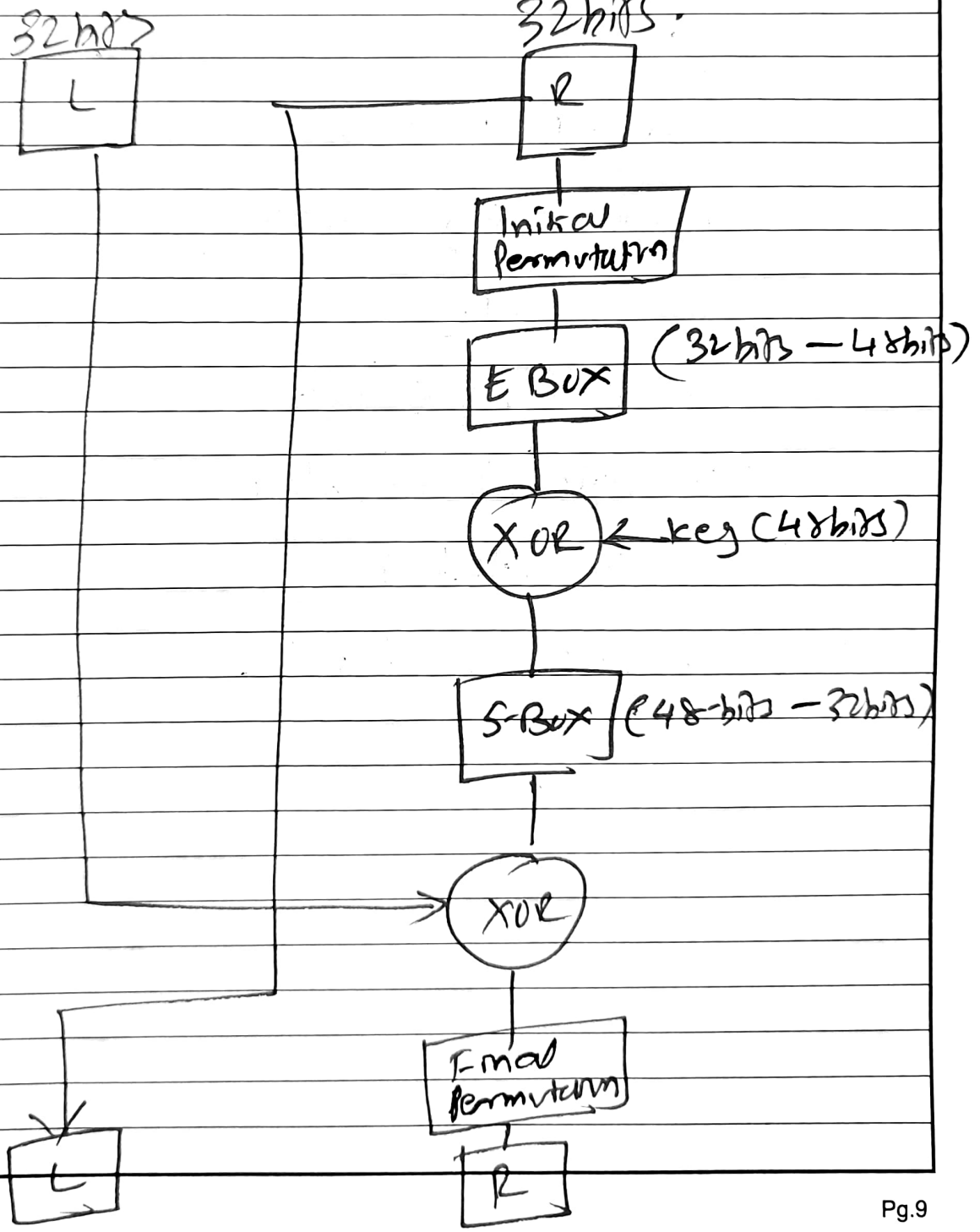
a) DES:

- Data Encryption Standard is block level cipher designed by IBM in 1970's.
- It uses block of 64 bits & performs the Encryption operation using 48 bits of key.



- As shown above, it divides plain text into 64 bits block & then applies 16 Rounds of operation on every block.
- Finally the cipher Blocks are merged to final cipher text.

Every Round operation:



- As shown above, 64 bits block is divided into L & R sub block each of 32 bits.

- L subblock becomes new L sub block

- for new R sub block perform:

1. Initial permutation.
2. Expansion using E-Box
3. XOR with key
4. Compress using S-Box
5. XOR with L sub block
6. Final permutation
7. Final new R sub block.

Q3 a) Diffie Hellman algorithm

Given

SX	PX
$q = 13$	$q = 13$
$\alpha = 6$	$\alpha = 6$

① Assume
$X_A = 5$
$(X_A < q)$

① Assume
$X_B = 4$
$(X_B < q)$

② Public key
$Y_A = \alpha^{X_A} \bmod q$

$\therefore Y_A = 6^5 \bmod 13$

$\therefore \quad = 7776 \bmod 13$

$Y_A = 2$

Public key
$Y_B = \alpha^{X_B} \bmod q$

$Y_B = 6^4 \bmod 13$

$= 1296 \bmod 13$

$Y_B = 9$

$Y_B = 9$

$Y_A = 2$

(3) Calculating Session key

$K_A = y_B^{x_A} \bmod q$

$= 9^5 \bmod 13$

$\therefore K_A = 3$

(B) Calculation session key.

$K_B = y_A^{x_B} \bmod q$

$= 2^4 \bmod 13$

$K_B = 3$