Name: Sradha Kedia
Date of Examination: 18 December, 2021
Time of Examination: 9:30 am to 1:30 pm
Examination Roll no.: 20234757053
Semester: III
Unique Paper Code: 223401302
Title of Paper: Information Security
Email Id: 200083@cs.du.ac.in
Mobile no. of student: ~~200083@cs.du.ac.in~~ 9899519848
Question no.: 3
No. of pages: 5
Name of the program: MCA
Name of the Department: DUCS

Answer 3 (iii) a) 145^{102} mod 101 using Fermat's little thm.

According to fermat's little theorem,
if x and n are coprime and n is prime
then $x^{n-1} \equiv 1 \bmod n$
i.e. $x^{n} \equiv x \bmod n$ } — (i)

here, $x = 145$, $n = 101$ (prime)
$\therefore$ $145^{101} \equiv 145 \bmod 101$ (By thm) (i)

$\Rightarrow$ 145^{102} mod 101
$= 145^{101} \cdot 145$ mod 101
$= [(145^{101} \bmod 101) \cdot (145 \bmod 101)] \bmod 101$
$= (145 \times 44) \bmod 101$
$= [(145 \bmod 101)(44 \bmod 101)] \bmod 101$
$= (44 \times 44) \bmod 101$
$= 1936 \bmod 101$
$= 17$ (Ans)

(b) 38^{-1} mod 180 using Extended Euclidean Algo.

38^{-1} mod 180 means a no. 'x' s.t.
$38 \cdot x \equiv 1 \bmod 180$

q	r_1	r_2	r	t_1	t_2	$t = t_1 - q t_2$
4	180	38	28	0	1	-4
1	38	28	10	1	-4	5
2	28	10	8	-4	5	-14
1	10	8	2	5	-14	19
4	8	2	0	-14	19	-90
	2	0		19	-90	

$\rightarrow$ gcd $= r_1$

∴ gcd is 2
∴ 38 does not have a multiplicative inverse modulo 180.

(2) (i) P = "MEET AT FIRST AND PINE AT MIDNIGHT"
C = "TTEIERIDMIPIITNTHFDMTESNNAAAG"

The devised cipher scheme

3	2	6	1	7	4	5
M	E	E	T	A	T	F
I	R	S	T	A	N	D
P	I	N	E	A	T	M
I	D	N	I	G	H	T

a) According to above matrix, i.e 4 × 7 matrix
$m = 4, n = 7$

b) Bob is given $m = 4$, $n = 7$. now, he will take the ciphertext, and key = 3261745 (is required to decrypt). Bob will write cipher text by picking first four characters TTEI and place it in column four of matrix as col. 4 corresponds to 1.
then ERID and put it in second column.
IIly MIPI in 1 col as 1 corresponds to 3 and like this he will create the above matrix and now read it row by row thus obtaining plaintext.

c) VOHMIAEAXYATED , 14 characters, 7 key length

∴ 14/7 = 2 → rows , we apply same technique as (b)

3 2 6 1 7 4 5

⇒ I H A V E E X

A M T O D A Y

now, we read it row by row

I HAVE EXAM TODAY.

3 (ii) The ways in which secret keys can be distributed to the communating parties are

a) A key could be selected by A and physically delivers to B.

b) A third party could selected the key and physically delivers to b.

c) if A and B have previously and recently used a key. One party transmit the new key to the other using old key to encrypt the new key.

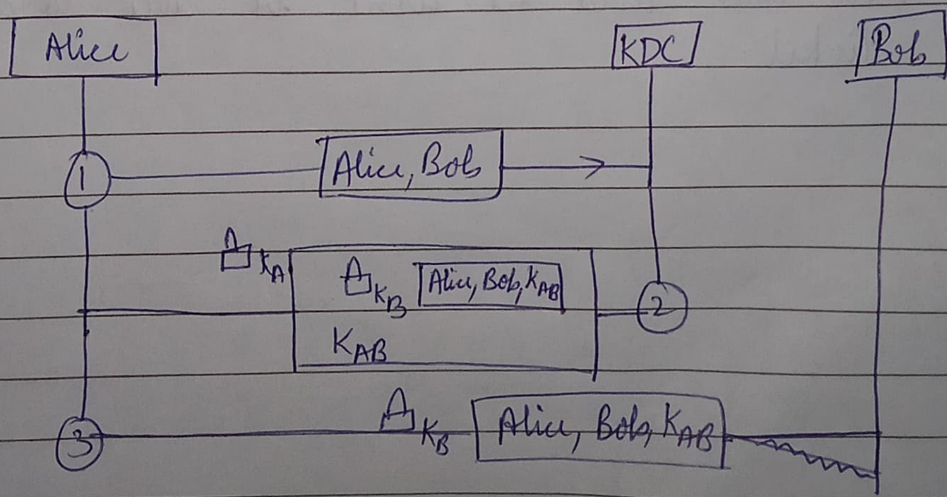
d) if A and B each have an encrypted connection to a third party C. C could delivers a key on the encrypted links to A and B.

K_A : Encrypted with Alice - KDC secret key.

K_B : " " Bob - KDC " ".

K_{AB} : session key b/w Alice and Bob

KDC: key distribution centre.



The KDC recieves a message from Alice which is identities of Bob, Alice in above diagram and generates a ticket. The ticket now contains the message and a copy of session key which is encrypted using Bob's secret key K_B, the ticket with a copy of session key is sent to Alice encrypted with Alice secret key K_A. Now, Alice forward the ticket for Bob to him. Note, According to question the message, session key copy & the ticket are encrypted using session key K_{AB} which is normally encrypted using Bob's secret key K_B. As a result the ticket Bob will recieve will be of no use to him because he doesn't have the session key K_{AB} with him yet so ~~he~~ won't be able to decrypt the text.

If bob was some how provided with session key b/w him and Alice K_{AB}, he can decrypt the ticket and the communication can continue.

In condition, Bob don't have session key K_{AB} with him and he wont be able to decrypt the ticket.