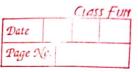
070/2K16/MC/13



01)	Alice & Bob use El- aana Schene with
	wommon prime q = 157 and a point how not
-	N = 5
a)	Bos hus public ky 78 = 10 (Alia chooses sondom in teger te = 3, what is viphotor of
_	sandom in teger te=3 what is viphotor of
	m=9?
_	
-	K = YR mod q
	B 77000 = 1
-	$Y_{B} = 10$ $k = 3$ $q = 157$
-	B
	k= 103 2mol 157 = 58
	g = 10 mg W 3 7 = 30
	In the second
	he know,
	(- 1 K 1 n = 53 2 d 157
.~	(1= xk mod 9 = 53 mod 157 = 125 mod 157
	= (25 httl (3)
.~	2 (25
.~	(= 1 Ma 1 = (ER =) 2 1 (FZ
	(2 = K. M modg = (58.9) mod 157
	$C_2 = 5\sqrt{5}$
	100 6-57 5
	Cipher text for M=9 (=57 51
1	

DTU/2K16/MC/13

Class FUN

Date

Page No.

b)	Alles thooses now value K so M = 9 is C
	= (25, (2) What is lin leger (2?
	but a discount 1 - of the
	King disult hanthan, he de
	K=1 dosh't work k=2 woons
	10 25 mil 157 = 52 mod 187 = 4 = 25
	150 (57 5 111000000)
	: K=2
	Given M=9
	(2 = KM 2000 g K = YB 2000 g = 10 2 200 157
	B 2
	= 100
	(= (100.4) mod 157
	= 900 mod 157
	2 115
	$\left(-\frac{1}{2} \right)$
	4 - 4

(02)	Effictic Ourse over Real Numbers
	Flliptic aure over Ren Numbers
	Find Pta and 2p?
	P= (10) Q= (1-5,1.5)
	Form the addition formula
1	S = 1p - ya
	× p · × a
	0-1.5 - 3
	1-1.5
	xp = 52-xp-x0=9-1-1.5
	= 6.5
	YR = -Yp + 5 (Yp- xe)
	= 0.3 (1-6.5)
	= -16.5
	P+Q = (6:5, -16.5)
	Non, por the dacting formula:
	S= (3xp2+a)/2yp
	3+(1)+(-17)/2(6)
	This is not defined.

DT0/2K16/MC/13

Date CLASS FUH
Page No.

	Tage No.
037	primitive not a = 5
ay	428 R = ?
	8 = 5 * mod 23
	h858 = x mod 23
	T= + x mon 33 = 10858
Î-	The solution to this equation is X=2 X=6
	5° 200d 23 = 15625 20d 23
	Now, Kz = K = (YA) > mod g
	56 gand 23 = 86 mod 23 = 13
	Henry 1 = 13
	To show S is primitive most:-
	P(23) = 22 (23 & prime)
	For a to be a primitive most, we just

	DTU ZKE l'b ME 13 Page No.
	ned to that a \$ 1 mod 23
	$5^{\circ\circ} = (5^{2})^{5} \cdot 5 = 2^{5} \cdot 5 = 7 \cdot 5 = -1 \text{ mod } 23$
	5 ² = 2 mod 23
-	So, S is a pointive most module 23.
· · · · · · · · · · · · · · · · · · ·	
-	
- 18. p 1	

DTO/ZKIO/MC/13 Page No. 6472 and 34,5 (20) ex mentiation 1216 11101 881 3346 3096 So, 6427 mod 3415 = 3346