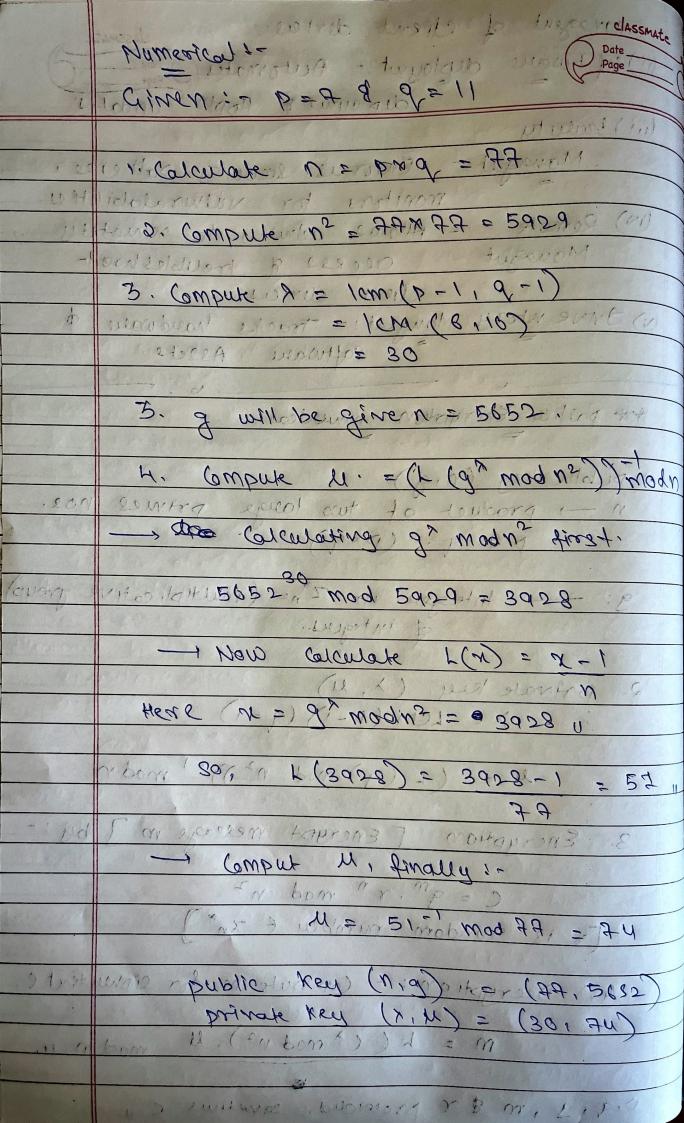
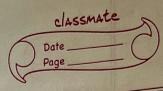
His borner ENCERBHON - warmencore 1. public key (n,g) - 11 sturing + n - 2 product of two longs primes nos. 3: Inteden in Ins (worthlicotine duchb) \$ integral. 2. Prémake kry. (), u) 1. 8 C () E = LCM/(p-1) (q-1) S (5) - ME (T (dy wag No D) - 1 mag N 3. Encryption [Encrypt message in] by:-C= 3m, 2 u mag Nz [x 12 reardom number & xn*] 4. Desryption: - Compute m for ciphentent C. m = L(c' mod n2). U mod n. 11. Did of was brought sometimes C.M.





	Page
-	Example 2 1 2002
5	Encryption: - mayof given message
	1 = 03 [diven] — Lendon wampon.
	, = as (diven) - vanopour
-	computer cipurtent.
	a life and a brancha !
break	- C= gm, on mad n2 [leasin]
1	The state of the s
to Lay	- 1 9 m mad n² = 565242 mod 5929
-	= 413A.
-	
-	- Computer runad no
	E89 2 1400 2454
	2399 mod 5929 = 4852
	11250 mad 5929
	-1 Compute (= (4137, 4852) mod 5929 = 4624
	2 3/02/
	C = 4624.
	6. ciphentent C= 4624.
	211001:
	7. Decemption:- (r (c, wag u, r), m) magn
	-> compule c'mad n2 -> compule c'mad n2 -> 4852
	-1 compare 462430 mod 5929 = 4852
	1 1122 2 2 2 1
	-1 compute L (425 x) = x-1
	1252 -1 112-11
	77
	m = (42, 74) mod 27 = 42
1	m = (42)
1	Decrypted mossing