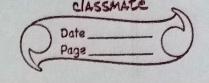
	Date Page
	Assignment 1
01)	Guier Plais Tent: CRYPTO
	separented as [2,17,24,15,19,14] key = SECRET
	represented as 518, 4, 2, 17, 4, 29]
an	Gi-chi+ki) mod 26
	$C_2 = (2+18) \mod 26^{\circ} = 20 = 0$ $C_2 = (17+4) \mod 26 = 21 = V$
	$C_1 = (2+18) \mod 26^{\circ} = 20 = 0$ $C_2 = (17+4) \mod 26 = 21 = V$ $C_3 = (24+2) \mod 26 = 0 = A$ $C_4 = (15+17) \mod 26 = 63 = 26$
	$C_1 = (2+18) \mod 26^{\circ} = 20 = 0$ $C_2 = (17+4) \mod 26 = 21 = V$ $C_3 = (24+2) \mod 26 = 0 = A$ $C_4 = (15+17) \mod 26 = 63 = 26$ $C_5 = (19+4) \mod 26 = 23 = X$
	$C_1 = (2+18) \mod 26^{\circ} = 20 = 0$ $C_2 = (17+4) \mod 26 = 21 = V$ $C_3 = (24+2) \mod 26 = 0 = A$ $C_4 = (15+17) \mod 26 = 63 = 26$ $C_5 = (19+4) \mod 26 = 23 = X$

ans

Q2) Given Cipher Text: XMPWYQ sepresented as [23,72,15,22,24,15] Key = KEY PAD represented as [10,4,24,15,0,3]



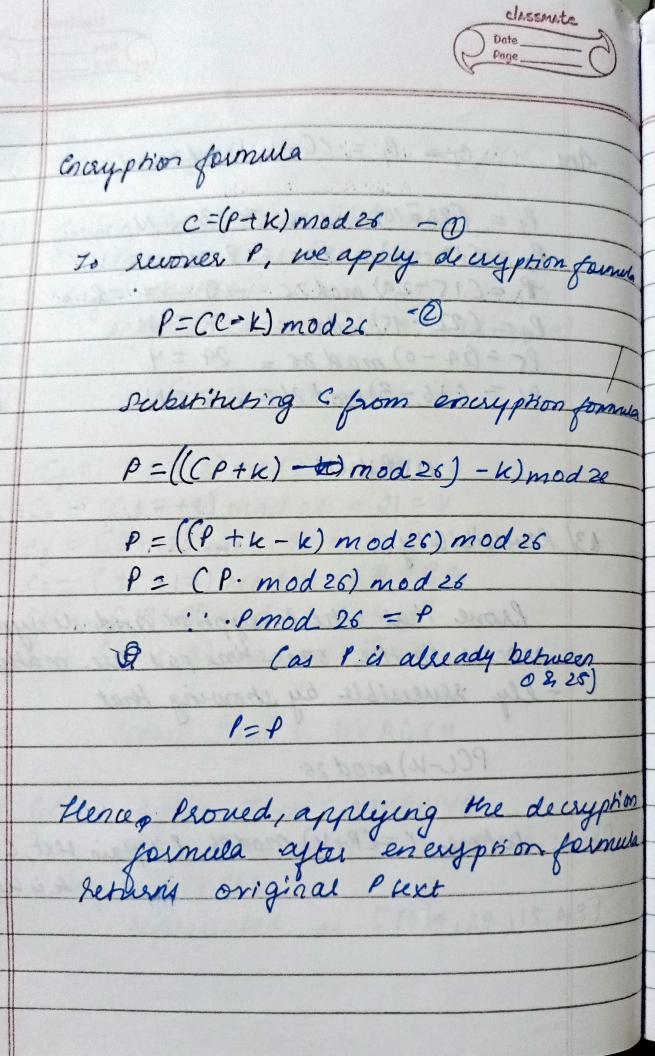
And $C_1 = P_1 = (C_1 - K_1) \mod 26$ $P_2 = (23 - 10) \mod 26 = 13 = N$ $P_3 = (12 - 4) \mod 26 = 8 = 1$ $P_3 = (15 - 24) \mod 26 = -9 = 17 = R$ $P_4 = (22 - 15) \mod 26 = 7 = M$ $P_5 = (24 - 0) \mod 26 = 24 = 9$ $P_6 = (16 - 3) \mod 26 = 13 = N$ NIRMAN

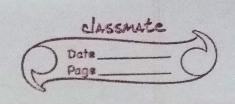
Prove that the encryption and decuption process in the one-time pas-are mathematica

-ely reverible by showing that

PCC-W) mod 26

Where C=CP+K) mod 26, P4 plais Lext, C il Cigher kir Key





of 9f the plaintext has 8 characters and
each character à sepresented as a
number modulo 26, how many possible
unique heys can be generated for
encryption? Provide the result as a
power of 26.

Guies: Pleus Text characters - 8 26 passible values (6-25)

key should be same length as the plainfest = 8 character

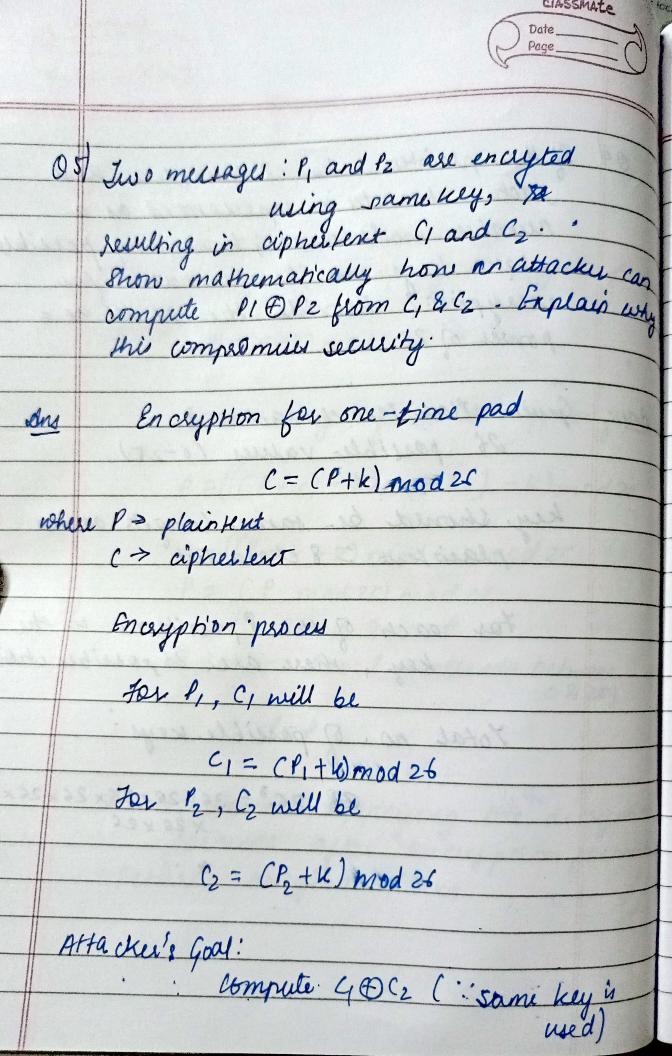
tor each of the 8 possitions is the key, there are 26 possible choice

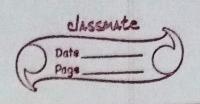
Yotal no. of passible keys:

15 (MA (MA A) =

26° = 26 x 26 x 26 x 26 x 26 x 26

4





C1 € C2 = (CP, + k) mod 26 € ((P2+k) mod 26)

GO C2 = (P1+12) O(2+12) = (P10 P2) mod 26

By XOR operation

 $C_1 \oplus C_2 = P_1 \oplus P_2 \mod 26$

Attacker doesn't need to know the keyk

to calculate P, D P2

24 attacker know some past of P, D P2

they can easily deduce information
about P, & P2

The fact that XORing two cipherkexts

gields the XOR of their corresponding

fundamentally compromises security.

One-time pool are supposed to be

Secure as long as the key is random;

used only once and is kept Secret.

Using same key for too messages allows

on attacker to compute selationship

between them, compromising the

cryptosystem's Confidentiality.