TUT-8

Name: - Souman Somanta Batch - BI 16010420133

Joy enveyption & decryption using following

P=7,9=11,m=3

n=p*9 = 7x11 =77

 $\phi(n) = (p-1)(q-1)$ = (7-1)(11-1) $\phi(n) = 60$

For value of e,

120460

ged (e, p(n) =)

for finding d.

1= edmod of(n)

1=7dmod80

public kuy = Se,n3 = S7,77]
pourate kuy = Sdin] = S43,773

	Date
	The same that the same to be a
-	Here m=3
ī,	Encuption
	J
	C= memodn
	$=3^{-7} \mod 7$
	= 2182 mod 77
	C=3\
	Dewyption
	M= Cd modn
	= 3143 mod 77
	== (312)21. 31 cmod 77= (39)77 4 (39)77
	=(812 mod 77)21 mod 77) (81 mod 77) mod 77
	= [1212 mod 77]21 mad 77) 2ha 201 97
	[] [] [] [] [] [] [] [] [] []
	$= ((372)^{10}37 \mod 77).31.177$
	= $((372)^{10} 37 \mod 7)$ = $((372)^{10} 37 \mod 77)$. 31 mod 77 = $(1(372 \mod 77)^{10} \mod 77)$ (37 mod 77) mod 77)
	31 mod 77
	a gray. W. W. W. W.
	we get doing all the apenations again.
	= (12146 mod 77) 37 mod 27)-31 mod 27)
	= (12146 mod 77) 37 mod 77)-31 mod 77) (67-31 mod 77)·31 mod 7-7
	= [2479 mod 77]. 31 mod 77
	#15B Book
	=15.31 mod 77 = 465 mod 77 M=3

	Page
2	use the vianeur rich
22]	the mula a remain muchod to encode a docada
	to "X YZ 10" (IR AFFE) Wind the anculation
	the musage "GIRAFFE" using the encuyption
	Y-7 - GIRAFFE (Clarates
	Troite - v 21 - March March
	Key - X Y Z
	23 24 25 (Chapmi)
	24 25 milignis
	Encuption.
_	
	Value of PT(Pi) 6 3 17 0 5 5 4
	1 ki 0 1 23 24 25 23 24 25 23
	C1=(Pi+ki)mod26 3 6, 16 23 3 24 1
	T P G & X' D E B
	The state of the s
	39 (TI Ken +60 TI 12 00 (TI Lon + (2)1) =
	Deveyption D 4 B X D E B
-	1 1 1 6 8 17 0 5 5 4
	Di= (10-ki) mod 26 6 8 17 0 5 5 9
	G I I
	The knowles of the low let the bound of the
	The Real Principles of Land By Call Delivery
-	f. +1.1.1



03] use the Affine substitution upher to encode E decode the musoge "UKRAINE" Assume the values a= 9, b= 2, m= 26 Plain Test = UKRAINE Encuption · y = (ax+b) mod m. Plain Test UKRAINE 92 20 10 17 0 g 13 4 92 +2 182 92 155 2 74 119 38 ighter Test A O Z C W P M Encoled msg: AOZLWPM. Devuyption, $p(y) = (o^{-1}(y-b)) \mod 26$ a = 0, b = 2, $a = 0^{-1} = x$ a value should be such that ax mod 26 = 1 92 mod 26=1. 9 x3 mod 26=1. 27 mod 26=1 ... D(Y) = 3(y-b) mod 26 = 3(y-2) mod 26 Cipher Text A O Z C W P M

y 0 14 25 2 22 15 12

3(y-2) 20 36 69 0 60 139 30

DIY) 20 10 17 0 8 13 4

Plain Text V K R A TIN E

acoded message : UKRAINE.