\			Camlin Page Date / /
	Name -> Adibya Vellore		100
	Roll no - Soub.	tool above of root	THE STATE SECTION
	707 001 000	2 6	- inmott
	Sop IO - 105 221000 8	Light to Alto tops	S SI S
			1000
	office Hellman key ench.		
Q1	Dibbie - Hell man try encha bulisch produces dectypt to Cestain numbers.	nge is a method of	6 digitalen cyption
	Inhich produces dectypt	ion thus wing spec	CILIC POMUS
10	to certain numbers.	sen Azt , 11	1. 152
	(a) I his all a Call at Power	hearing mu chimonial	
		THUS IS THAT THE	C10141141
	code should not be	noulled him is the	21101 Br 3 1 .
Ć	Q Framples > Cti Credi	t cond translation m	rails,
15			
Q2>	ay = 14	. 30	2640
	8 = 5 = 400t		
	0 145 1, 5, 18	more and the second	7 7 12
	Public try 05 die	Value Carro	1 K = 17/ st
20	=54 mod14	bob endalile	= 1, 0 boin
		Nop endaule	15 16
	= 1.6 2 1 10 miles = 1	C 1 C 1 C 1 C 1 C 1 C 1 C 1 C 1 C 1 C 1	Volenda
	tod wand of lune to be	Sect Sweet Kay	20 (m. 19)
whole	Sevoit Key obtained bybob	when mulbing	in all they
25	a 2 mod Monda	1 Option JA. a va	1 416/41/19
100 केंगर	n allow enderence wit	a good of the Both.	278 6-0
`(k)~	very rendered to stocked with	Googet tours 'n	that will
and i	Secret hy obtained by	borg runtin A say	less than
	ALRCE - Juston A De Con	de contra les lous de	and state for
30		muller liver liver liver	to war I ?
	=16	U	
	9	A South Control of the Control	
		,	

p.c.		Camlin Page
,		Date / /
021		d
(3)	Encryption formula bor vignere Cipher =	1 10 A
		11.
	The plain tent (And key (w) are added or	الماء ط
5		
	Fic (Pôt ki) mod 26	ho
	mod 26 mg	13,1813 110
49		
	Decouption = 11	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
10	00 = 1 E: -10: 10)	Jin !
i	00 = (Ei - Ki + 26) mod 26.	
&ul	X = Lamboda a b a * b	it is
7	Protoda a billa & b	o 1
15	1 5 mi (x (5,6)) and I mis rid with it is a sign	
13	Output: 30	9
	o wipm 30	V (12
	9. + 2	1 1
Q2)	Steps have being	
100	Steps 60 + Dibbie - Hellman => To implement by enchange =>	Fig.
	Definition of the state of the	
	Vaibban and Nigati are two end was abile communication over a Channel thy know	
	abile communication over a change to	1,
	promote, and her a mutually as you	1 tobe
25	promote, and here mutually agree on por numbers Agand B. Such that Ais a pome nu	alla
a	of Bisa and report Ar A. The and report R	TO CO
11	at When chief to a sile I late = Object	is a number
10	e there A sever ready the come of the	is pands
C	is thank, A, news produces the same result	box crytus
- Su	the block numbers the value of A maybe large	e but the
30 00	hu bo Bison Whally Small.	
PS- R		
1		

Public Key anailable = frg Public Kuys ansilable & P. ty Prognate Ky Sulutud=b Pornote My Schubed = a My generated y = gb mod A Ky gernatid= n-ga mod BA Emborge Os generated kys takes place. they sind = b by recioned = \$ a. Generated Ecust hy

No mod P ferencted Sot Sweet

my = ha = ya modA Vigerese cipher is a method ob energebing alphabetic

fent. It uses a cample boom of polyal phabetic Substition.

Apolyph polyaph Apolyphr poly ath

Apolyphrabetic Substitution Cipher is any Cipher bound

On Substition, using multiple Substitution alphabets.

The encyption Other original tent is done by using the

Vignesso square or vigners table.

The Last in the old alphabet with itten out 26 times The table consists of the alphabets wit itten out 26 times In dibberent toing, each other or of phobers Shibted Cyclically to the lift compared to the premious approbat, points inthe energiption process, the cipher uses a

	alphabet brom one bothe bows, The alphabet used at
	Each point depends on repeating keymond.
	Cach point depends on repeating keyword.
	Input: Plaintent: gents for guts
	did ded a key word i mandax it dads all days of
	Out put Cipherant: ycyczem L LFIM
	for generation key, the given kymord is repealed ma
	Citular manner until it matches the length Ostruplath
1	bent and a si
	key word "Mendas" generates the key" Manday RGLE"
	· ·
Qyl	Encryption rode for vignoe cipher
15	0''
الذر	Strong = " yelks forfecks"
in the second	Strong = " yelks for yelks" Heyword = "SHARAN"
	deb generate key (String, Ky):
/3	deb generate key (String, Key)! Key = list (key)
	if lent string) == len (my):
Mary Care	toturn (key)
	else: else: management individual pody
4	
25.20	tori in senge (len (strong) -len (huy)).
2	ky oppend (ky [i is len (key)])
	retran (" · join (My))
	det energht - cipher Tent (String, Key):
3.3.c.	Ciphe tent = C]
	fori in range (len (string))!
1	x= (1 ord (strong (2]) tord (key [3])=26)
Un the	de la cord (A)
V _	Ciphatint: oppend (chi (m))

				100				1 45%				1
		Ciphentent: XLEBSSYY VEXK	hyword 'Shatan	Original musicia Gula Forgales	Prist ("Copher Eend". Tipher - tent)	Ciphen: fent = encrypt cophertent (string, luy)	Print (Keyword: ", Kymord)	Post ("Osland Muscae" Storna)	0 0 0	Ky = 90 resche Ky (String, Kymord)	Jedus (" . john (john + mt))	