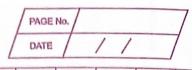
		PAGE No.
.va	> Sampukta bus radonus anigo sig	
	-> SOIS redund is si protormap and	817.
-	Balana Dora auxino m balla	010-0
81	8 1622 WAN BY LENG BARANGS IN COUNCY	Ration
-	1+ 15 exponential ken-exchange is	111.00
	The state of the s	MOLLOW Alless h.
	transmitted making it mathematical	14 overwhelmine
	N. C.	
	It is used to exchange the secre Sender and recieves	et rey between
	Tibors	
	eg > card transaction	
	eg > ĉard transaction belorer	len gen
0.		
- Wa	Q2) Robom de = N 9bom a) = JC
8	83) Encryption	
,	E; = (P; + k;) mod 26 yours	9
	Recryption L= box	redes
	Di = (Ei - ki + 26) mod 26	
0	ou) x = lambda a, b: a*b	
0	$\frac{\partial u}{\partial x} = \frac{ ambdaa,b:a*b }{ a }$	gener
	Apom = = D Apom p	J = n.J
6	(6) Eq - let Alice and Bob be two	end users
	unole numbers p.q.	»osinive
	whole numbers p.q.	



of P The generalisty is a number mout, when raised to positive whole-number powers less man p, never produces pro same? result for any too such whole numbers raised to specific powers to produce decryphor us renAuces that sherogenes Bobod ent no unpublic likeysmannon ti pripublic bellimenort ' Iceys = P, G = P, G It is used to exchange the secretical p Private key Private lay reened rey generated key generated ol = 6 modP y = Gb mod P Exchange recieved = 4 generated d* p: d o generated x ta = yamod P

PAGE No.		7
DATE	11	

B)	vignère ciphen is a meahod of encrypting
	alphabetic text. It uses simple polyalphaboxic
	substitution. The encryption is done using vignere
1.	(table: bro + (tippains bro)) = x

eg > stext > med HELLOTHERE

Encryption

Encryption

The plaintext (p) and lay (k) are added modulo 26

E; = (P; Tti) mod 26

Decryption

Di = (F; -k; +26) mod 26. Jugue

string = "HELLOTHERE" 134 . long key = "SAM"

det generale key (string key):

key = list (key)

if len(string) == len(key):

· rehinn (key)

elle.

for i in range (sming) - len(key):

key. append (key[i]. len(key))

rehvin ("".join(key))

	PAGE No.
L	
	def encrypt ciphenText (string key) - on on (8
	alphabetic text. It us (s) sintxot audinabetic
LD	pir pri forsio in range (len (string)) prividedus
	x = ((ord(shing(i)) + ord(ker(i)))).26/+
-	ord('#)
+	return ("" ioin (cipnor_text))
	return (""Join ((ipros)_1ext))
	randody, sum, denotates sums ums um sum
	key = generate key (string keyword)
	Encryphon ,
	print ("Original:" string)
	print (" kowywad:" layword) Txx riving wit
	ciphon text = encrypt - cipen Text (string, key)
	print ("Cipher text: cipher text)
	Decruption
	Di = (E; -k; +26) mod 26; tuqtuo
	ourput;
	original: HELLOTHEREOUTH = prime (8
	regnard: SAM "MAZ!" = prints (8)
	Ciphertext: ZEXDDFZEDW
	det gareraletey (shing low):
	(may = list (lay)
	if len(sming) == len(lay):
	(mex) current.
	ولياء ،
ارد	for in range (lentsming) -lent
	return ("" , win () a)
	(hollant. 1111an
_	