		CNC A	a Paris de la
		(//\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	selgnment 1
		00000111	
		MPKI, lalwani	D15B/37
	91)	Explain the difference	between substitution cipher
		and transposition eigher.	
	~ .	110	
		Substitution Cipher	Transposition Cipher
	_		,
	(1	In substitution apher,	In transposition cipher, plain
0		ploun text w substituted	text characters are regranged
		with numbers, apphabelses and	with respect to position.
	-	symbols.	
		J	4 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	2)	Two types: monoalphabetic	Two types! keyed transposition
		eubstitution apper and	Two types! keyed transposition
		polyalphabetic substitution	Epher.
		apper.	
	-	T .	
	요)	Character's identity is	Characters position is
		changed but position is	changed but identity remains
		same.	same.
			most in the second of the
	4)	ean detect plaintext.	
		can detect plaintext.	can disclose plaintext.
	5)	Centr upper is	Rail Jence cipher is
		substitution cipher	transposition apper.
		1	
6.			
Sunda	ram)	FOR EDU	UCATIONAL USE

	to the second of	1 4		-				
Q2)	Explain the difference cryptography.	90	stego	nogr	raphy	and		
	Cryprography.							
7 y 1 - 2	Steg an ography	1 4 de 1 de 1	Conjpto	graph	Ϋ́.			
	. 1100						1 .	
7	Information is hidden	Injo	rmation	n us	brand	ommeo	Lin	
-	Information is hidden in steganography.		rmation					
721 2	Medden information is	Tran	sjorned ble.	d int	ormal	700 -	is_	
to be to be	not visible.	V) 81	ble.	1.83	rili	>)
	rings at finisher with a torus	3011.1	CATAL S	11.1 11.11	**/	*34		-
3)	Provides confidentiality	Prov	ides o	office	lon tic	elity	,	
	Provides confidentiality only.	9.ntec	sty.	000-	repud	Patro	<u>n.</u>	
		+ 1	1 1 1		1 1 1			
4)	No speuffe algorithm.	Var	lous r	engr	ired	and	us) * postPos	pro-
		appri	ved al	gont	b'm.	2 7		-
я					- 7*-Y-4			
				1	1			2 = 6
03)	Deupher the following any	pher	text	eina	bout	ė :		
The course	porce -attack!- " un m 700Ei	00 RW	to be the	1. 4	1271111	- V		
: -X	V interv				P. 1. 1. 2.7		7	
	Algorithm - Rail Fence							
		<u>v = _1</u>	and the	400	17/1	23.7		
i die	key = 2.	1	i com	£ 1,900		() () () () () () () () () ()		1 V
		Г		7/4				
	CIMIT		M		7	R	0	
	0 5	0		0	11.			Q.
	10 11 20-17							
	plain text - come rome	1120	h					Tags
(Sundaram)	FOR E	DUCATIO	NAL USE					

Q 4)	Encrypt the following using playfair cipher using the keyword-"MONARCHY"-"SMARAT IS MY BIRTH RIGHT". Use x for blank space.
f" (N	BIRTH RIGHT" Dice X tox blook come.
6 7 5	
7-1	Key-MONARCHY
	Plaintext-SWARAJ IS MY BIRTH RIGHT.
	- 1. Planes - corte for force
	matrix- male in this
	W
	mon AR
	CHYBD
	E F & II K
	L P Q S T
that I are all the	UVWXZ
	SW AR AJ XI SM YX BI RT HX RIGHTX
	OX RM BS AS LA BW IS DZ BV AK PY SZ
	the state of the s
	Cipher text - OXRMBS ASLABHISOZBVAKF YSZ.
(5)	Apply caeser apper 1c=5 deand decrypt the given
	Apply Coeser apper k=5 deand decrypt the given sprer text- "YMJTYMJWXNIJTKXNQJCHT".
- 4	for encryption -
	5
	C = (P + K) 1/. 26
	for decryption-
)'
	D= (P-K).1.26
(Sundaram)	FOR EDUCATIONAL USE

138 1 PA	in the fact of the manual of the language of the
The Value of	7 M J T 7 M J M X N I J 7 K X N P J 'S H J 24 12 9 19 24 12 9 22 23 13 8 9 19 10 23 13 16 9 18 7 9
; -	19 7 4 14 19 7 4 17 18 8 3 4 14 5 18 8 11 4 13 2 4
	THEOTHERSIDE OF SILEON CE
	THE PROPERTY MAY STEET AND STREET
	Plaintext after decryption- "The other side of silence."
φ6)	Apply vigenere cipher encrypt "explanation" vsing very "leg"!
i i i	key-leg
	plaintext - explanation.
ACCE BY	
er at	legleglegle
MI SA	explanation
	+ 19 9 0 4 7 11 15 2 3 9 Ht; a e hilpcdj
	I'M I'L J J A TEAN A RIP IC A J
	ipher text - htjarhlpedj
	A MARIE TO THE STATE OF THE PARTY OF THE PAR
* 1	
Sundaram	FOR EDUCATIONAL USE

(47)	Compare symmetric and	asymmetric cryptography.
	Symmetric	Asymmetric.
1)	Same key for enemption & decryption.	Desing a pair of key! public key, private key por encryption & decryption.
2)	Simple as only one key is	More complex as two keys
3	Paster execution speed.	comparatively slower:
head y	AES, DES are common	RSA : Diffie-Hellman ave common algorithm.
	algorithm.	common algorithm.
. 7.3	Article (Artist Control of	· . ale s'a land of the file
89	Explain AES along with) AES stands for Advan	h its major entimbutes.
@ Ans	i) AES stands for Advan	ced Encryption Standard.
îi) DES was replaced by	AES.
111	It is symmetrie key	based algorithm.
iv	Morks as a block up	ne m
	and the second s	. 1 . 1 . 1
v)	# uses 128-bit kee	•
vi)	It can work with	128, 192 & 256 bit key
(Sundaram)	FOR EDU	UCATIONAL USE

			de sono ben size
VII	No of 2	ounds of operation as	penas upon seg
	No of sounds of operation depends upon key size 128 hit key 10 sounds 192 bit key 12 sounds 194 sounds.		
	192 bit.	ey 12 monds	1 1 V 1 1 - 1
	756 DIT	eq.	1 - nt . 3 - 0 1 2
1111	75 (111)	considered highly seen and is used in ind	ne due its long
vil	AES is	considered highly sea	natori today.
	. key sizes	and well in ma	Dering teasing
			das of operation:
<u>ea</u>)	Explain di	Herent block cipher mo	aco 1, /
		Dagaston	Application.
	mode	Fach block of plaintext bits is encoded	Sewre transmission
	Herronic Con	hit is encoded	of single value
	Com BOOKICOS)	independently using they	1. 0 4 4
	Parallicon In	KOO! : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	. miltereptt 10 11 11 11
2	Cloner Block	The fringet to encryption	Authentication.
	chaining (CE)	algorithm is MOR of	
THE KOR	u	the next block of	Gieneral purpose
	*	plaintext and preeding	block mented
		The fringet to encryption algorithm is MOR of the next block of plaintext and preceding block of aphertext.	transmission.
			Authentication
3)		Input is processed &	· ·
	(CFB)	Ophertext is used as	General purpose
		input to the encryption	stream - omented
		algorithm to produce	trensmission.
a Programme		pseudorandom output	
		which is xored	
		with plaintext to popular	
Sundaram		FOR EDUCATIONAL USE	

	a sofesion for all	next unit of ciphertert.	- xouth in Eg L
1			
4	Output Feedback	Similar to IFB except	Stream-onented
	(OFB)	that the input to the	transmission
		encryption algorithm is	over vojsh
		the preceding encryption	channels
1, 1, 1,		output and full blocks	leg catellite
	4	are used.	communication)
			17 T.
(5)	Counter (LTR)	Each block of plaintext	General purpose
	3 3 6 7 - 1	is xored with an	General purpose block oriented
i		encoupted counter. The	transmission.
1 2 1		output is incremented	1 2 2 2
143 143 143	A STATE OF THE STA	for each subsequent	Veeful for high
		block.	speed requirement
	1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	a Plan of the Lordonae	Service Services
			A Comment
(010)	Explain roo	thits and its types.	20 6 4 . Try 19 1 1 2 2 2
Ans) Pootkits are	malicious software that	give hackers
	holl access to	your PC.	V
(d 1	I helps had	ress to enunge or etert	
	settings or ti	les the way an adn	ninietrator court
	do.	1 0 1	
c)		derived from two won	
, , , , , , , , , , , , , , , , , , ,		U	
		esents a collection of to	2013.
4	types of mo	a sale or a constant	* * * * * * * * * * * * * * * * * * * *
i)		framware mothst-	4-4
		netalled on your hardur	
e e	can affect. F	FOR EDUCATIONAL USE	.20
Sundaram		. OR EDUCATIONAL USE	

=	
	Mackers can use this to introcept data sunthen
4	on hard drive.
11, 4	went former of the comment of the day of the
11	Boot bader rootkit-
	Bootloader loads computer's os.
;	This rootkit attacks and replaces ligitimate bootlands.
	This means the soothit is active even before the Os.
-8 * 8 7 -11-11-11-11-11-11-11-11-11-11-11-11-11	
	Memory rootkit-
	Hides in RAM or Random Acress Memory.
	carries out harmful activity in background.
1 1 2 5 -	But only line to till the computer is see
HE INC.	rebooted.
, ,	
er variable v	Application 2001/21-
plan Total Ling of Total Trans	Replace standard files with mother tiles.
	Affrects programs such as word, paint etc.
	pon every time a affected program is reminorning.
	Difficult to detect, as affected program son normally
	I The second sec
· v)	Kernel mode rootkits:
ist, her of	Target core of PC's Os.
*	This can give easy access to computer and steal
7 2 3	your information.
14, 1 / 4 · /	
011)	Explain DPos attack.
Ansc	DDOS stands for distributed denial of sorrice.
	The involves sending large amount of traffic to a
	website from multiple sources to presubelm it.
(Sundaram)	FOR FOLIOUTION AND AND AND AND AND AND AND AND AND AN
Quincaram)	FOR EDUCATIONAL USE

SCHOOL OF CHICAGO STRUCK CONTROL OF CONTROL OF CONTROL OF CONTROL OF C	Consideration of the Constitution of the Const
	In this malicious network attack, hackers send
Elminor de la Colomia de Santa de Colomia de	traffic from multiple network connected devices for communication to one website to overwhelm
effective was emining the programme which company and a second	por communication to one website to prerunden
more state home and objects and come and come or a second	it with palse traffle or requests.
1	
5	This helps to type up all resources for request and crash or distort it so normal users cannot acuse it.
	request and crash on distorit it so normal
	veers cannot access of
	that you is a section of the
(d)	This attacks consist of multiple affected
	This attacks consist of multiple affected device called as bots and a group is called
	botnet.
e)	once a botnet is etablished, attacker is able to
	send remote instructions.
	oil i b the and a sold of the
	address causing Dos.
	address capting prof.
	As all bots are legitimate devices separating
9	Them from normal traffic is difficit.
allices de Carde Ballet (Alle Control y Control alle Alle Control and Alle Control and Alle Control and Alle Co	The state of the s
(12)	Explain various measures against social engineers
	Explain various measures against social engineering attacks from individual user perspective and organizat
	perspective.
Anca)	Best defence is to be watchful.
b	As an individual-
Committee of the Control of Contr	Don't open emails from strangers
to the control and the control	pon't provide important into such as cur, date of
	birth to others.
(Sundarum)	FOR EDUCATIONAL USE

ų,	Do not dick on every ernait link you get.
*	
, c	As an organisation-
	Provide training to all employees
	Provide training to all employees Man corporate cybercewsity program for adequate divital recority
o control	digital sewrity.
	stup an internal team for employee's to
1	
A 1 1 4 1	
15 16	te and the tree of the first the factor of the state of t
	The state of the s
1	affect the said of
1 1 6	ensit house out to the said of the said of the said of
	the transfer of the transfer of the contract o
	e himse instead in regard the sign of the
-1, -2, -1	1 - 19 Town to go i how I had many white the
	Control of the second control of the second
	The state of the s
8 24 4 4 4	Constitution with the second of the state of the second
Sundaram	FOR EDUCATIONAL USE
	1