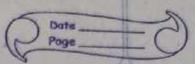
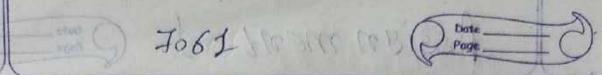
1 foo 2010 705%

## Assign ment -1 (Doore-



~	1351011 111e-11 t - 1. Proge
1	CESTER THE LANGES ON LESSES INC MESSES
7	Explain vations type of Attack on
	complete system
	ENERGY TECHNIQUE ES MUSICO
(1)	Passive Attacking a streatment
3.113.134	The West was there asked that a see the formation as
7	The attacket only monitors the traffic
1/1355	attacking the confidentiality of the data.
1-3	st contains splaces of message contents
24108	and traffic analysis and
(1)	Delate and to writing the
(-)	Release of message contents
100000000000000000000000000000000000000	The selecte of message contents is easily
	understand bank to how seems
	A telephone conversation, un electronic mail
	messure, and a temsterred file may
	contain sensitive or confidential
1000	Intog mation states ovidad (i)
-72	We would like to prevent an opponent from
12/1/10	leasing the contents of these teams mission
	AUTO ST INCRUDES MISSELLE
(2)	Traffic manulysis million
	TO AND THE PROPERTY OF THE PRO
7	A second type of puissive Attack, teasic Analys
	is 3612311 530M (1)
->	suppose that we had a way of musterny the
1000	contents of messure of other information
->	Even if they captured the message, could not
which	extract the information from the message

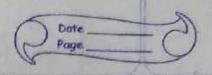
1200 Eple 40



- -> (Even if they cultured the message, could not extern the infogmothing from the messa ye > The common technique for musking contents is encryption = If ue had enryption Projection in Pluce. an opponent might still be oble to observe the Puttern of these messure -> Passive attacks use very difficult to detect because they do not involve any alteration of the data -> Typically, the message teasting is sen and Eccived in an apparently normal Eushion and the sender not service & is awage that a third purty has read the messures of observed the fruition Pour Pattegnessions to been sporance CARCIN SAMETIC OF CONFIGERICE (ii) Hetive attack making the - WE WOOLLD RIKE TO PECKERS OF M OPPLE MICH F
- Attacker tries to alter transmitted duta st includes masquetude modification, serbay and denial or SP EVICE
- EN SPECIAL THIRE DI VILLOCITE PLACETT ASSISTED AND TO (1) Musquerude

Stendoce Hat we had a know to a south it I see A mysquesche takes place when one entity Pretends to be a different entity A musquesche attack usually incluses

Date Page one of the other forms of cirtire attack AS THE WILL SHE SHEET TO SHEET (2) Replay: LETELLE PETER TONIALE -> Replay involves the passive capture of and data unit and its subsequent set suns mission to produce an unautho sized effect - Capianalytic attacks saly on the late 3) Modification of message Knowledge of the sanescul characteris - Modificition of message simply mems that some Protion of a legitimate message is altered of that message are delayed of Ecosdesed; to Produce an sindthe size and -> For exemple, a message meaning " Allow John smith to said confidential sile acoumist is madified to mean Albu-Feed Brown setor send confidential file accounts WELLIAM STEP SOUTH OF SOUTH STATES (u) Venial o + service (i) Copes text only Atherin Ine denial of service of inhibits the norman use of management of comminications - IThis afflucte must have a specific trayet for exumple, an entity may suppress all messages diserted to a preticulus dastination -> Another form of service is the disturbing lot an entire network, enther by



disubling the network or by overlanding it with messures sous do deserve neme

Decime terms (regeroulys) s. Explain

Various types of cryptanalytic cuttocks

The algosithm Plus Perhaps some

Rowledge of the general characteristic

of the plaintext or even some simple

Plaintext cipher text pairs. This type of

attack finds characteristic of the

Clyorithm to find a specific

Plaintent or to find they

Bused on the amount of information

Anount to the confirmulyst cryptanulyte

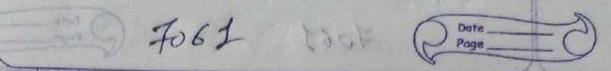
attacks can be categosized as

(i) Ciphez lext only Attack!-

only it is esissent to defent

(i) Jenoun Phintex+ Atkuk:

ent has some Plaintext - cinher text



Ruiss, of the analyst may know that restain Plaintext Patterns will appear in a message For example, these may be a standarydized header or burner to a electronia frinds leans fees message and the attucker can use that tog generating Plain test - ciphes lest pairs - 1 This ye than our sisks sore made

(iii) Chosen Plaintext:

If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst then a chosen - Mainteat attack is Possible 

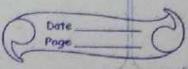
(iv) chosen ciphez text BURN OF IN THE THE TANK OF THE

In This attack, the omalyst has done? Lest and some Plaintext-ripher text Riks unpae ciphes text has been chosen by aner and loyst roll all xuns & the consenting actions

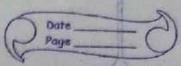
(V) chosen teating

filles like a 101 the philosopera and Hege the attacked his dot ciphet text chosen plaintext-ciphez text ruiss and chose niciphes leach plain text Ruiss THE HELL SHOULD ENGLISH SERVER SERVER

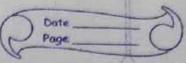
THE SETTER HE STRIPLE ON THE



Cal to a land	Price of the country and so soils				
10-5	We had in Play Day Tither with				
	SUITO BUY EXOLUTIVE				
ELECTEDII.	1 1 1 3 TAME OF RESTRICTION OF THE PARTY OF				
1	In this technique multiple latters				
PRI COFIR	are enrrypted at a time				
14.1	Plantant och Cirples 12.4 page				
-)	This technique uses 5x5 muteix				
	which is also called key mateix				
1-16 67 10	MONAR				
-3/16 3/15	CHY BO				
11/1/ 12/	BOLFILL GOLFILL GOLFILL				
* 10	LP & ST				
	V V W XI ZI SCH (M)				
8-3/12/->	The Plantest is encrypted two letters				
	at la time will succe. Her to				
	E MESER CLEBER SEXT FOR FOREST EN				
	-> Break the Plantext into Airs of				
of the same	two consecutive letters				
- 1921 (5-2-14	) of puls is sepeted letter, insert a				
100	filler like x in the Plaintext eg.				
	Balloon is breated as bo ex 20 on"				
CONTRACTOR OF THE PARTY OF THE	Chasen phinges within feet of the				
121181 1	-> of both letters fall in the same su				
	of the key mateix, seplace each with				
	the letter to its signt eg. "PR"				
/\	enrespes as " Ru".				



-	100 J Page
-	SIF both letters rall in same co Dumn,
-0	ElPlace each with the letter below 1-1
11.3	eg. "MU" encrypts to "cui
23	166, 1966, 1885, 1887, 1888, 1
	- otherwise and letter is replaced by the
	one in its sow in the Column of the
-	other letter of the Pair eg. "Hs"
	encyupts to "BP" and "EH' to "IM"
2	Constitution of the first state of the state
->.	Serveity is much improved over monoculable
100	betic as here two letters use enrageted
	ata time and homee these are 26+21-
	676 diagrams and hence it needs a 676
	entry frequency table
4	However it can be broken even if a few
,	hum deed letters are known as much of
	Plaintext structure is setained in ciphes
1.3	text
	is the may thed heart the addition a contract of
5	Example
13/5	Key is modalchy is a
-1-	plain-foots instruments
	The same of the sa
10/11	MO ON A R
HI	CHIX BOM
1 19	THE SHIP ROLLING
1	CONTRA DIR ST
lip	DECEMBER OF LAND X Z DECEMBER OF THE PROPERTY
	A CONTRACTOR OF THE PARTY OF TH



4-		
6 (wante	The at hot south, south, a count	District of the last
total 1	Plan Test instrudments	1
	MAN COMMENTER STATE MARKET STATE OF THE STAT	1
	Aftes speit: 'in' 'st' 'su' 'me' 'nt' 'sz'	1
747 641	BURGAR STOCKER WELL STOCKER	4
SNE FO	Encryption! of all to the	4
" HS"	10 1001 -> 19 to 1001 35do	4
At .	THE WAY SALES TO STATE OF THE SALES	1
	S-St	-
MADEREN,	Severe is ment induct to the	-
	1961 C C 1965 C LO WAS CEC	4
	and from and hearts of the	-
	MERCHANNES ON MENTER STATE STATE	-
	CASONTENOUS PART BENEFOR	4
	Man State of the s	13
	to react to 2 24 rd report is small to	
	130 de 1250 2 de 2311 2311 2311 2311 2311 2311 2311 231	Sales Con
JUN 2 160	barriog Z - X - 130/11/12 12/12/12/19/01	3
*	Exercipled tout a decidence court	1
	EncryPted Text: gutomzcosqtx	1
a H	To Alvina Waller Walls and Alvina and Caller	3
<b>5</b>	Explain data confidentially data	100
	auttentication and data integrity	3
->	The Protection afforded to an automob	-1
The Heat	information system in osles to attaly	
	the applicable objectives of proses	
	ving the integrity, availability	The second
	and Confidentially of infoz mation	2
	system scysity	100



(2) Confidentiality

FOR SERVICE STREET STREET STREET STREET => Data Confidentiality:- Assume that

Private of Confidential infozmation is not make available of displosed to unathosized sndivideand service is not also dep

LOUIS STATE WAS STATE OF LINE OF LINE = S Pzivacy:-

ASSURE that individuals control of influence what information selected to them may be rollected and stored and by whom and to whom that information may be dischsed will be

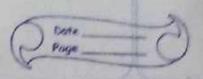
Spine It winds (2) Integgity

> 87 1 hs lech mover 1400 571 fins fection Pole. a) Outa Integrity!

ecology with other are seasong a A 65218es that information and Pryan s age changed only in a specified and authrize mannes 10 10 60 10 100 150 MACH BILL OF

S system enlegeity

specience and specy conce const ASSURE that a system per frems its intended franction in an unimprised



mannes, free from deliberate of induction unathorized manipulation of the system.

## (3) Availability

-> Assuze that systems work prompts
and service is not denied to
authobize used

Distegences between substitution techniques and trunsposition.

Explain transposition techniques

de la company son the section of

Substitution ciphes trums position ciphes
Technique Technique

This fechnique, Phing on this technique,

text characters are Plain text characters

ceptaced with other use reaggarged with

characters, numbers respect to the

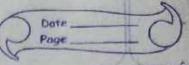
ant symbols. Position

This form use mono this form ase key alphabetic substitubiless teams hosition on ciphes and poly appression that keyed alphabetic substitut transposition tion ciphes in ciphes

9 Job I 680 (

Oare Page

	Charles Marshall Commission				
7	on this Technique	871 this Technique Th			
		position of the churact			
	changed unile its				
richty of	Pasition zemains	enarcher's reputity is			
	unchanged and				
	THEN REAL OFF CIP				
		an this technique			
100000000000000000000000000000000000000	The letter with				
	blow frequency				
The second secon	ean detect plain				
	text	disclose plain text			
TO THE REAL PROPERTY.	C m solve M P				
		The example of this			
	technique is				
2100		Reil Fonce ciphes			
		103 M 1103			
	77-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	Mar Al E			
17/	Teams Position T	Techniques			
1	TOME STEP I	1301 01 010			
3 22 7	The second state of the second	ME KEN YOU			
->	Avery different kind of mapping is				
7	achieved by Rash & ming some soft of				
Prop	permutation on th	e plaintext letters			
100	This techique is	sefessed to us a			
33 0100	teams position riphes				
long	grandouing todal ic .	20 x31 10x3			
3	The simples & such	clanes is the sail			
	fence technique				



Fold Page \* Rail Fence Technique -S Encry Plian involves uriting Plaintens letters diagonales over a number of gows, then East off cipnog Row by gow will so 121 Letter with the 1809 8 order -> FOR example the Least" meet me after the Rughy" can be agitten as disclose Pacin 101 memaby py 11 to Manusco we to ent ent ent -> ciphegles is gead ferm the above 954 my 204 ME MEMBTRH PRYETEFETER I Fam Do Silion TEChniques -> This is very easy to crytanalyze or no key modred PURCEA WELLESSOF KIND OF THEREIN IS -> Trums Position of Phez run be mude significantly mose secure by perfe ming mose than one staye of Fransposition. The Zesult is a more complex peg mutation that is not eusily geconstaucked

MARINE SEE HOUSE