Mame	: chhagan kumawat
Ration	: chhagan kumaucd 0: 20230201067.
,	
	Hssignment No.2, DATE / /
01	What are the classic priciples of cryptography?
The state of the s	How does cryptography contribute to hiw securit
-	brighter of coursemphy:
11	What are the clousic priciples of cryptography? How does cryptography contribute to hiw seaing briciples of cryptography?  Confidenticulty—  Ensures that information is only accessible to
10 - 21 - 1	C C C C C C C C C C C C C C C C C C C
	Ensures that intermettern is only accessible to
	those who are authorized to access it.
adr bod	lengthing police of the end of the course
	Integritying data and habitations had be
)	Ensures that the informatication has not been
	altera l'est de de l'illian de l'est de
	storage.
1/	Storage. 22 pm to A low to action to action to the
	Techniques such as conflooprathic hoch fun
	ensure the interpretay of data by generaling a
	fixed-size string that uniquely represent the
	fixed-size string that uniquely represents the original data.
1 2 36	Tophopida checking in chamber . One M
	Huthentication: home my locario la fini
	Verifier the identify of the individual or systems
	Involved in communication.
-	Cryptography method such as digital signature and certificate authenticate were and devices conforme
L. Cinca	certificate authenticate were and device conforme
	their identity.
	Treat (acriting)
11 + 412	
and My	Mosi-Reputations
-214/11	Ensure that once a party sends a mersage, the
hor in	Cunnot deney having sout it. Digital Signatures
<u> </u>	provide proof that a specific individual sent a pag.
	this merentines do not produced in the
haralta lara	this preventing donal of porticipation in a transaction.
- CM A JAG.	a to the shoot of the runn on a many little
S)	trajablity: - & withcosts were nowed in will
2400	Information & resource when needed. Which primary
201/00	Information & resource when needed. While primare

	PAGE NO.  DATE  DATE			PAGE NO CATE
3, 6	a contem in broader nlw security.		Ocenption:	-10/2 del (selection
- Fada	Contem in Checase Man 1000 Los		The revenue moies	of primation where II.
100	Children Constanting to Min Ceccinty 1-		aichentext is emvented	of energytion, where the back into planlext using
	The community of the consider the color		a decryption algorithm	La Ven
	Contribute of Cryptocraphy to N/w. Seccenty:-  It place a conciol role is a seccusity n/w/s by address  various subnerabilities & consuming secure communication.		On any the size of a control	at the connect less and
-h. 7/4/2	vanow vomerabilities & containing server communities to		discould be hard	ith the correct key can an I dices the original dat
	Securing Ruta Promspyssion:	1÷ .	arcage the information	on Taries The original son
	Encaption protocols like SSZ/TLS enrure that the classe transmitted over nlws remails contidential. I secure from exerchapping by affectes.	1100	ailed to minary min	The state of the s
	clara transmitted over nive remains contratential.	CIL	Vittemente.	Haymmetric Crypteopophy
- X XY	secure from excremologing by affected.	Chitema	Symmetric Carptopaphy	Haymmetric Crypterpophy
The state of the s			MICONDAN SU DATE AU	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
- <del>2</del> y	Authentication of vier & denices!	VKey	Sirgle, Sheined key for	Tun key publish key for enry
	Construration of one of southenticate the entier		both encryptions decryption	-on parate key for diryon
D 831	Communicating in a niw.		0 1	63
2.20		2) Spreed	Faster	Slower
3)_	botecting Agellist lata lempering.	,	. h va r in	Consider Control
~	brotecting Ageilinst Pata Tempering  Interprity checking mechanism like MAC's a  digital signatures prevent unauthorized modification of data.	3) Security	Key clistabetton is a challe	Lasiar Key distribution.
	digital signatures prevent unauthoused modification	1		
200	de distance alle por un suchi unde partico	4) Vse	Used to encrypting lang	e Used for secure they exchange a authentication
-	- Committed man of barrey	Case	amounds cridata	exchange a authentication
- hiny)	Enconed Decrise Mitel			
1000	PKI emobile secure acress control by managing	5) Encry	block or Stream Cipher	problem like factoring
-	digital certificates.	ptien	the supporting of	problem like tactoring
-		1 (Me		clarge immer or ellipter
02	What is Enzyption & Decryption. Distuis He dist. Deta			curves.
- politic 9 1	Symmetrics of asymmetrics compriography algorithms.			Shally without the
71/11	Entit the cull types of symmetric Cryptocyraphy and		DOLLYCOM CONCUE	(a) (b) (b) (c) (c)
- 40 M	explain any one	(-)	Type of Symmetric Cry	ptocpaply Algorithm -
1100) 15	What is Entruption 4 Decryption. Discuss the diff. beta symmetrics asymmetrics comptography abjointhms. Entit the cull types of symmetric cryptography and resplain any one.	-0	LLOCK (Phers:	
	uing an encryption algorithm & a key:		Encrypt date in	ixed size, blocks if
	ung an encryption algorithm & a key!			Merchanis francis (
- Th 573	Energetian ensures that only authorized were who			and the many + Kenty to from the fee
ACCREC	have the key can read the energeted information.			Coplered of the contraction

PAGE No. DATE / /		PAGE NO / CLATE / /
2) Stream aghers:	2)	Block Cipher principle:
Execupt data one lost of bate at a 11 me	ر - ادون	Place cipter poiciples and fundamental to under
ex. Scalce 20 1 201 on 1	ola d	Standing how block ciplers work in Cryptography
ex in Ray: Scalce 20 in months of the control of		They are excential for cocurity digital communication
CO3 Shoot notes :		and date.
Stragonorachy:		- 120 minutes 1 102 -
- Stepanography is the practice of maling secont		key priciples of block cipher:
intornation within non-secret data. In such a		Gual Clark Cine 's
Info: within the existence.		Delock liphens work by dividing plaintent into
- Stegunsomaphy is the paractice of concealing measure		Fred = sized me blocks
message or Info. within other mon-secret text or		Common blocks size Include 64. bit.
data to prevent detection		-5 with the 12 (4
	(2)	Roger ould which who had at 278
D (arriar medoum:		The same key is weed for both oneryption !
D Carrier medoum:		decryption.
The file or media when the holden meg' is embaled		Class Carlot Grant
	May) c	Substritution Perinahation NW (SPM):
2) Payload: - du la beirg conceded:		Most block cithers, like AES, user an SPN
The actual mig or duta heirg concealed.		structure where the encryption irrolves rounds
2) (2) (1)		of subfidution b permulation.
3) Stear file :- 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	<b>Y</b> )	Parada's
The output Pile after embedding the payload into		Rounds:- It wes pulliple round of fratimission to achieve
the Corner medium.	- 10 -	Confusion & diffusion, essential for security.
y) forcoding method:		CONFESTION & STREET, ONSEMBLE SECTION OF SEC
DIST sociation By Tourney downing		Forular Block Cither Algorithms:
1) Meta hiding.	,	Onto Emplica (DEC)
-: 200 1710 200 TA De-	2)	Triel DE3
5) Application in a level windship and in	2	Data Encryption (DFC)  (Diple DE3  Advanced Encryption Standard: 1016000111.
D'Convert Communication . 10.	+	Jan
2) Digital Worldemarking		
3) Cybersecurity.		
J. J. S.		

	PAGE No / DATE / /		PAGE No / DATE / /
3)	Rata Encryption standard (DES) 1500 Green Che Data Encryption Glandard 15 9 Symetric-Key bolock cipter that was wistely wed for data encryption in the late rate on contuny.	1	International Data Encryption Algorithm. (IDEA) The International Data Encryption Algorithm or a Symmetric-leasy block cites that was decigned to provide strong energytical Improved Security over older algorithm William DES.
<u> </u>	Key Size  Key Size  Rounds:  DES penformains 16 round of emeryption.	()	Dikey features:  Block size:  It operates on Gu-bit blocks of Dala.
	Ferdal structur: -  DES is based on the Feistal him a Etructure that absides the data black into two halves.  S-Boxer:-		Key-Size: -  It used a 128-bit key for encryption bedic.  Structum: -  It is based on a felstel-like Structure.
MT	DES is relies on s-boxes to instruduce no-lineonity Into the enemption process.  P-Rex.	-	Found: - Found: - Security: -
. 2)	DES Emonytien process:-  inital fermulation have aliche in the second function of the second in the	2) ————————————————————————————————————	Resilience to cryptanalyris  Posute-force hesistance.  Advantages:- O Relative
-	Security Concerns! - : :  Bruste fore vulnerability.  Differential 4 linear Congpton Congresoralysis:	3)	Strong récurity Low mensory Requirement.  Disadvantage: - Application
			Place size 1) Pretty Good privary Patent. 2) Other Cryptographic System.