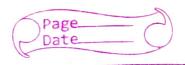


	Manne - Harsh Mishra Subfert - 2001 Roll WO - 20 class - MCA-1
	Assignment -I
1	List of all symmetric algorithms.
`	
ng	Symmetric encryption is a type of
	encryption where only one trey is used to both encrypt and decrypt electronic
	to both evenot and decept electronic
	information.
· · · · · · · · · · · · · · · · · · ·	(V (10 th Not
+	This encryption method differs from
- 1	a symmetric encryption where a pair here.
	is one public and one private is used
	to encrypt and decrypt messages.
	10 cucilla
_	The Secret her that the Sender and
	The secret trey that the sender and secripient both use could be a specific
	passing code or it can be random string of
	letter that have been generated by a
	Secure random number generales (RNCa)
	•
	These are maisty the type of Symmetra
	energetion of continued
11	Black algorithms:
	Let lengths of bits at
	encrypted in block of electronic data with
	the use of a specific tray.



2/	Stram algorithms:
	Dolla is every prece or
	Stream it instead of bizing tetrained
	in the System's memory.
A	Some examples of Symmetric encryption algorithm Nobode:-
~	AES (Adianced Encryphan standard)
. –	DES (Dota Encryphon Standard)
	IDEAC (Inkrictional Data Energetion Algorithm)
	Blowfish (Redacement for DES or 20EAG).
•	R(U (Rivert Cliphere U)
,	
	·



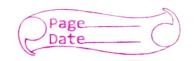
037	hist all assumetric trey algorithm.
4	0 0
Ave	Asymmetric tres algorithm work in a
	Similar mamner to Symmetric heg
	alognithm where paintest is combined
	exit a trey input to an alogoration
	and outputs ciphochest.
	The key pair is comprised of a private they and a public trey. Its the name
	key and a public key. Is the name
	wold books the is made anywhich to
	everyone where private teg is tept bearet
*	The Two main uses of asymmetric-they exception and
	aboutpus are hopic-les exceller and
	digital squatures public-key encryption is
1°	a nethal while anyone an send an encypted message within a trusted returns
	only selecter can dy decrypt the message
	only selecter can dydecrypt the message
,	·
,	Type of agymmetric her algorithm.
•	JOSE- Hellman Kegagerenent.
	Pivest Shamir Adlerman
3	J. Willes St. Silvering
`	S) Elliptic (ore (globography (Ecc)
	1) Digital signature Algorithm (DSA)



QB) List the algorithms for message digest Message digest algorithms sely on appropriate that suchars to generate a unique whee that is compiled from data and a unique symmetric heg. * It comptographic has hinten imposts date of ath strang length and produces a unique value of a lined length. -Adding a conjeque symmetric trey that in order to compute message digest that value provides consider talky to ensure that the message digest cannot be as easily changed if the date of changed in an unathorised or other mayoner. hist of message digest algorithms message Digets (MDS) 3) Leone Hash Algorithm (SHA-2) 3) SHA2 - 224 W SHAZ -256 5) SHAZ-SIZ



	Page
,	Name - Harsh Mishra Subject - Ion
7	Rallo-30 CK21: MCA-I
	Assignment - 2.
O	Discuss briefly in one-thro Sentences
cs)	PIL: Personally Identifable information (PIL)
	is any data that can be used to
	12 14 a conde in dividual a social
	Security mailings phase nois have most Commanly
	Considered as PIL.
	szin szintegy meg
18	Us privacy Act of 1974.
	Mil Oct Mar Delog secon of the statemen.
	and civil liberties Open 13
	a discission of privacy Acts disclouse phohbition
	a discission of privacy Acts disclouse phohoina its amendment provisions into across and its agency
	second terping registerents.
6	POZA:
	FOIA Stands Br Friedom of Information Act.
	It is a united states federal law that good grants
	phlis Access into processed by government agencies.
_	Dona Com Com to a Barrie Com And of 107ml of
g	FERPA: (family Educational Prights and princy Act of 1022) a. This is a federal legislation in us that
	This is a received registance in as
	probets privary of students presently. This art applies to all educational institutions that receive
	federal hods
*	



e) CFAA: The compiter froud and Abuse Act (CFAA) Uns enacked in 1986, as an amendment to the first federal comprise found law to address hacking (8) COPAA: The Council of Parent Attorneys and Advocate (COPAA) is an independent rational American association of parents of children with disablifies, attorneys, advocates and related professionals who protects the legal and civil rights of strents with disabilities and their families. (a) UPPA: - Video Privacey Probeton Act (UPPA) of
1998 generally prohibites the disclosures of a
Consumers who sental or purchase Jeconds to third parties. (H) HIPAA: -- The health inscreance portability and
Account ability Act (HIPPA) is an act cretar
by us congress in 1996 that amends both
Employee retrement Income Security (Act (ERISA) and Public Health Storice Act (PHSA) also known as blas Prantial modernisation act of 1999. It is a united states federal law that dequires lineacial institutions to expain how they share and ported their customers

proale homation



(I) PU DS: - The Payment Card Industry Data
Security Standard (PU DES) is a get of
sequirement prohibed to ensure that all
Companies that process stope or transmit
Choit Card Infor oraintain a season environment.

(K) FCRA: - The fair Chedit Reporting Act is
a federal law that beginness the conjection
of consumers credit Information and accers
to their acidit reports.

ACTA: - fair and Account Godit Towns art
Act is an Amendment to FCRA that
this Added primarily to probest Consumers
from identify typeff.