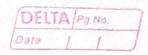
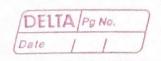


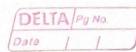
	AGSIGNMEN	7-1
	SECURITY IN	COMIPUTING
qi]	Differentiate between Lollips	p model 8 onion model.
Ansi-	Lollipop Model	Onion Model.
•	Also known as perimeter	· Also known as defense
	8ecurity	in depth.
•	involves building a single	Has multiple layers of
	wall around the objects	wall around the objects
	of value.	of value.
0	It is like a dollipop with	" It is like a onion with
	hard country shell on outside	moltiple layens & plenty of
	10	orying write peeling each layer.
	fails to add wess inside.	A layened security
-	threats & provides no protection	auchitecture provides
	against a perimet et broach.	multiple levels of protetion
		against Internal 8 external threats
0	Fisher only network .	There are move tayers
	scourity strategy	siather than blereware which
		also shows better protection
		against throats.
Му	NoteBook	Sign.



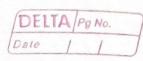
02]	Differentiare between authentication and
	authouization.
Ani-	Authentication Authorization.
1110	norroughor.
	In authorition process, the In authorization process
300 Page 100	identify of users are checked users authorities are
	for accessing the system. checked for accessing resources.
0	voeus auc venified voeus aux varidated.
	Done before the done after the
	authorization process authentication process
•	usually need usey's needs usey's privilege
	login cuedentials ou security levels
. 0	defermines whether the determines what permission
	neuson is user ou not do user nave?
- 8	4
0 -	eg. Emproyees in a company o eg. After an emproyee
	and required to authenticate successfully authenticates, the
	through the network begove system determines what
	accessing their company amail in to the employee elle
	allowed to access.
1	ly NoteBook Sign.



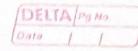
03]	write down the steps penformed to cheate Digital signature & explain it with proper example.
Ans!-	of digital signature is a mathematical technique used to validate the authencity & integrity of a message, slo out digital document.
	· Steps to create digital signature;
	O mes sage digeot is computed by applying has he function on the message & then message digest
	is encuypted vsing private key of sender to form the digital signature.
	Digital signature is men tuansmitted with the
	3 Receiver decrypts me algital signature using the
	The upreived now has the message algest.
	from the message
٨	Ay NoteBook Sign.



	6) The message digest computed by wereiver 8 the
	message digest need to be same four
	ensuring integritys
0	To cue ate a digital signature, signing apportitume
	like email programs create a one-way hash of the
	c-data which is to be signed.
8	The signing algo then encrypts the hash value
	volng private key.
0	This encrypted has no along with other into like the
	hushing also is the digital signature.
m	hashing algo is the digital signature. This algital signature is appended with date &
	sent to the verificy.
	The neason bon encypting the hash instead of entire
	hast message is that a hast function convents any
	an pitary input into a much shout or fixed value.
	an birary important
***	
-	
	Ny NoteBook Sign.
	17 13 13 13 13 13 13 13 13 13 13 13 13 13



04]	Differentiate between public key anyptography & private key anyptography.
	private key cuyptography.
	0 6 1.
C.	than public key puivate key.
0	
	is used to encuyet & key used for encryptions
	decayet the message other four decryption.
	The key is kept as a one of the 2 keys is
	Scoret.  Rept as a secret.  Delic te de la commetrical
	because there is only one because there are 2 types
	Key that is scoret key op key a private & public.
	Sender & Meresvernoed . Sender & geresver does
	to shave the same key not shave the same key
0	Performance besting cheeks · road testing checks the
	the gelfablily, scalability & sustanibility of the
	speed of the system. system.
٨	fly NoteBook
	Sign.



05] Waite a shout note on PKI.

Public Key Johnsonweyoure (PKZ) is a deannology four authenticouting users & devices in the digital would. The basic idea is to have one our more toursted parties digitally sign documents countifying that a particular cryptographic key belongs to a particular user for device. The key can then be used as an identity four the user in digital networks.

The useus & devices that have keys are often just couled entities. In general, any thing can be associated with a key that it can use as its identity. Besides a user our device; it could be a program, process, manufacturer, component, or something eve. The purpose of a PKI is so securely associate a key with an entity.

A pub PKI relies on digital signature technology, which uses public key enyptography a The basic ldea is that the secret key of each entity is only known by that entity & is escal for signing. This key is failvate key there is another key derived from it palled public key which is used for vealifying signatures.

My NoteBook