

Assignment No:2

9.1	Write: short note topiloligital algoratures and
	digital cextificates.
\Rightarrow	digital certificates.
•	Digital signatures subv bed DIV (
_	A digital eignature is a hosti walve that has
y the for	been senery pled solth vities senders private lay.
1 Jinn	The last of stanting means enoughting the
	the messages back welve walth add solved a large
\bigcirc	the message's hach value with ad private lary
	So the sender computes and energylos the
	hash value buigh her private beyon
126-	EAH the traceiving end, you decript the
	hash value with sender's public key. Now,
	because no one knowns the private key of
	the sender, altering the hack wallie and
60	seelgning coith the private lary of the
	is bender is not possible tong bit
	Idrahi majaran Las revisione ya ita
,	Processing applied Security Ripporty
	handid on meacagle de la lacheved
(A	2) Encryption of all confidentiality
(2)	Hashing to sides i Integrity or
	Digitally signing Integrity, authorbication,
	4 doot to be began a some repudiation.
1000	Encouption and digitally confidentiality wintegrity,
	signing authentication is non-repudite
-	Applications:
	I sending and receiving occurs emails.
107	2) signing do cuments.



Sign thompies A

131851C

Properties loof: Idigital reignature: -9 11-11 1.2 . 29 knother on lotipib 1) Integrity =) Via hach value calculation bligis. soil 12) 1. Author tication of smutorple lotipit 1 (= DoviNia the ability to prove sender's identity by deanyphings hashered the dendered known of allevipublicatively auton dond s'agressom att att 2 Mone repudiation more above att of C 3 ender connet deny reending the meating brequer due used her private très do enouget hach value with sender's make bythe wow permise no one knowns the private may at but Digital contitiones enter bla sones out Digital contillades Is to Issued by a liveded third party which proves cendering entity to the secriver and secretary identity Avidiquidal certificate is a certificate 15 suediaby a Certificate Aithenity (CA) to wealfy the identity of the contincate offer totalder Hirpshot / Eningia plating Digital ceatificates is used to attach the the public they will the ab particular mairidual with you or or samilentity. Applications! 2) Signing decuments.



1	
	2; 20/2/20 10 Coodalas :-
	Digital Ceotificate Contains:
ž) Name of certificate holder
	2) Sevial number which used to uniquely identify
	a Chinistate
	3) Expiration dates
	4) Copy of controle holders porting
	5) Digital signature of certification
	4) Copy of contistione holder's publickey: 5) Digital agratuse of centificate resuing
	() ()
	· · · · · · · · · · · · · · · · · · ·