PARSHWANATH CHARITABLE TRUST'S



# A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester:

Subject : \_\_\_ C& S

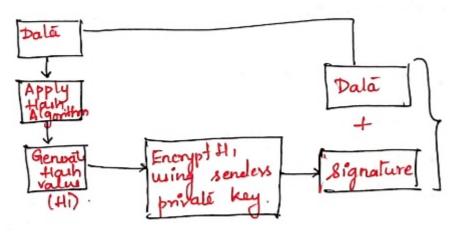
Academic Year: 2028- 2024

DIGITAL SIGNATURE - RSA:

When sender sends a message to receiver, receiver needs to check the authenticity of the sender. Receives needs to be sure that the message is coming from authentic sender and not an adversary, for which he can ask the sender to sign the message dedronically.

A digital signature is a mathematic technique used to validate the authenuity and integrity of a message, software or digital document. It allows us to verify the author name, dali and time of signature, and authenticale the message contents. Digital signature are created and venified using public key/asymmetric

key cryptography. Sender signe the Digital Signalure



Receives Dala along with the Digital signalure.

Sleps: sender applies hash algorithm on the original generalis hash value H1. dala

Subject Incharge: Prof. Sarala Mary Page No.\_



#### PARENDIANATH CHARITABLE TRUST'S A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester VI Academic Year: 2028-2024 Subject : CSS Stip 2: Sender enoughts He using sender private key. The encupted value is the signature Steps: The sender sends the plain list data along with the signature to the necessel. Receives verifies the Signature: Apply Hach Algorithm on the dala = H1 Dala Meelage Decrypt the signalure using public key of senser = H1. Step 1: Receiver receiver the original date along with eignature Stepa: Receiver applies the Hash Algorithm on the data and generalis H1. Steps: Receiver decrypte the signature using public key of

the sender and generales 41. Slept: If Hi generated in Sleps and Hi generated in Steps are equal then "Message is not modified" else "Message u modified".

Subject Incharge: Prof. Sarala Mary Page No. 2



PARSHWANATH CHARITABLE TRUST'S



### A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering



Semester : VI Subject : \_\_CSS Academic Year: 2023-2024 sign the Digital Certificate? CA -> Certifical authority Version Slep 1. Certificate Senal Number Apply Houh Algorithm Algorithm on date and generale Hashvalue HI. Parameters Issuer Name Encupt Hi, wing CA. Validity private key. Subject Name Subject Public key Information Issur unique ID. CA 20 Digital Subject unique ID signature Extensions Slép 3. CA signature Slip 1: Hash algorithm is applied on the data of the Digital Certificale and heigh value Hi is generated. Step a: He is encupted using CA private key and CA digital signature is generaled. Step 8: The digital signature is appended at the bottom of the Degilal Certificate and it is chared

Subject Incharge: Prof. Sarala Mary Page No. 1

with the Receiver.



#### PARSHWANATH CHARITABLE TRUST'S

## A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: V Academic Year: 2028 2024 Subject: CSS How does the receiver veuilles digital e exceptificale? Vusion Receive applies houh algorithm Certificate senal No. on the data Algorithm Certificali and generales Parameters is audhent 41 ceded. Issuer name Validity Subject Name No. Certificat Subject Public Key Info i no Issur unique ID autherteate Subject Unique ID Receive decaypts the signalureusing Extensions. CAi public key CA Signalure and gereceives H1 the Digital certificate along with Stép1: Receives receives CA Signalure Stepa: Receiver applies the Hash Algorithm on the dala and generalis H1. Steps: Receiver decypte the signature using CA's public key and receives HI. Slep 4: It HI received in Slepa and HI received in Slip 3 is equal then the Certificate is authenticated and signed by right CA, if not the Custificate is not authenticated

Subject Incharge: Prof. Sarala Mary Page No. 2

