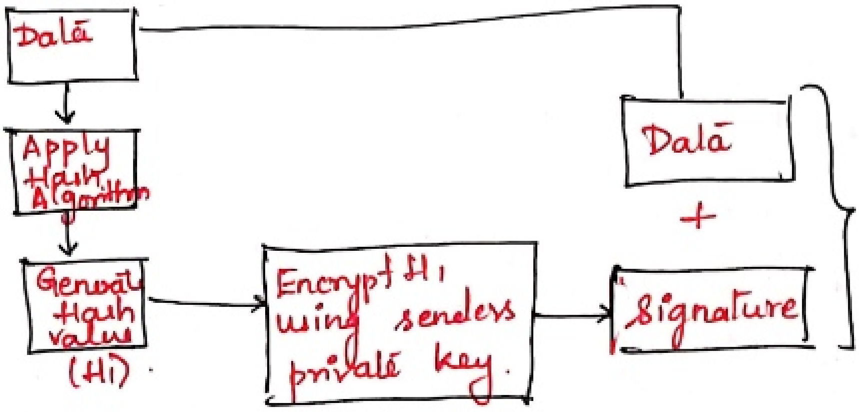
DIGITAL SIGNATURE - RSA :-

When sender sends a message to receiver, receiver needs to check the authenticity of the sender. Receiver 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 electronically.

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

Sender signs the Digital Signature



Send to the Receiver Data along with the Digital Signature.

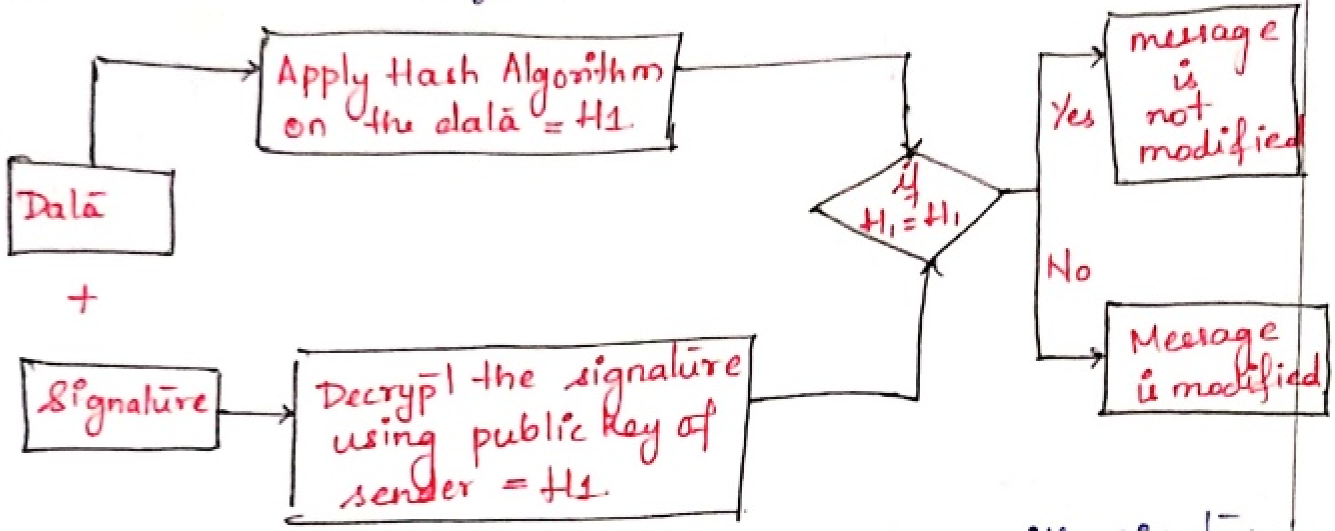
Step 1: Sender applies hash algorithm on the original data and generates hash value H1.

Semester: VI Subject: CSS Academic Year: 2023-2024

Step 2: Sender encrypts H_1 using sender private key. The encrypted value is the signature

Step 3: The sender sends the plain text data along with the signature to the receiver.

Receiver verifies the Signature:-


Apply Hash Algorithm on the data = H1
Data
+
Signature
Decrypt the signature using public key of sender = H1
if H1 = H1
Yes
No
message is not modified
Message is modified

Step 1: Receiver receives the original data along with signature

Step 2: Receiver applies the Hash Algorithm on the data and generates H_1.

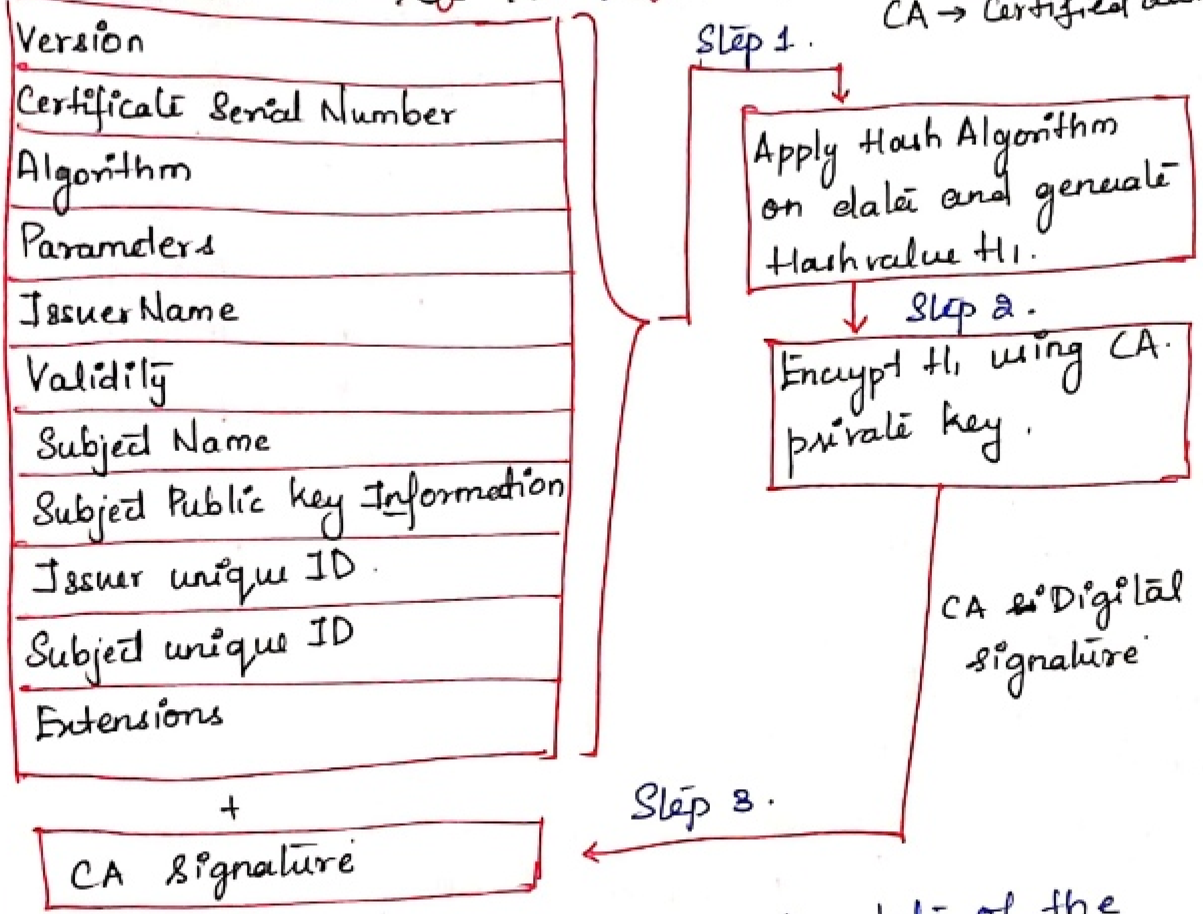
Step 3: Receiver decrypts the signature using public key of the sender and generates H_1.

Step 4: If H_1 generated in step 2 and H_1 generated in step 3 are equal then "Message is not modified" else "Message is modified".

Semester : VI Subject : CSS Academic Year: 2023- 2024

How does the CA sign the Digital Certificate?

CA → Certified authority



Version
Certificate Serial Number
Algorithm
Paramaters
Issuer Name
Validity
Subject Name
Subject Public key Information
Issuer unique ID
Subject unique ID
Extensions
+
CA signature

Step 1.
Apply Hash Algorithm on data and generate Hashvalue H1.
Step 2.
Encrypt H1 using CA private key.
CA Digital signature
Step 3.

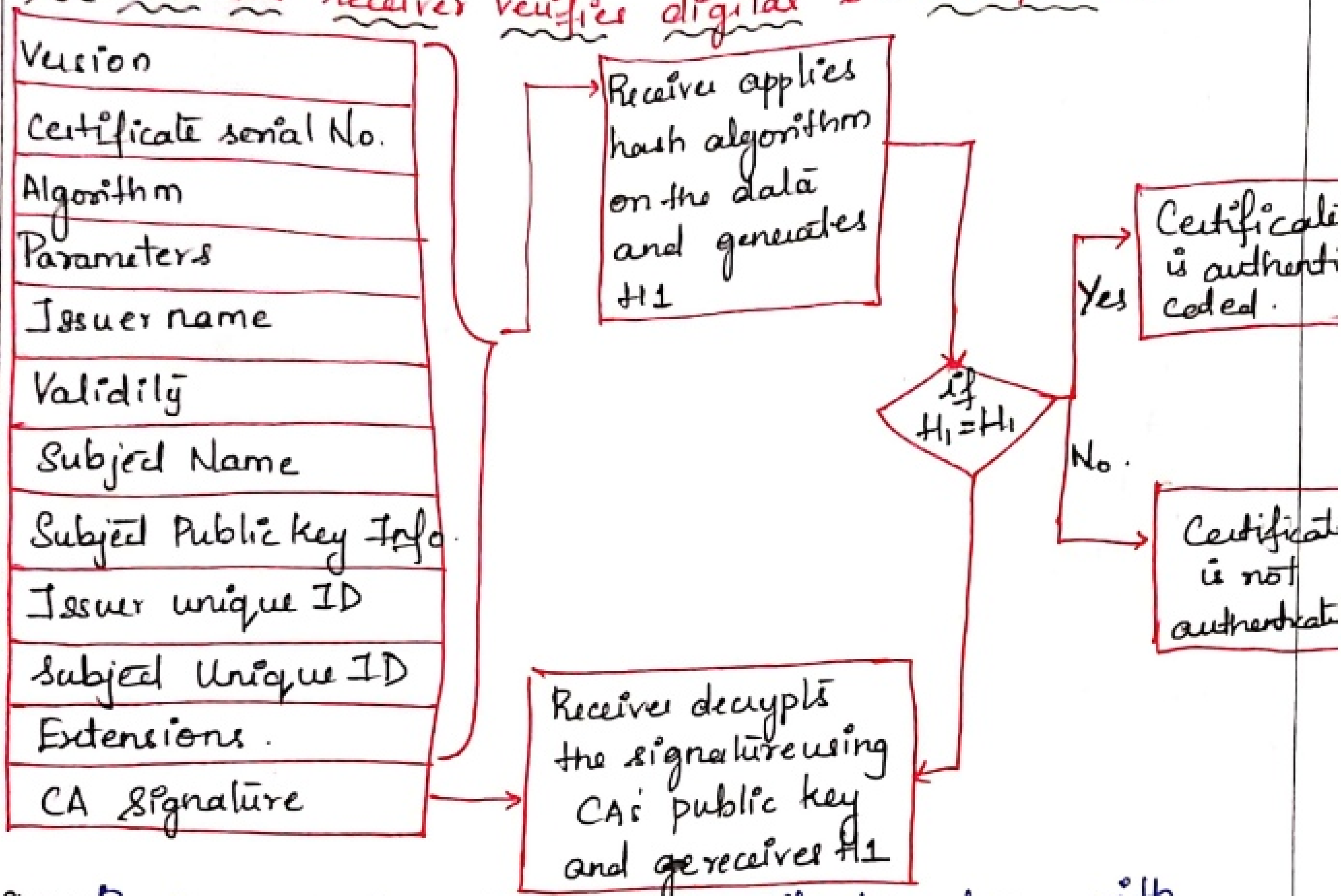
Step 1: Hash algorithm is applied on the data of the Digital Certificate and hash value H1 is generated.

Step 2: H1 is encrypted using CA private key and CA digital signature is generated.

Step 3: The digital signature is appended at the bottom of the Digital Certificate and it is shared with the Receiver.

Semester : VI Subject : CSS Academic Year: 2023 2024

How does the receiver verifies digital & ~~si~~ certificate ?


Version
Certificate serial No.
Algorithm
Parameters
Issuer name
Validity
Subject Name
Subject Public key Info.
Issuer unique ID
Subject Unique ID
Extensions.
CA Signature
Receiver applies hash algorithm on the data and generates H1
if H1=H1
Yes
Certificate is authenticated.
No.
Certificate is not authenticated
Receiver decrypts the signature using CAs public key and ~~ge~~ receives H1

Step1: Receiver receives the Digital certificate along with CA Signature.

Step2: Receiver applies the Hash Algorithm on the data and generates H1.

Step3: Receiver decrypts the signature using CAs public key and receives H1.

Step4: If H1 received in Step2 and H1 received in Step3 is equal then the Certificate is authenticated and signed by right CA, if not the Certificate is not authenticated