CSS

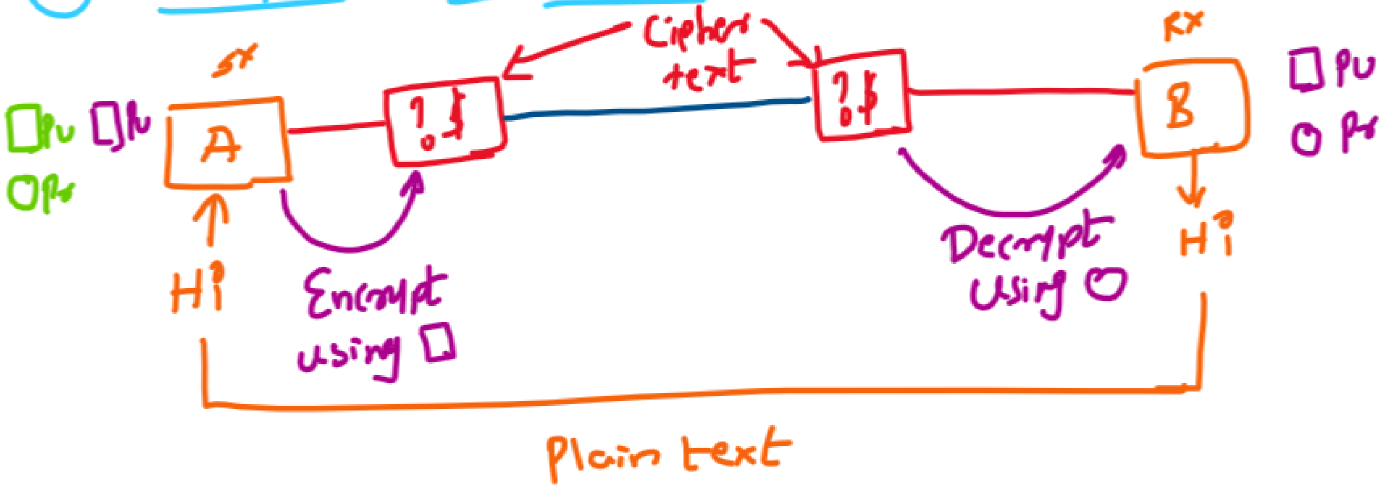
Prof. Amit K. Nerurkar

Assistant Professor

Department of Computer Engineering

Vidyalankar Institute of Technology, Wadala

① Encryption & Decryption



① Two process a. PT → CT (S^x)

b. CT → PT (R^x)

② C.T. Length = P.T. Length [Variable]

ie P.T. = 2 char

∴ C.T. = 2 char

③ Protecting data in the n/w

② Hashing

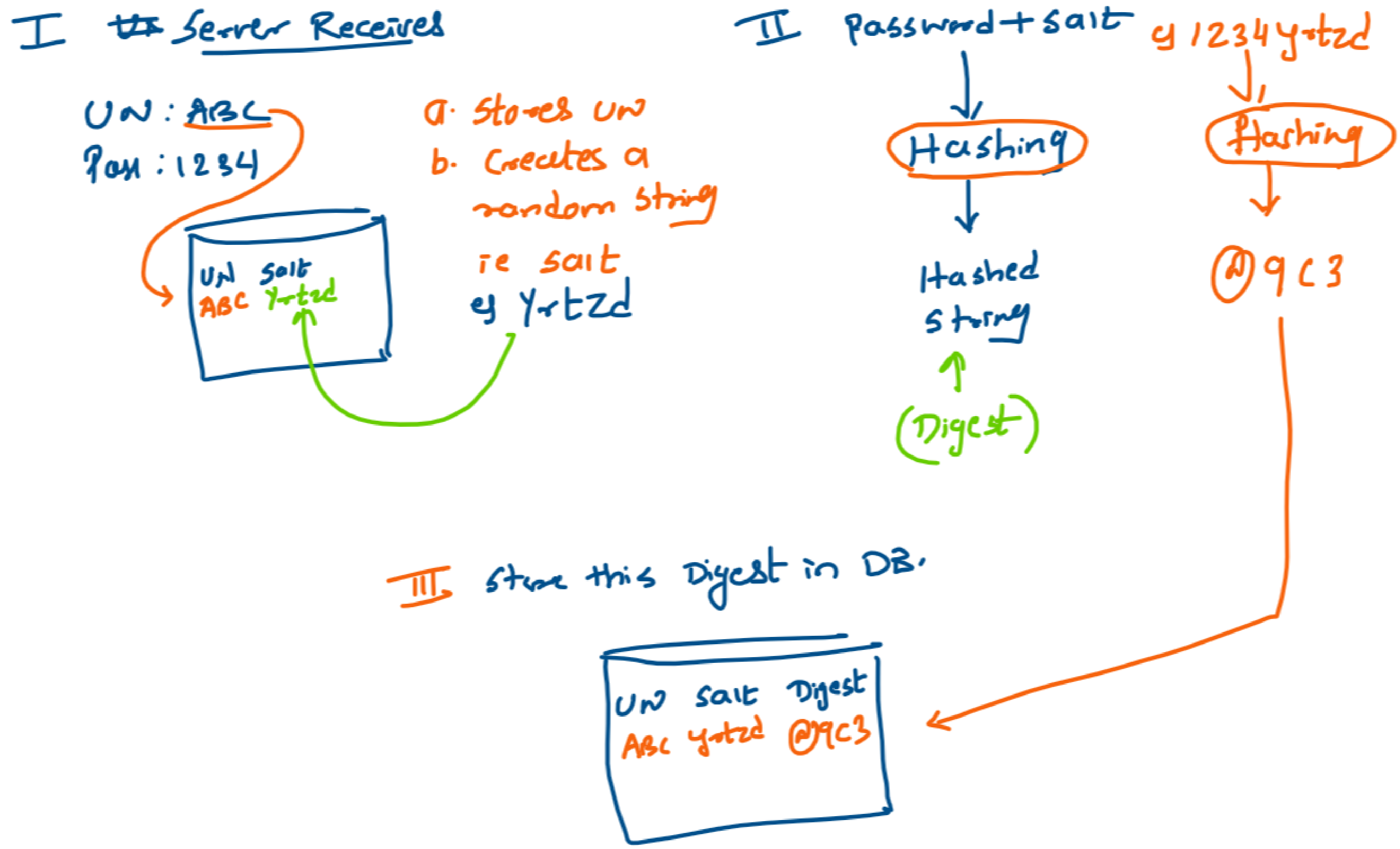
① oneway a. P.T. → C.T.

② C.T. is of fixed size

③ Protecting data on bearer.

Hashing:

① Password Creation



I ~~tt~~ Server Receives

UN : ABC
Pass : 1234

a. Stores UN
b. Creates a random string
ie salt
eg Yrtzd

UN	Salt
ABC	Yrtzd

II Password + salt   eg 1234Yrtzd

Hashing → Hashed string ↑ (Digest)

Hashing → @9c3

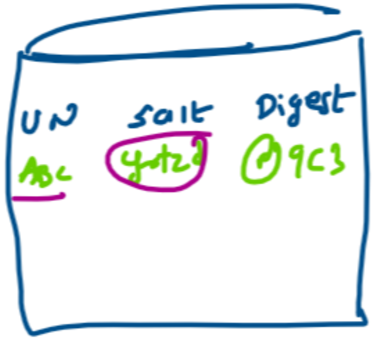
III Store this Digest in DB.

UN	Salt	Digest
ABC	Yrtzd	@9c3

II Password verification

I Server Receives

UN: ABC
Pass: 1234



UN	Salt	Digest
ABC	ytzd	@9c3

1 searches for UN

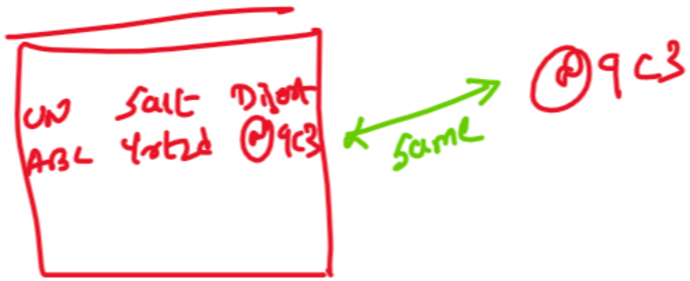
2. Fetches the Salt

II Pass+Salt eg 1234ytzd

Pass+Salt ↓ Hashing ↓ Hashed String (Digest)

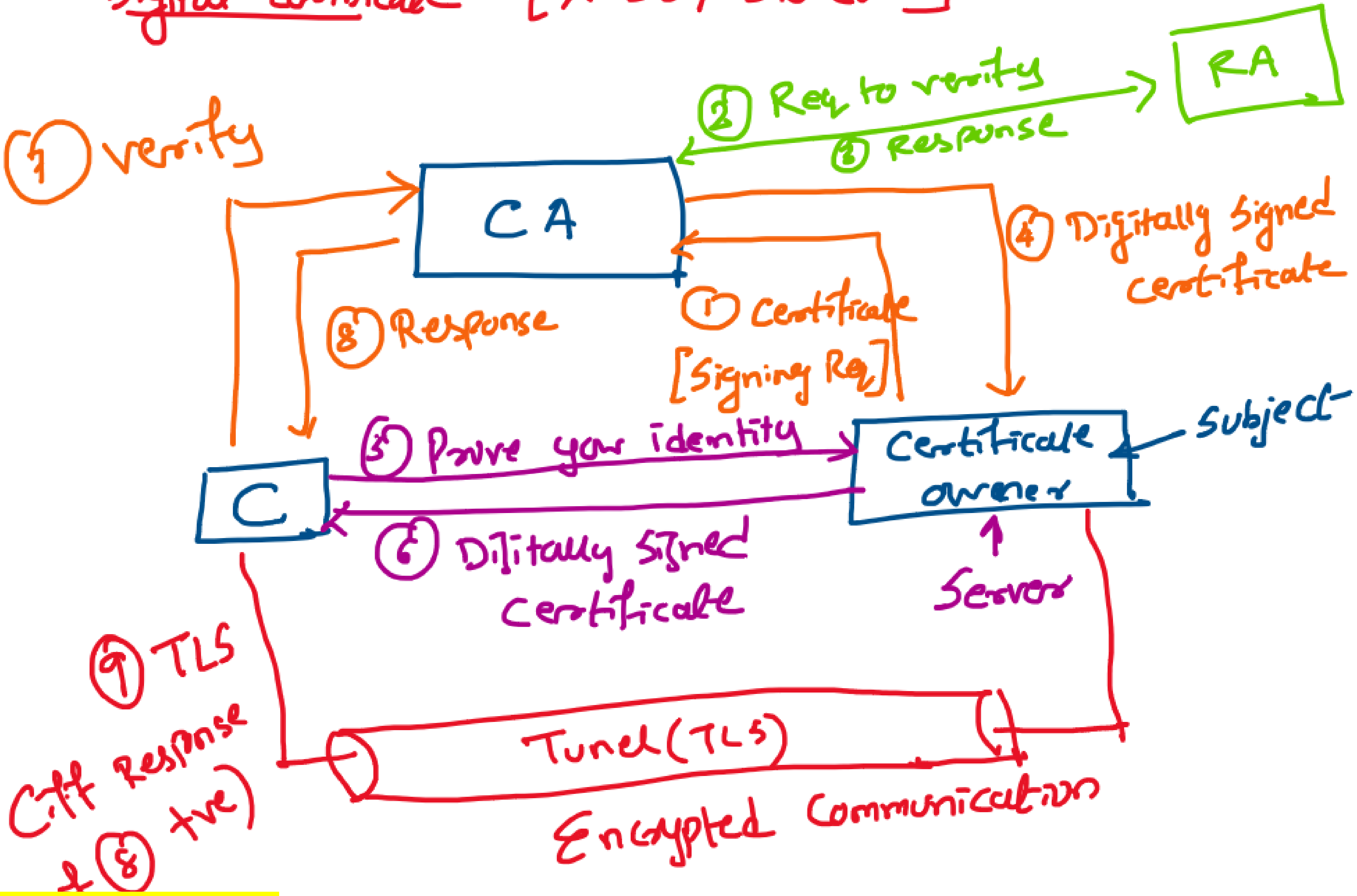
1234ytzd ↓ Hashing ↓ @9c3 ← Note: If password is wrong then Digest will not match the Stored Digest.

III Compare the Digest, if same user is valid

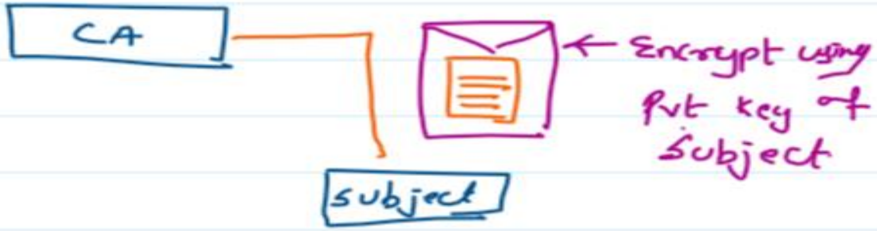


UN	Salt	Digest
ABC	ytzd	@9c3

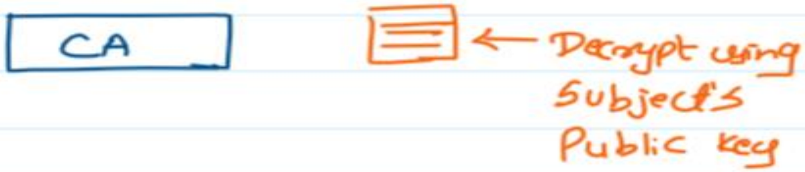
Digital certificate [X.509 Standard]



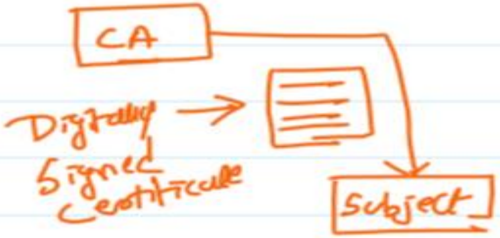
I Subject creates certificate & encrypts that using subject's private key. This is now sent to CA.



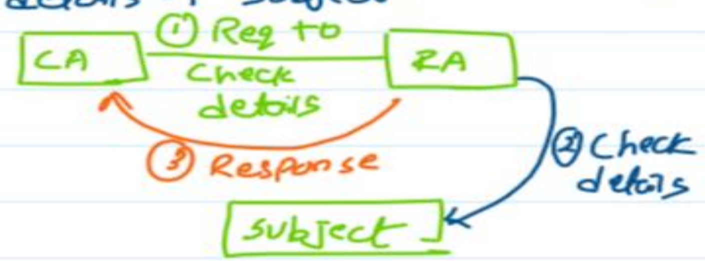
II CA now tries decrypting using subject's Public key, if sucessful then Req is accepted.



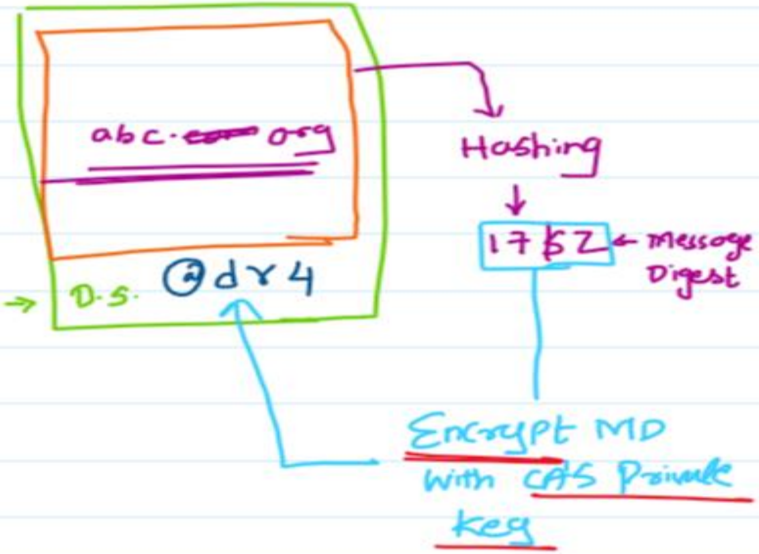
V This Digitally signed certificate is now handed over to Subject



III CA gives Req to RA for checking details of subject.

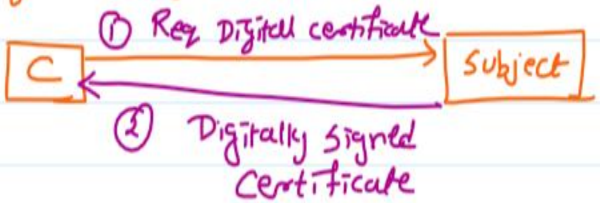


IV If Response is true from RA, ~~CA~~ then CA starts ~~preparation~~ creating the Digital Signature.



Verifying the Digital certificate

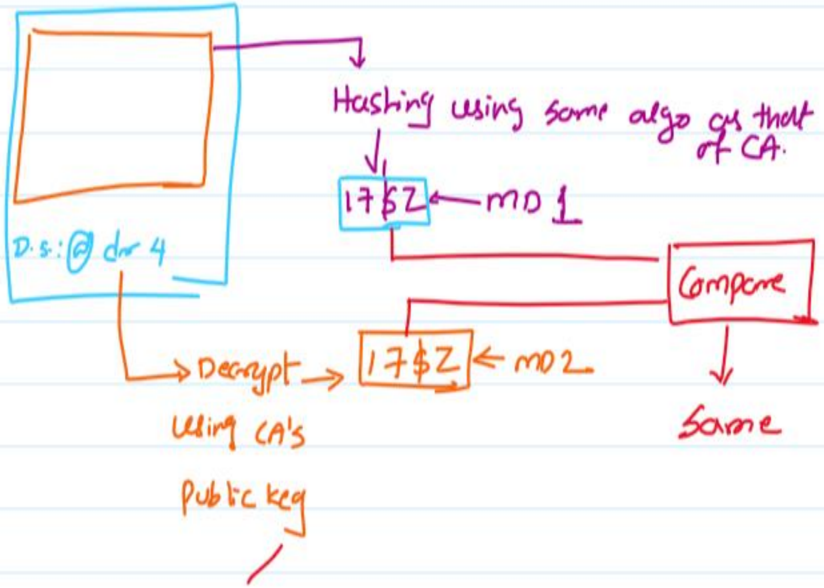
I



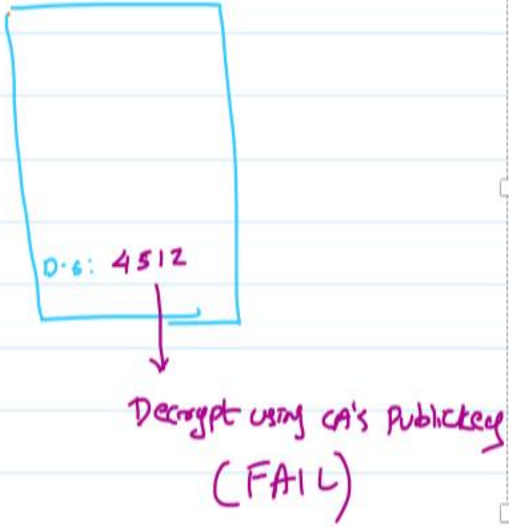
Client Request subject for its Dijital certificate.

II Client verifies the Dijital certificate.

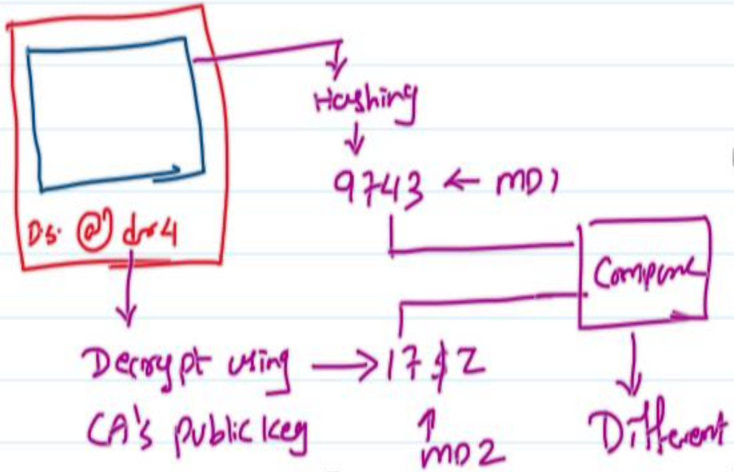
Case 1: Valid D.C.


Hashing using same algo as that of CA.
17$Z ← MD 1
D.S.: @ dr 4
Decrypt using CA's public key
17$Z ← MD2
Compare
Same

Case 2: Invalid Dijital signature:



Case 3: Digital certificate intentionally changed after D.S.



Prepared by Prof. Amit K. Nerurkar

Thank You

Name: Amit K. Nerurkar

Designation: Assistant Professor

College: Vidyalankar Institute of Technology