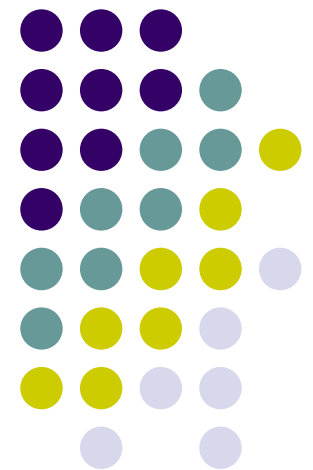
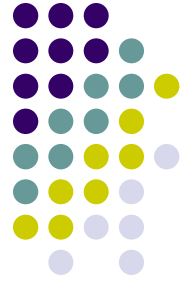


E-GOVERNANCE SECURITY ISSUES

N.VIJAYADITYA
CONTROLLER OF CERTIFYING
AUTHORITIES
MIN.OF
COMMUNICATIONS&INFORMATION
TECHNOLOGY



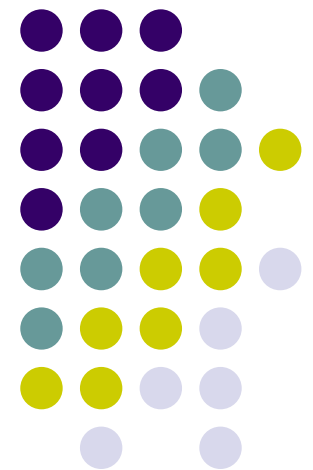
Security Issues :-



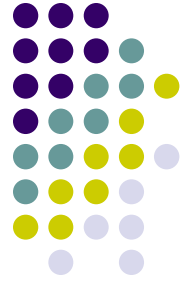
- Confidentiality
- Integrity
- Authenticity
- Non-Repudiability

E-SIGNATURES

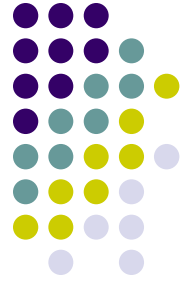
Is electronic equivalent
Of
Handwritten signature



NEED FOR E-SIGNATURES

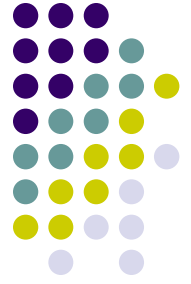


- speed transactions
- Reduce travel time
- Reduce in person meetings
- Reduce the amount of paper



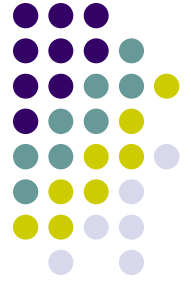
TYPES

- PKI..based digital signatures
 - the most full-featured
 - most secure
- BIOMETRIC based
 - fingerprint
 - iris of an eye
 - sound
 - dynamics of handwriting



BIOMETRIC

- Unique characteristics that separate the person scientifically from anyone else
- With biometric data a 100 percent match is not probable
- Organization must determine the acceptable parameters
- If too generous false matches follow
- If too strict too many false matches



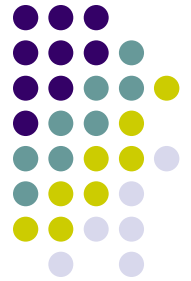
Threats to Authenticity

- Masquerading

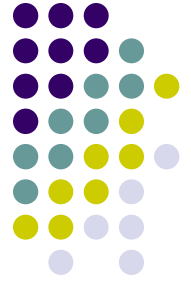
Counter Measures

- Strong
 - Digital Signature - Cryptographically generated credentials.

Authentication of electronic records



- By affixing
 - **Digital signature**
- Affected by use of
 - **Asymmetric crypto system**
 - **Hash function**



Encryption:

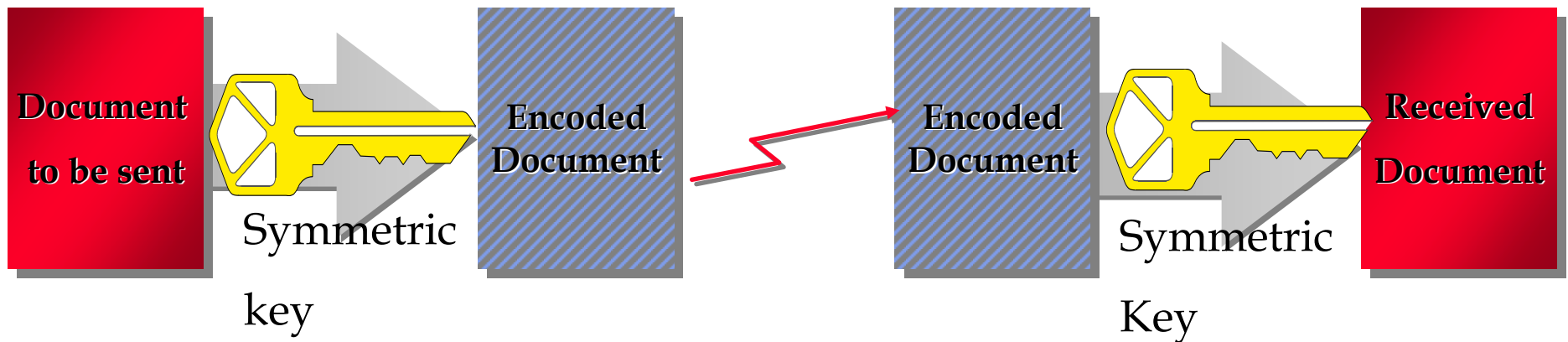
- Transformation of data to Prevent information being read by unauthorised parties.
- Sender and Receiver have to know the **rules** which have been used to encrypt the data.
- Based on **Algorithms** which are **mathematical functions** for combining the data with a **string of digits called the Key**. The result is the encrypted text.

Eg: **Adding** a fixed number of characters, say **5**, to each character in the message that is being encrypted.

The word SECURITY then becomes the encrypted text XJHZWNYD



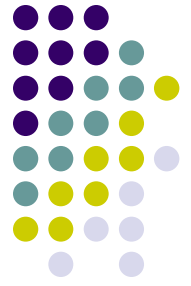
Symmetric Key Cryptography



- **Identical keys are used for encryption and decryption.**
- **Requires both parties to do a digital conversation to know the key.**
- *'n' Partners means handling n secret keys*
- *Authenticity cannot be proved.*

Public key cryptography

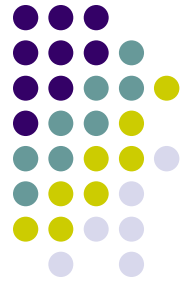
(Asymmetric)



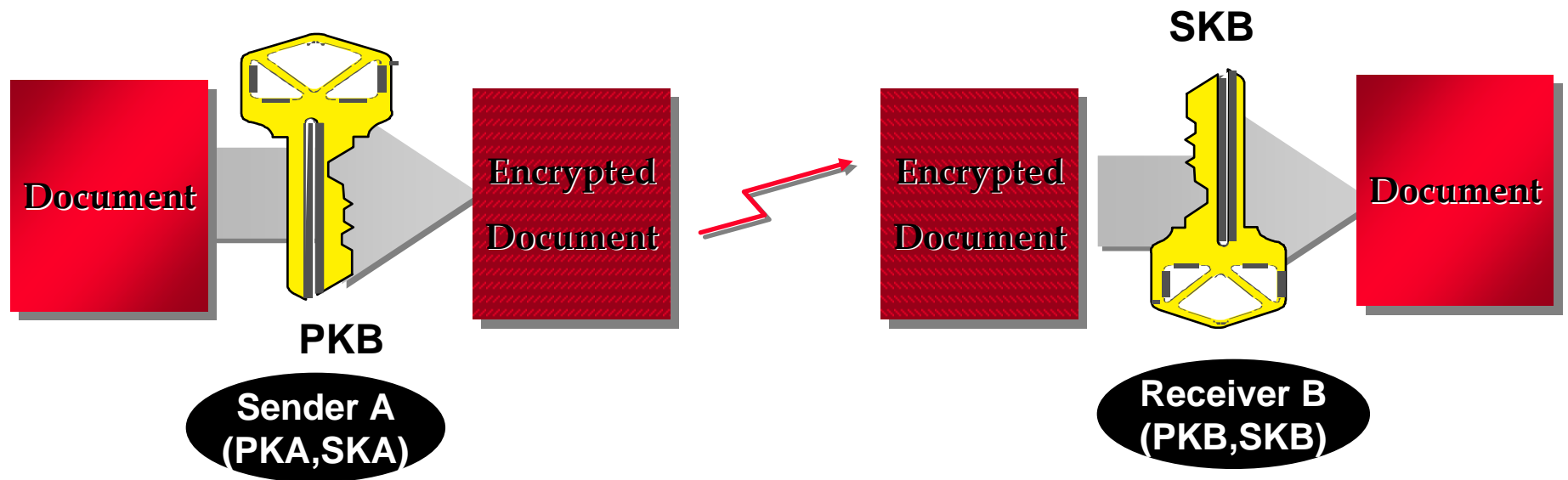
- Each party is assigned a pair of keys –
 - One **Public** key – known to everyone
 - One **Private** key – known only to the possessor
- Information encrypted with the private key can only be decrypted by the corresponding public key & vice versa.
- *Fulfils requirements of confidentiality, integrity, authenticity and non-repudiability.*
- *No need to communicate private keys.*

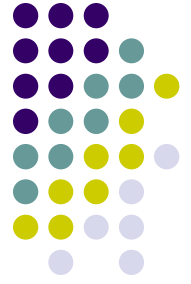
Public key cryptography

(Asymmetric)



Confidentiality





Digital Signatures

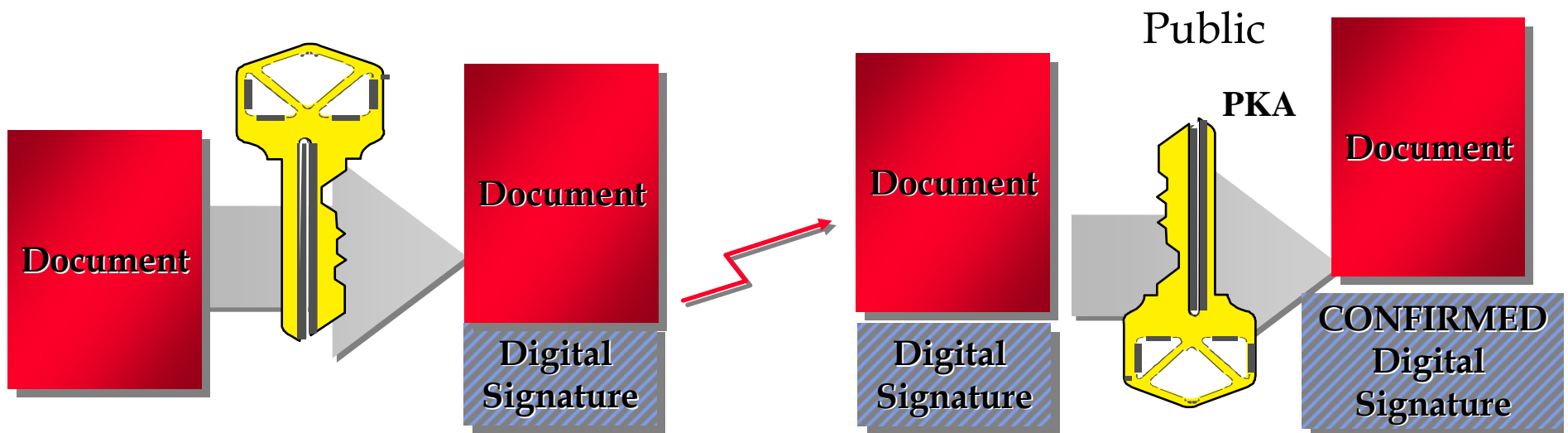
- To ***digitally sign*** an electronic document the signer uses his/her ***Private*** key.
- To ***verify*** a digital signature the verifier uses the signer's ***Public*** key.

Public key cryptography

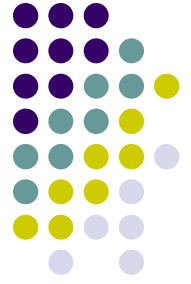
(Asymmetric)



Digital Signature



- *The message is encrypted with the sender's private key*
- *Recipient decrypts using the sender's public key*



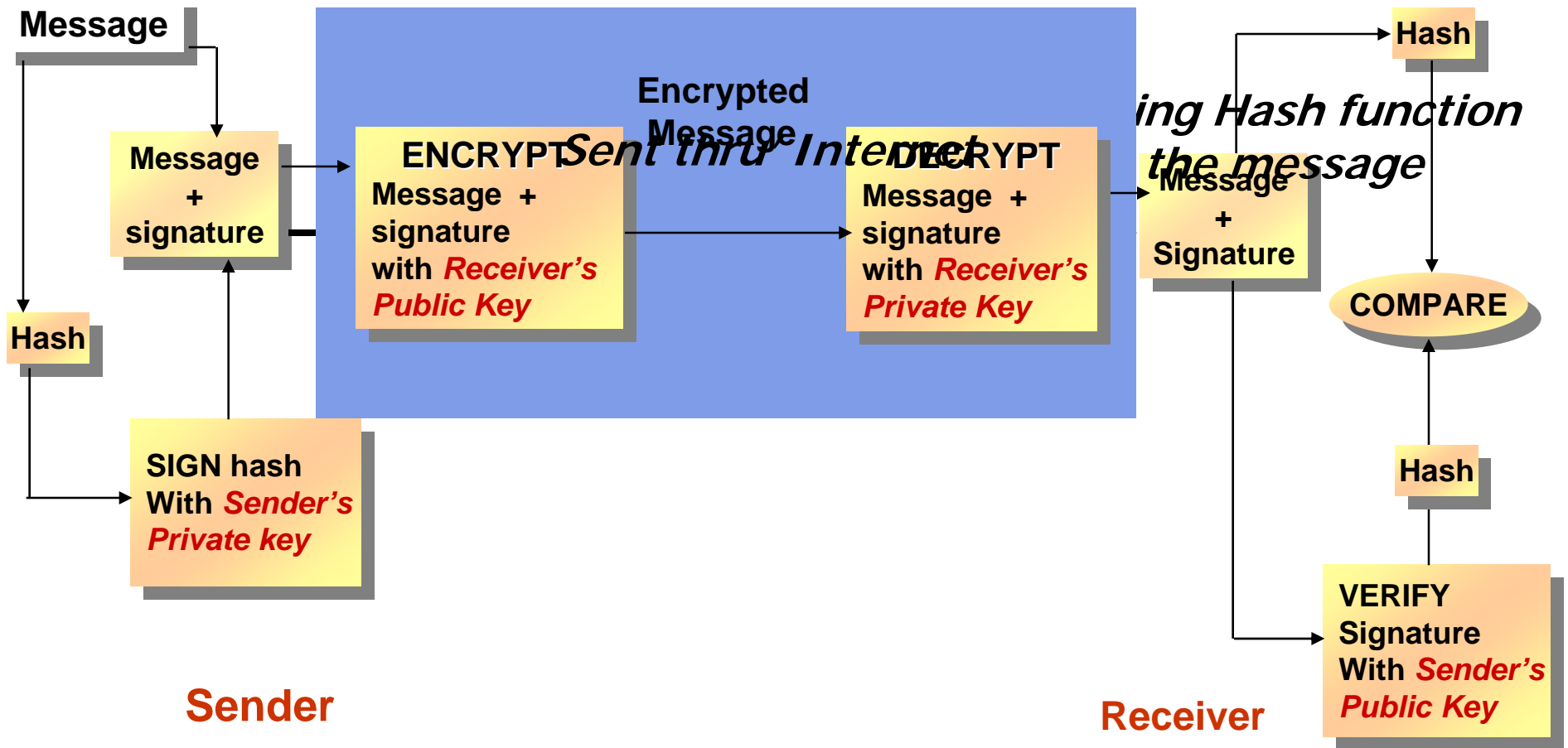
Message Integrity

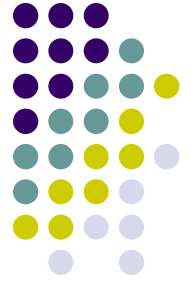
- **one-way** hash functions
- original data cannot be generated from hash output
- No two messages will generate the same hash.

SIGN the HASH

NOT the entire Message

Confidential Signed Messages





Issues in Public key Cryptosystems

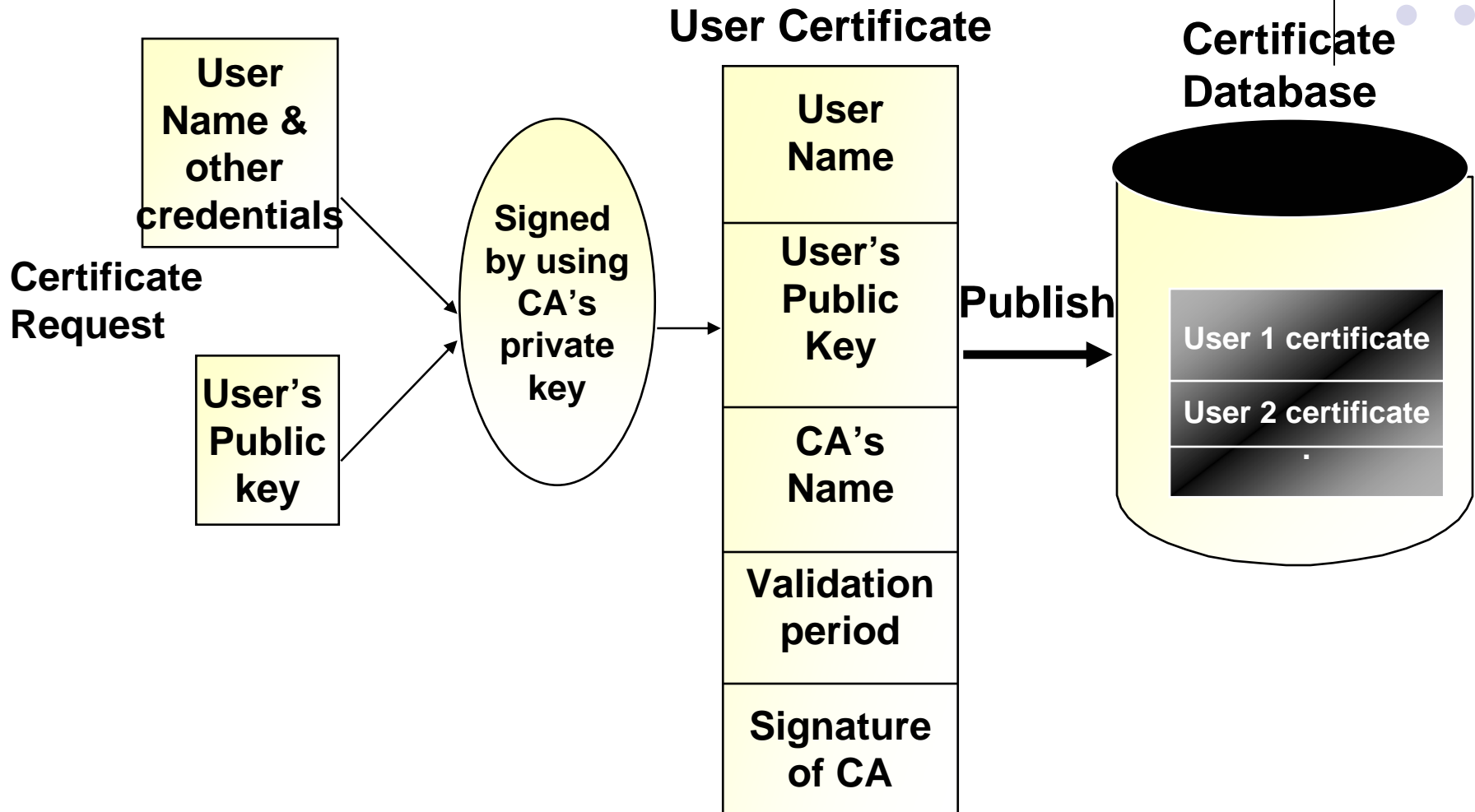
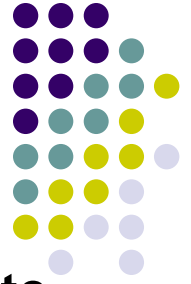
- How will recipient get senders public key?
- How will recipient authenticate sender's public key ?
- How will the sender be prevented from repudiating his/her public key?

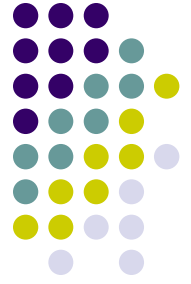
Certifying Authority



- An organization which **issues** public key certificates.
Must be widely known and **trusted**.
Must have well defined methods of assuring the **identity** of the parties to whom it issues certificates.
Must confirm the **attribution** of a public key to an identified physical person by means of a public key certificate.
Always maintains **online access** to the public key certificates issued.

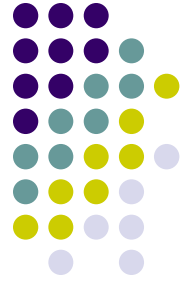
Public-Key Certification





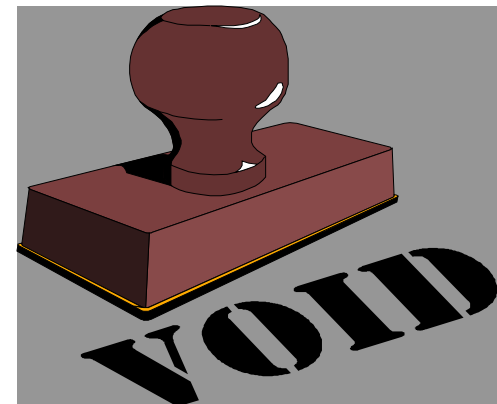
Contents of a Public Key Certificate

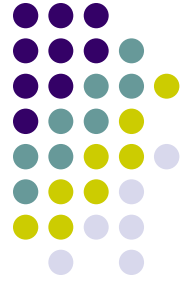
- Issued by a CA as a data message and always available online
 - **Serial Number** of the Certificate
 - Applicant's **name**, Place and Date of Birth, **Company Name**
 - Applicant's legal domicile and virtual domicile
 - **Validity period** of the certificate and the signature
 - **CA's name**, legal domicile and virtual domicile
 - **User's public key**
 - Information indicating how the recipient of a digitally signed document can **verify** the sender's public key
 - **CA's digital signature**



CRL

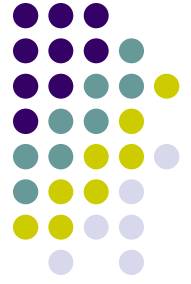
- Certificate Revocation List.
- **A list of all known Certificates that have been revoked and declared invalid**





Technical Infrastructure

- CCA as the “Root” Authority.
- Certifies the technologies and practices of all the CAs licensed to issue DSC.
- CCA operates the following :-
 - Root Certifying Authority (**RCAI**) under section 18(b) of the IT Act, and
 - National Repository of Digital Signature Certificates (**NRDC**) under section 20 of the IT Act.



End entities, subscribers and relying parties

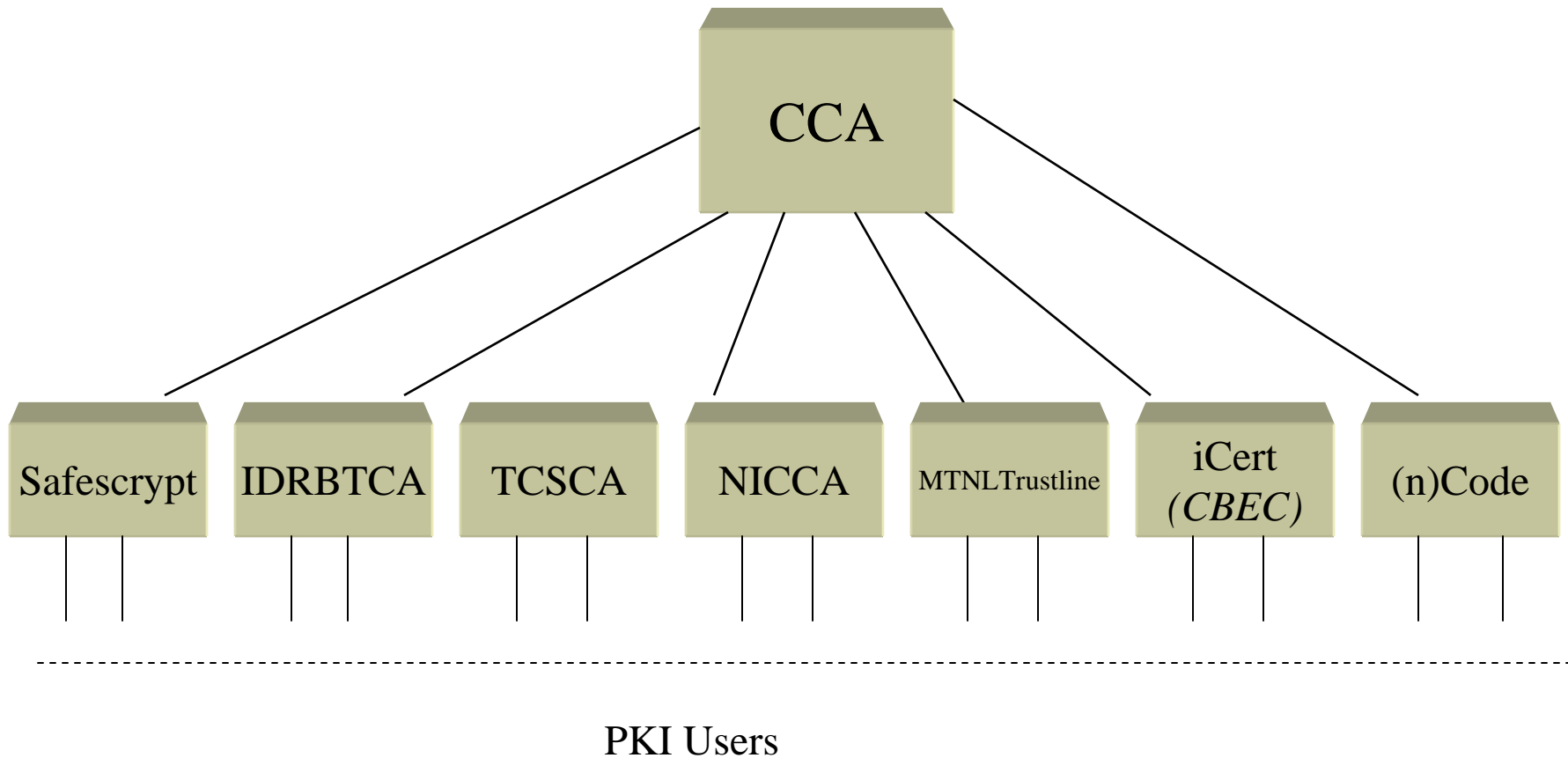
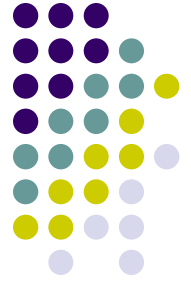
- The End entities of RCAI are the Licensed CAs in India.
- Subscribers and RPs using the certificates issued by a CA need to be **assured** that the **CA is licensed** by the CCA.
- They should be able to verify the license under which a PKC has been issued by a CA.

National Repository : NRDC



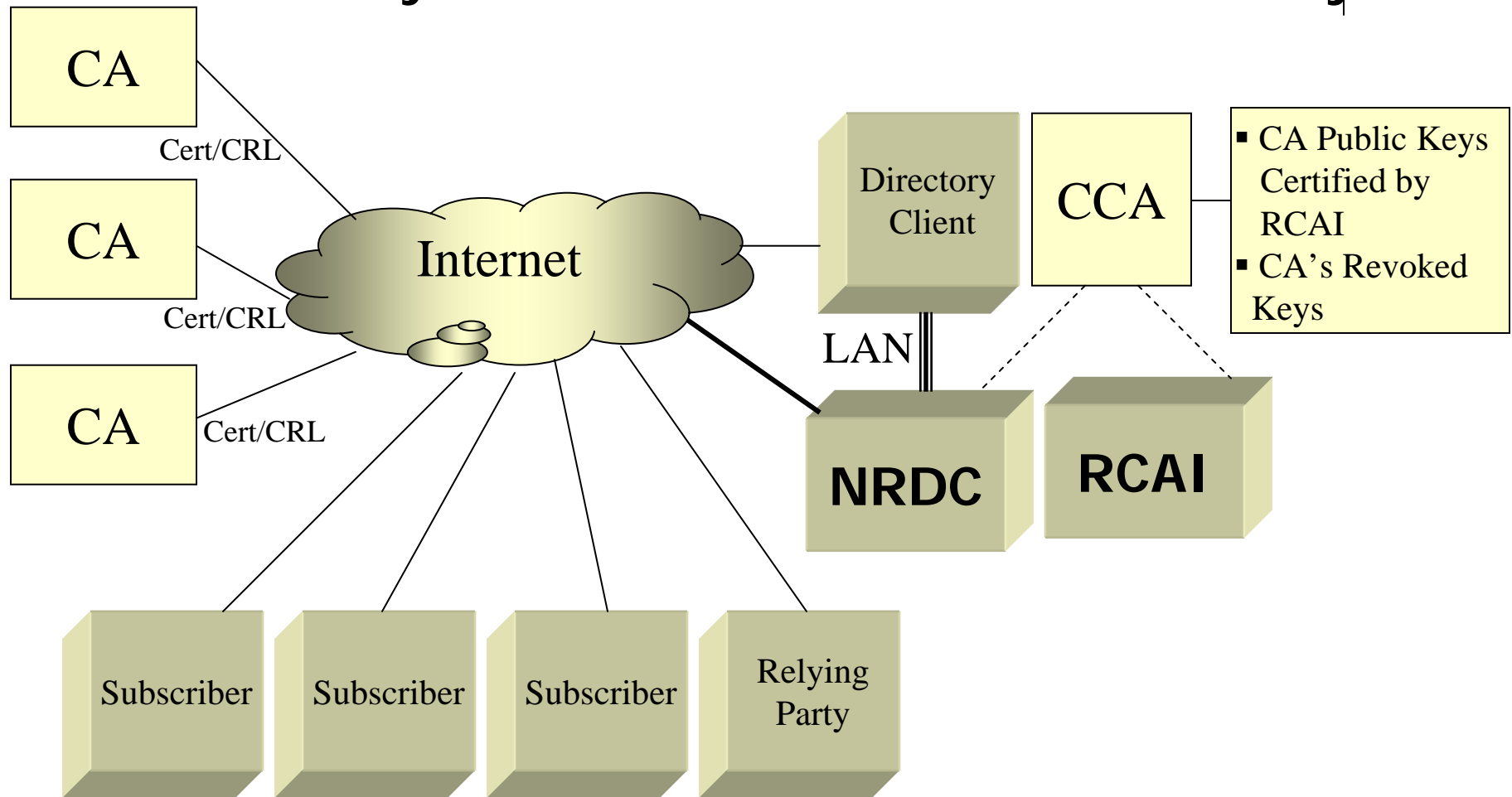
- National Repository of
 - Digital Certificates
 - Certificate Revocation List

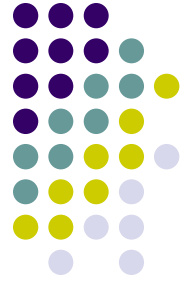
India PKI Hierarchy





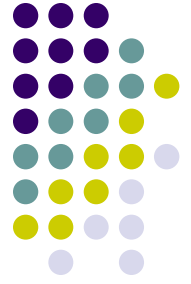
CCA : National Repository of Certificates of Public Keys of CAs and Certificates issued by CAs





IT Act 2000

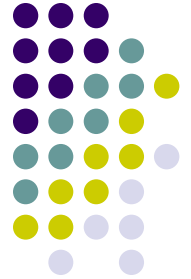
- Information Technology Act, 2000
- Enacted on 9th June, 2000
- Provides **legal recognition** for **transactions** carried out by **electronic** means.
 - Use of **alternatives** to paper-based methods of communication & info. Storage.
 - To facilitate **electronic filing**.
 - Amends other acts.
- Based on **UN Model Law** of EC



Indian IT Act....

- To facilitate EC & EG
- IT Act 2000
- Rules
- Regulations
- Guidelines
- Notifications & Amendments

THANKS



Public Key Infrastructure
for
Digital Signatures

under
IT Act 2000

