Bachelor of Computer Science

SCS2214 - Information System Security

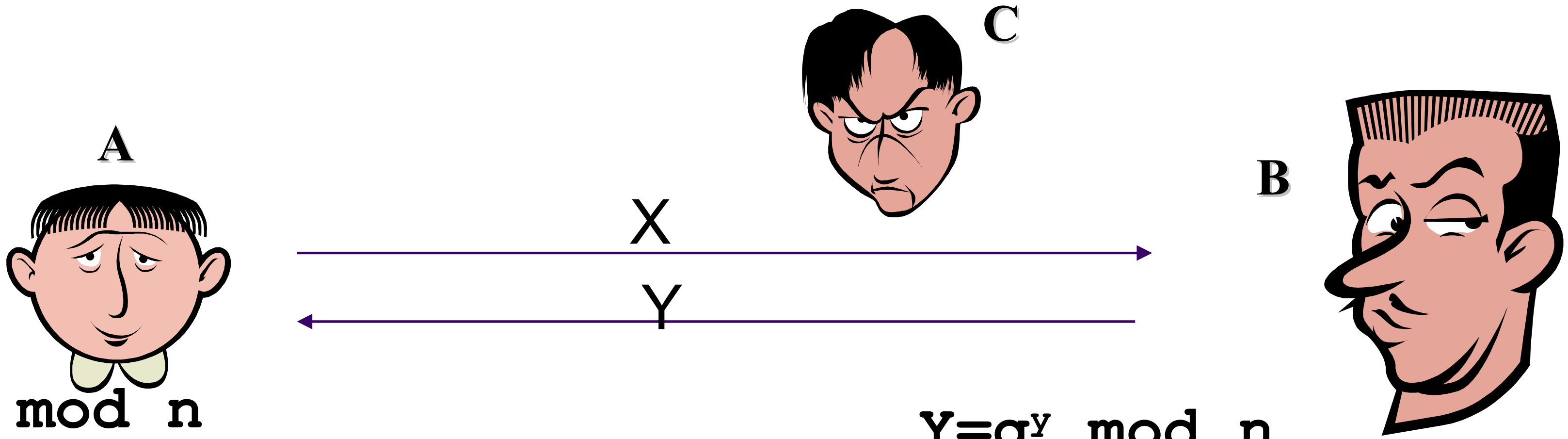
Handout 5 - Key Distribution

Kasun de Zoysa
kasun@ucsc.cmb.ac.lk

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

Diffie-Hellman Key Agreement

- Published in 1976
- Based on difficulty of calculating discrete logarithm in a finite field
- Two parties agreed on two large numbers n and g, such that g is a prime with respect to n



$X=g^x \bmod n$

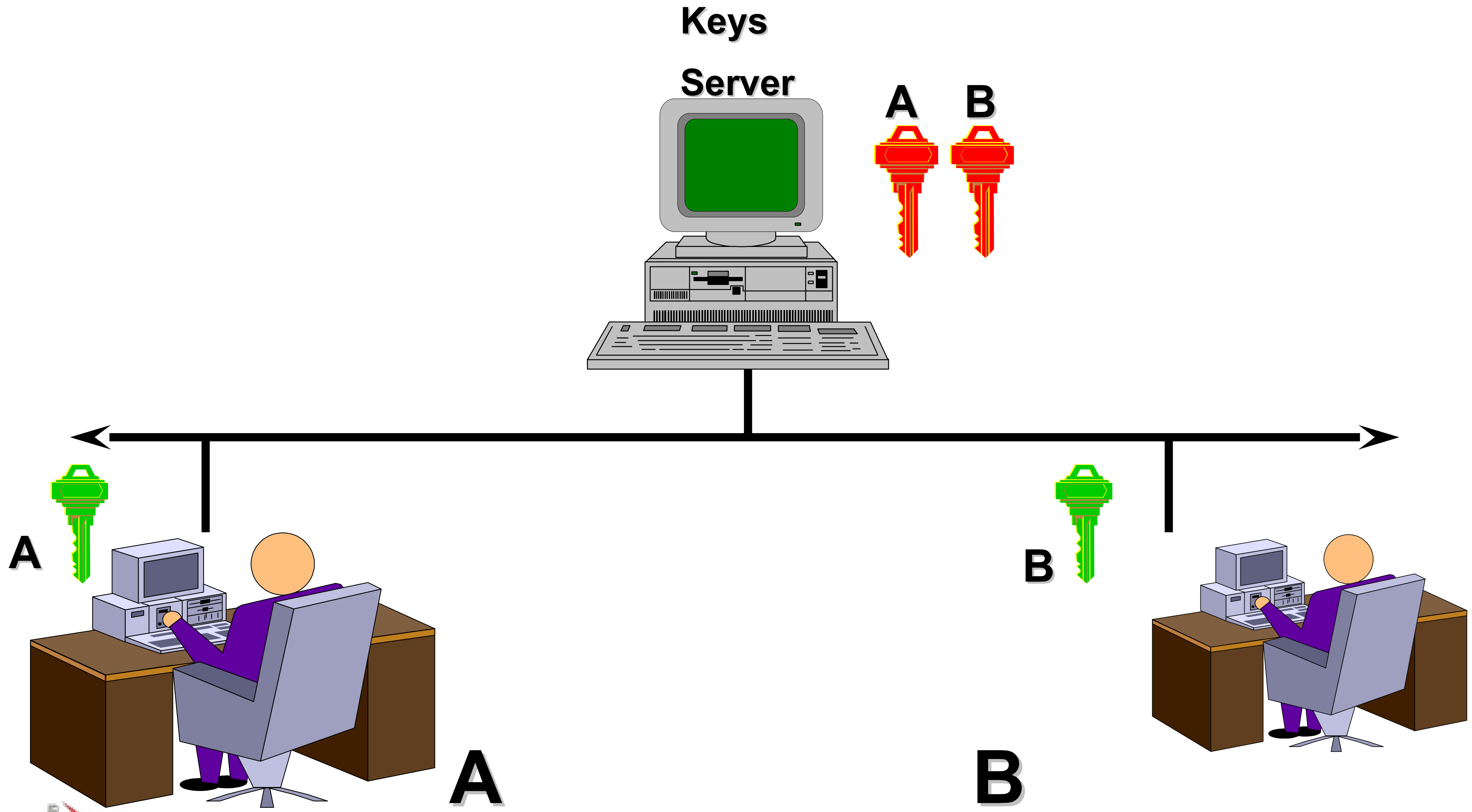
$k=Y^x \bmod n = g^{xy} \bmod n$

$Y=g^y \bmod n$

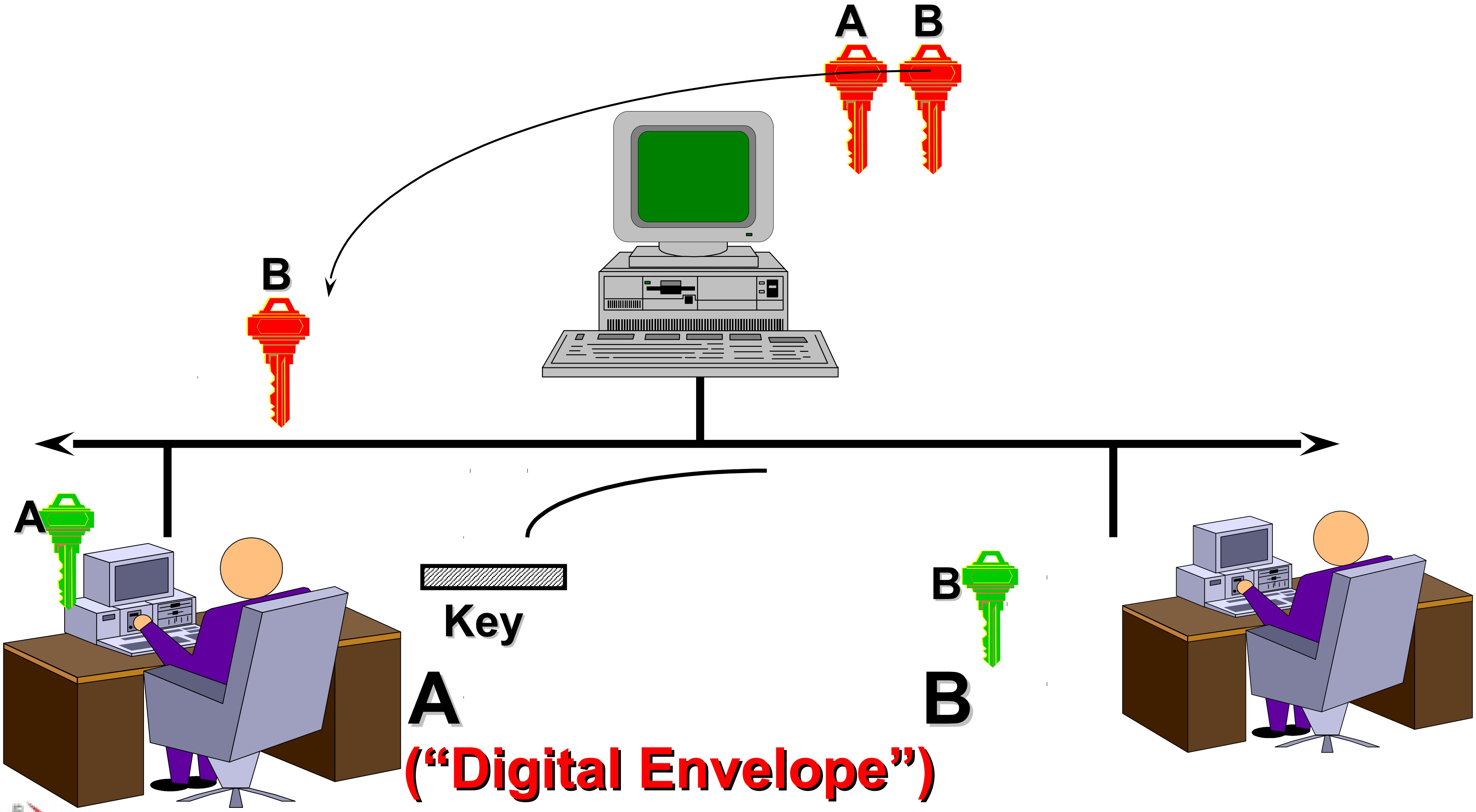
$k=X^y \bmod n = g^{xy} \bmod n$

Possible to do man in the middle attack

Storage and Handling Public Keys

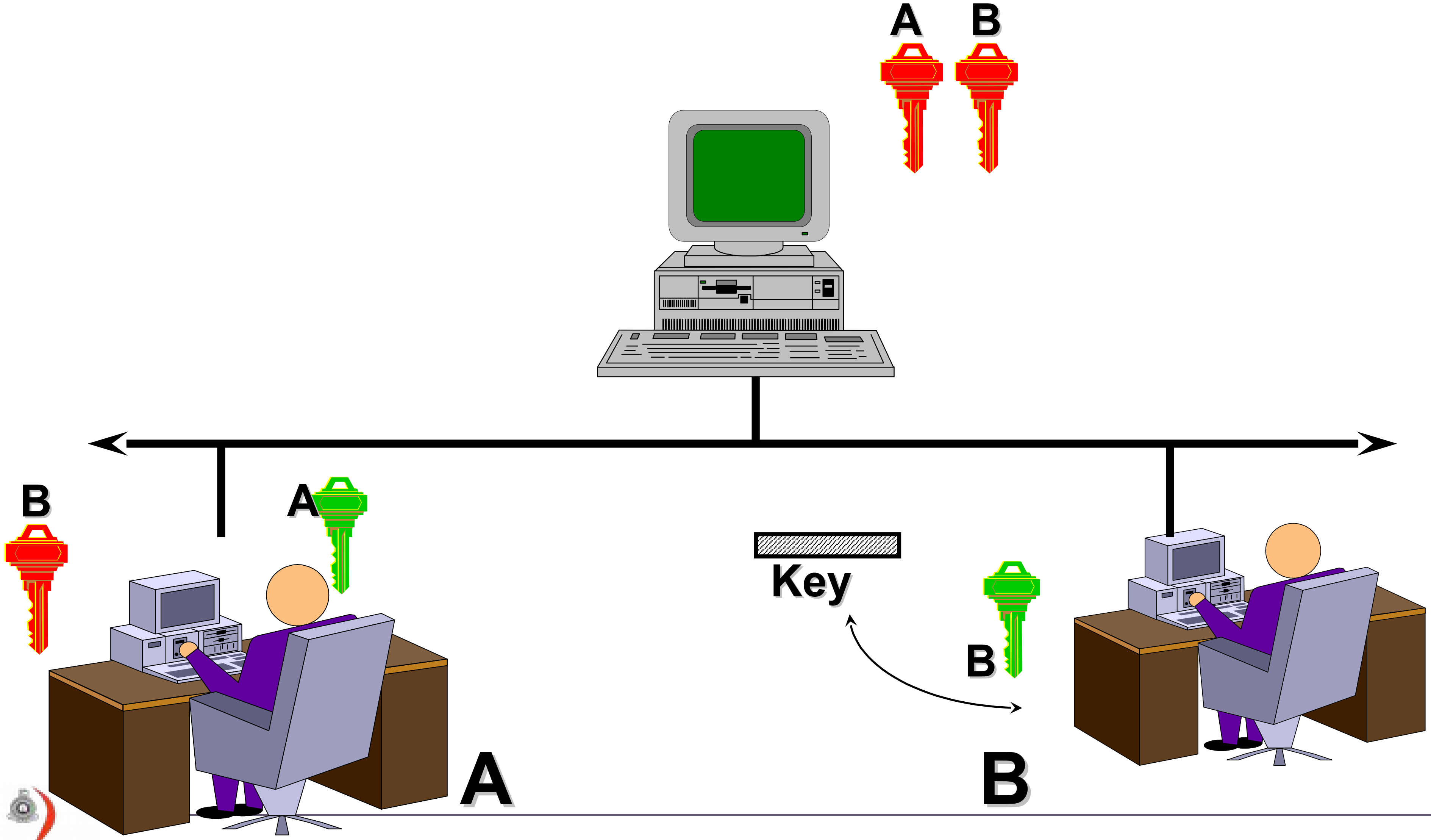


Secure Sending of secret key

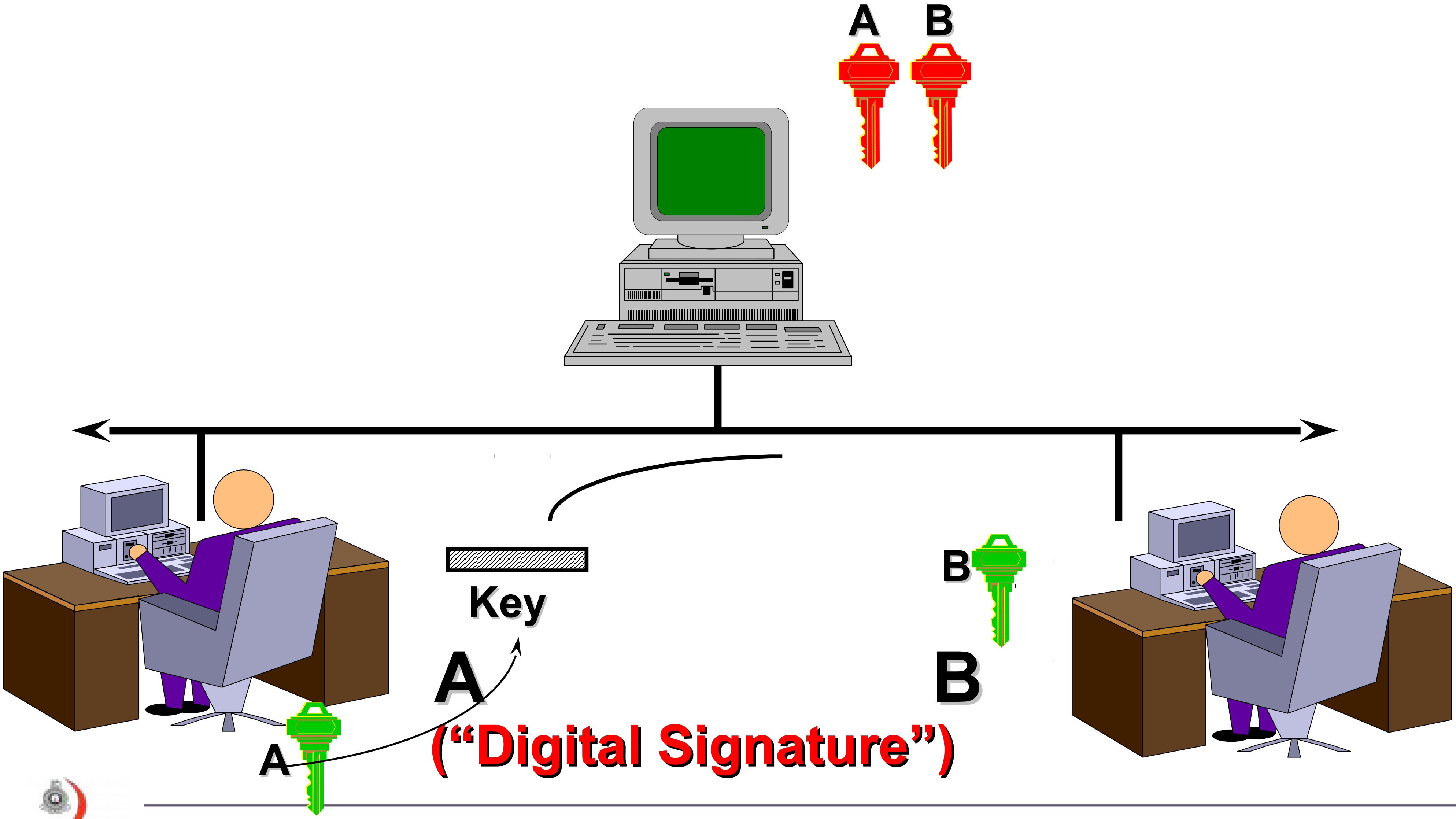


("Digital Envelope")

Recovery of Secret Key

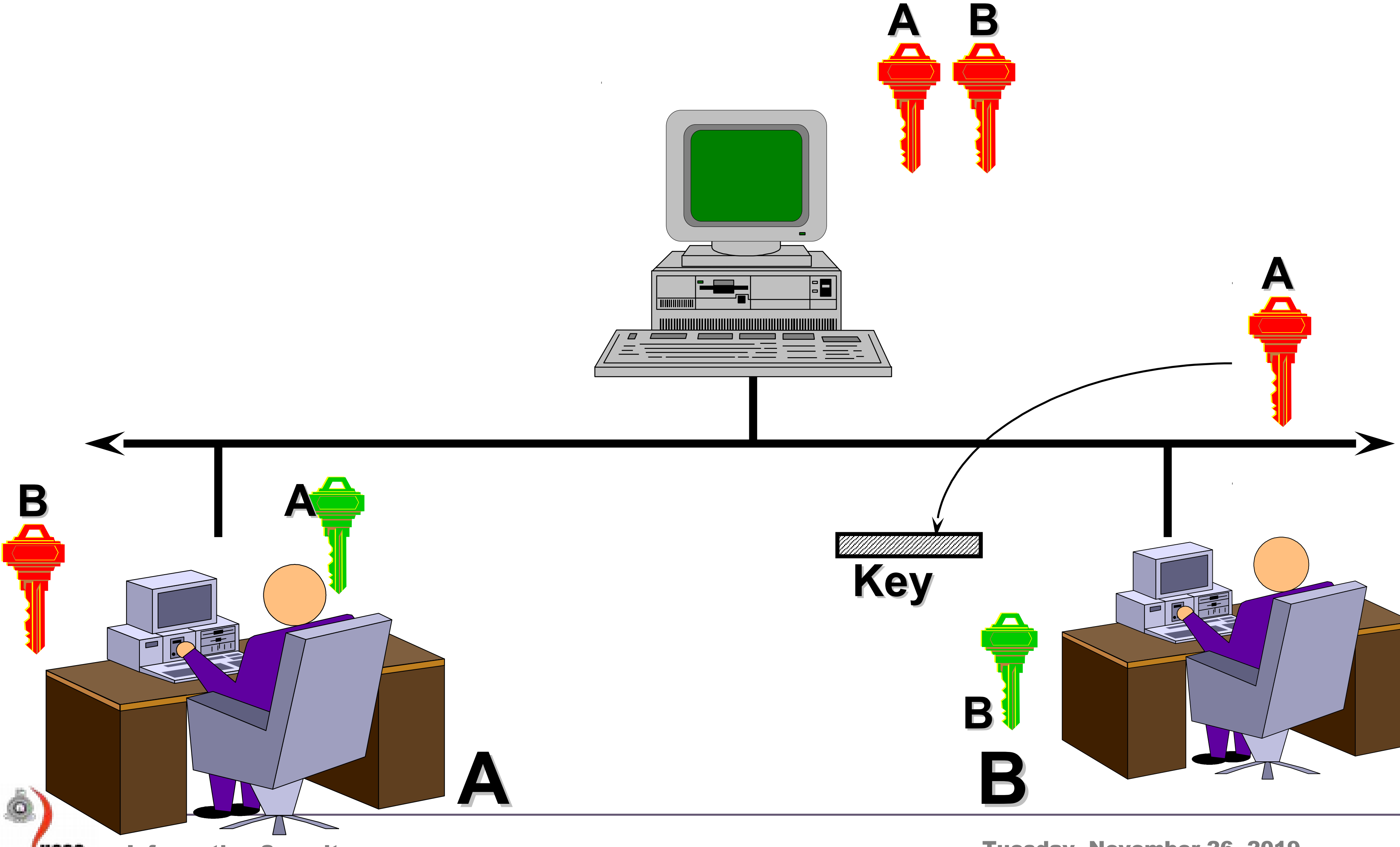


Authenticity of Sender

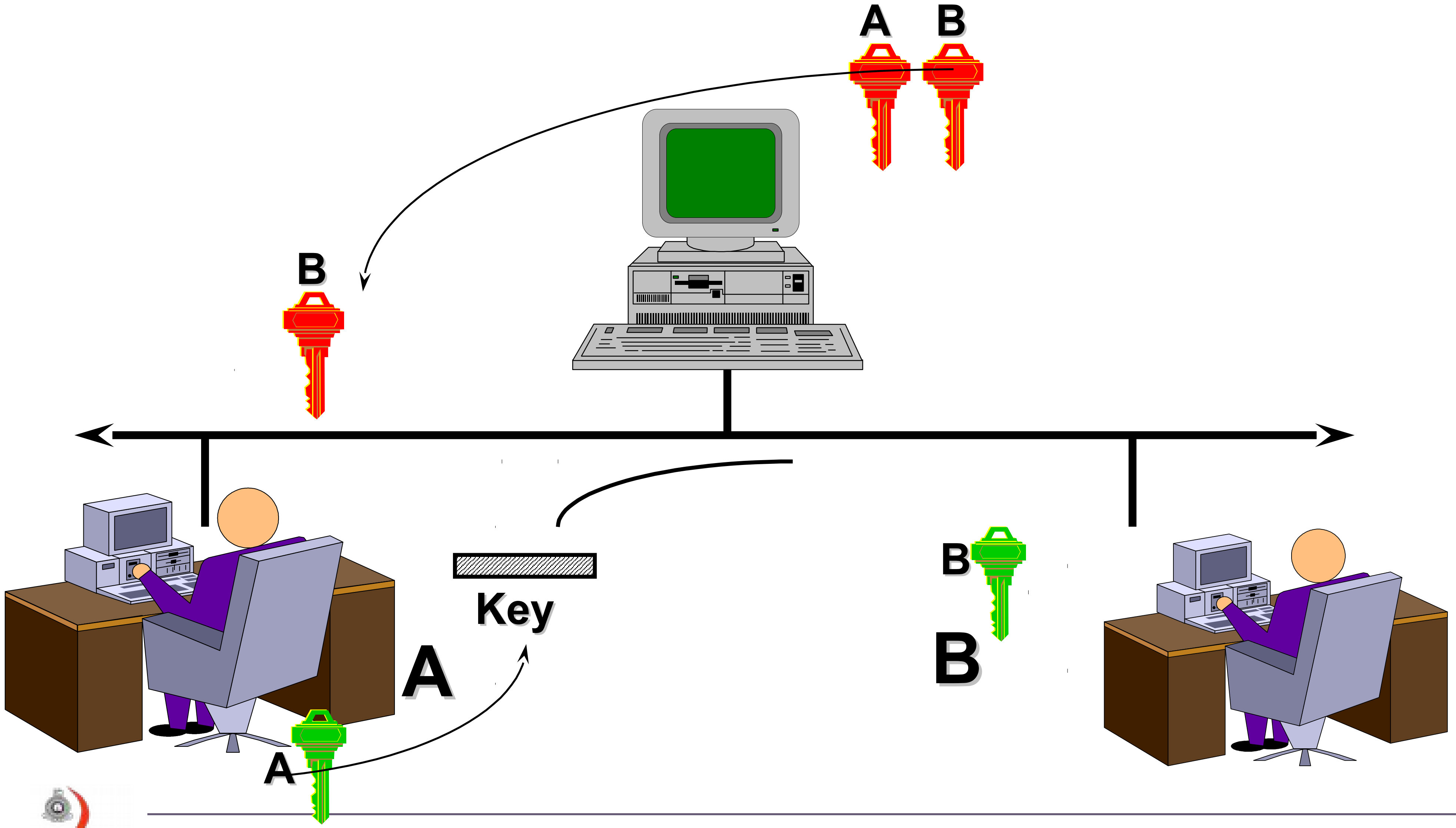


("Digital Signature")

Verification of Signature

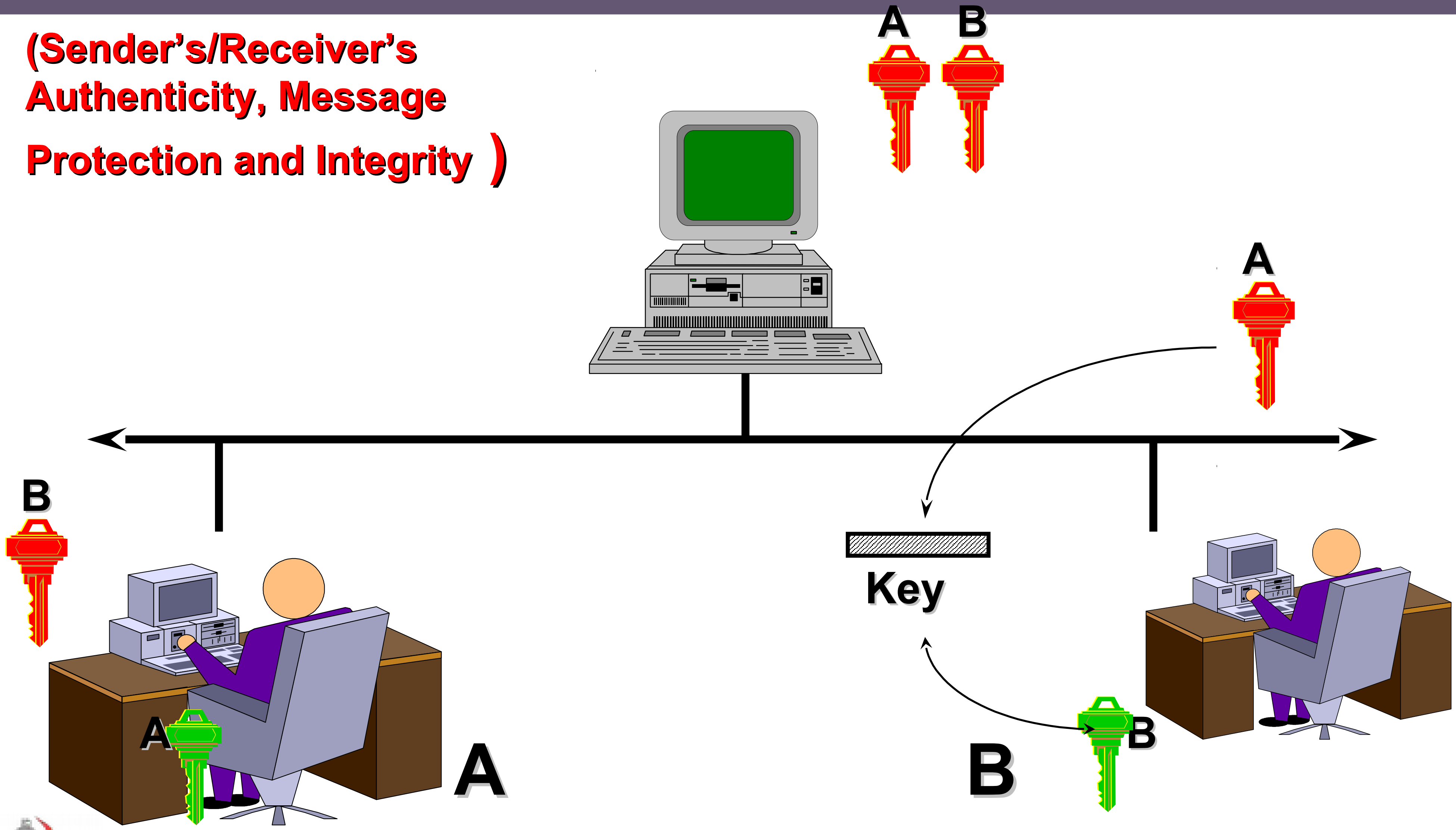


Authenticity of Sender and Receiver

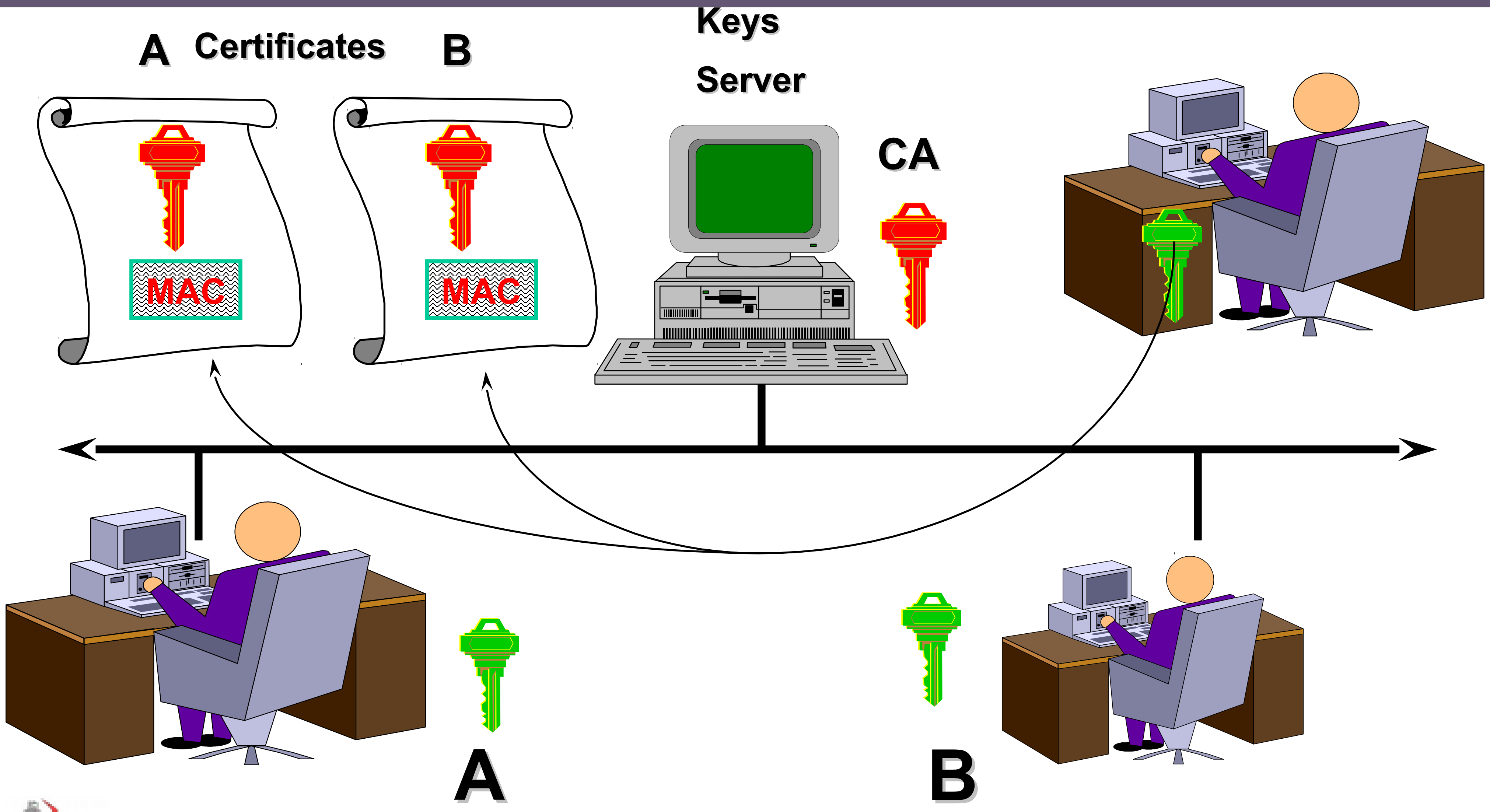


Full Verification

(Sender's/Receiver's Authenticity, Message Protection and Integrity)

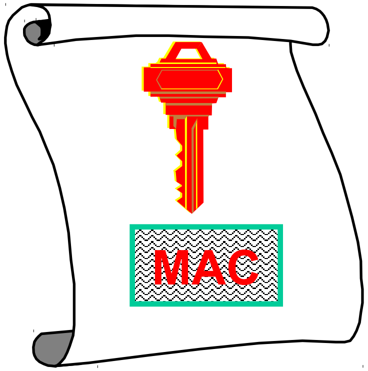


Certificate Authority



Internal Structure of Certificate

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Subject
- Validity
- Subject Public Key Information
- Extensions
- Signature

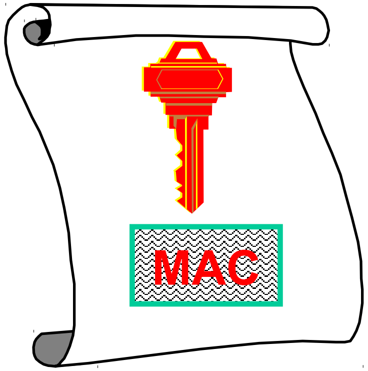


Structure of Distinguish Name

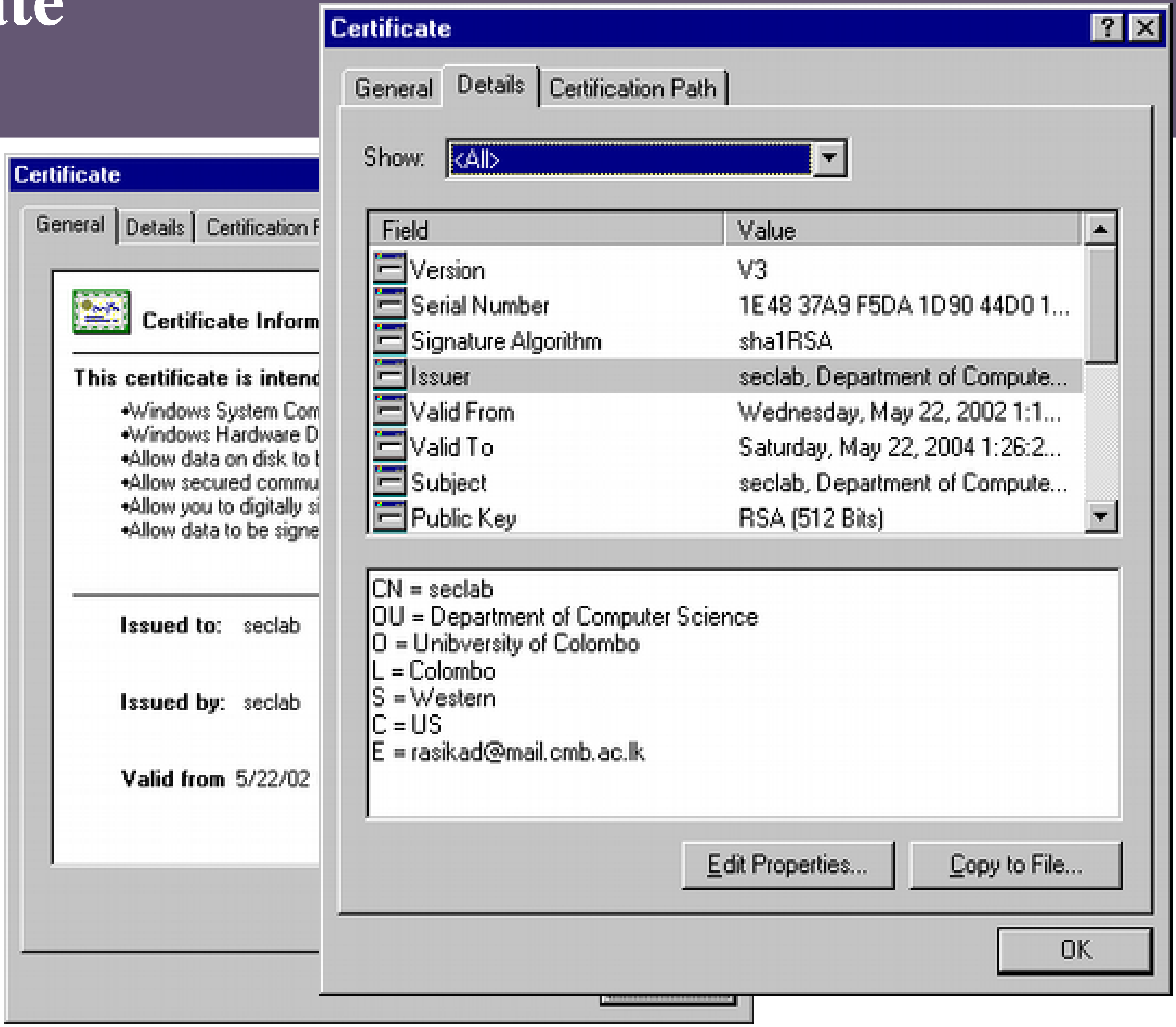
- Country Name
- State and Province Name
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- Email Address
- URL

Certificate Types

- Digital Signature
- Key Encipherment
- Data Encipherment
- Key Certificate Signature
- CRL Signature
- Object Signing



Root Certificate



This certificate is intend

- •Windows System Com
- •Windows Hardware D
- •Allow data on disk to b
- •Allow secured commu
- •Allow you to digitally si
- •Allow data to be signe

Issued to: seclab

Issued by: seclab

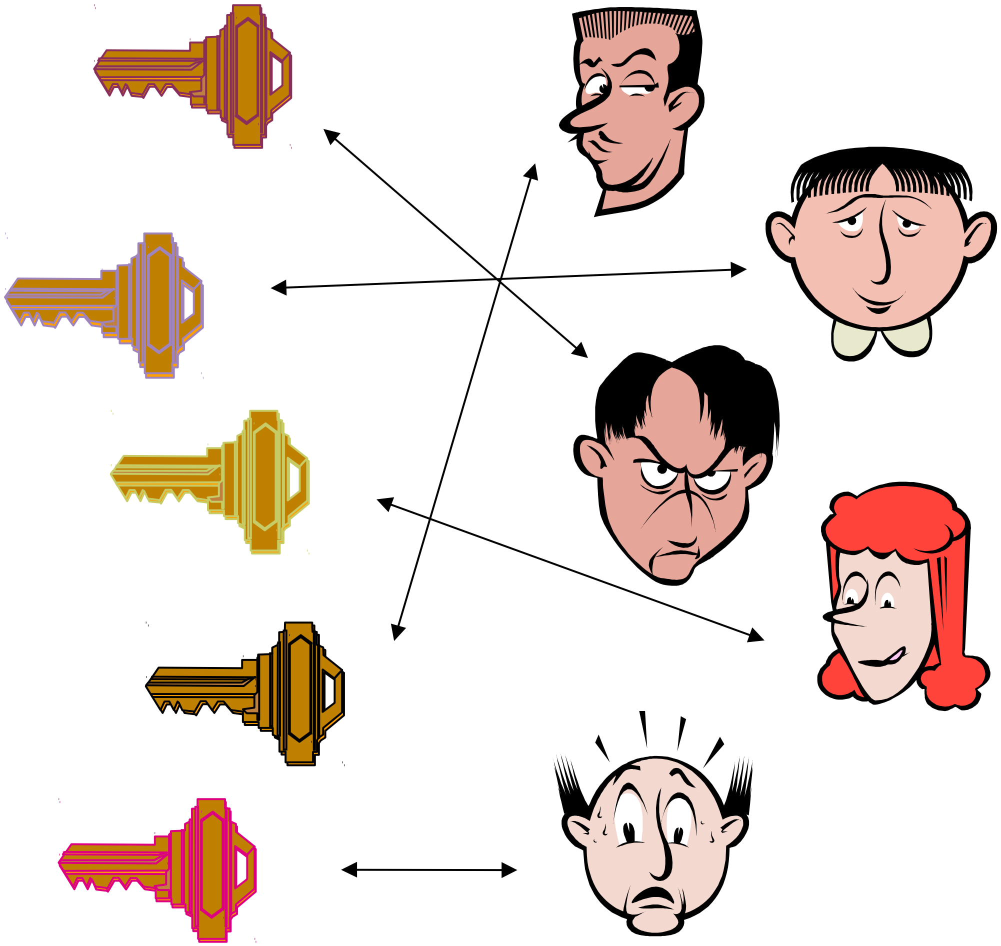
Valid from 5/22/02

Show: <All>

Field	Value
Version	V3
Serial Number	1E48 37A9 F5DA 1D90 44D0 1...
Signature Algorithm	sha1RSA
Issuer	seclab, Department of Compute...
Valid From	Wednesday, May 22, 2002 1:1...
Valid To	Saturday, May 22, 2004 1:26:2...
Subject	seclab, Department of Compute...
Public Key	RSA (512 Bits)

CN = seclab
OU = Department of Computer Science
O = Unibversity of Colombo
L = Colombo
S = Western
C = US
E = rasikad@mail.cmb.ac.lk

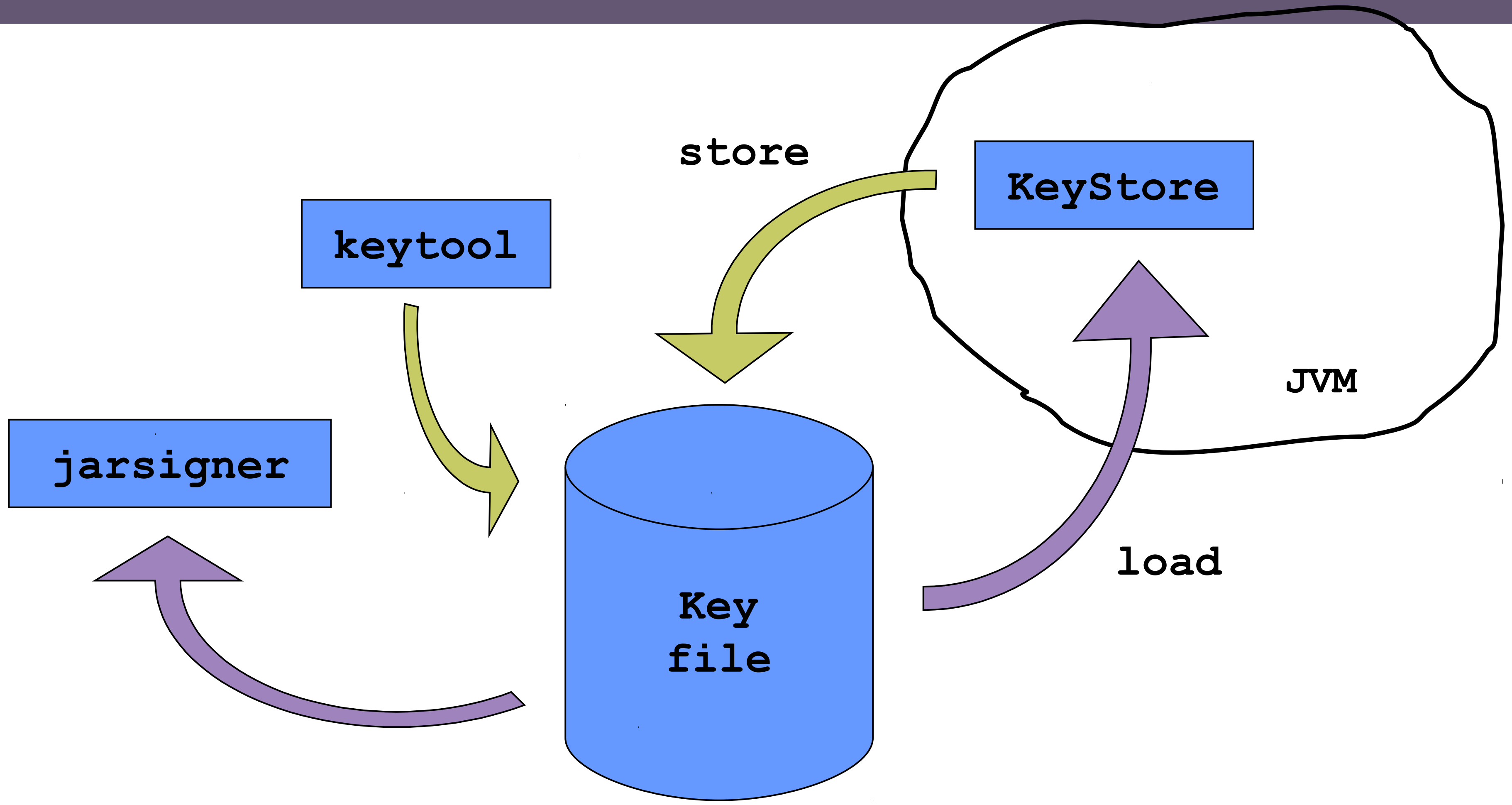
Key Management



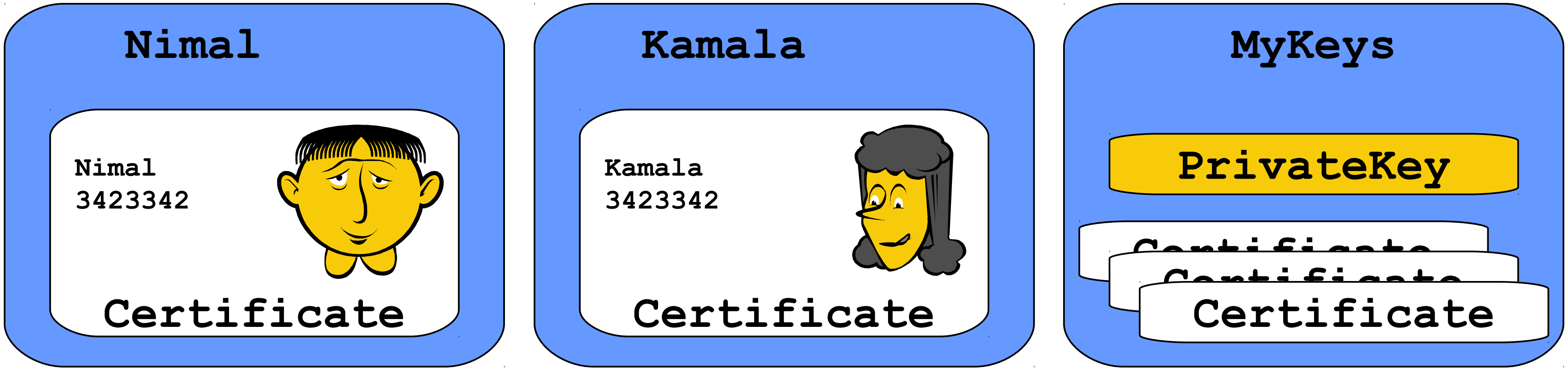
Key Management System:

- database for the public and private keys
- makes it easy to retrieve the key for a certain identity

Interactions with key database



Two types of entries:



Certificate entry

Key entry

Key Tool

Generate Self Signed Certificate

```
E:\JavaExamples\SSL>keytool -genkey -alias kasun
-keystore Key
```

List Entries

```
E:\JavaExamples\SSL>keytool -list -keystore Key
```

Export certificates

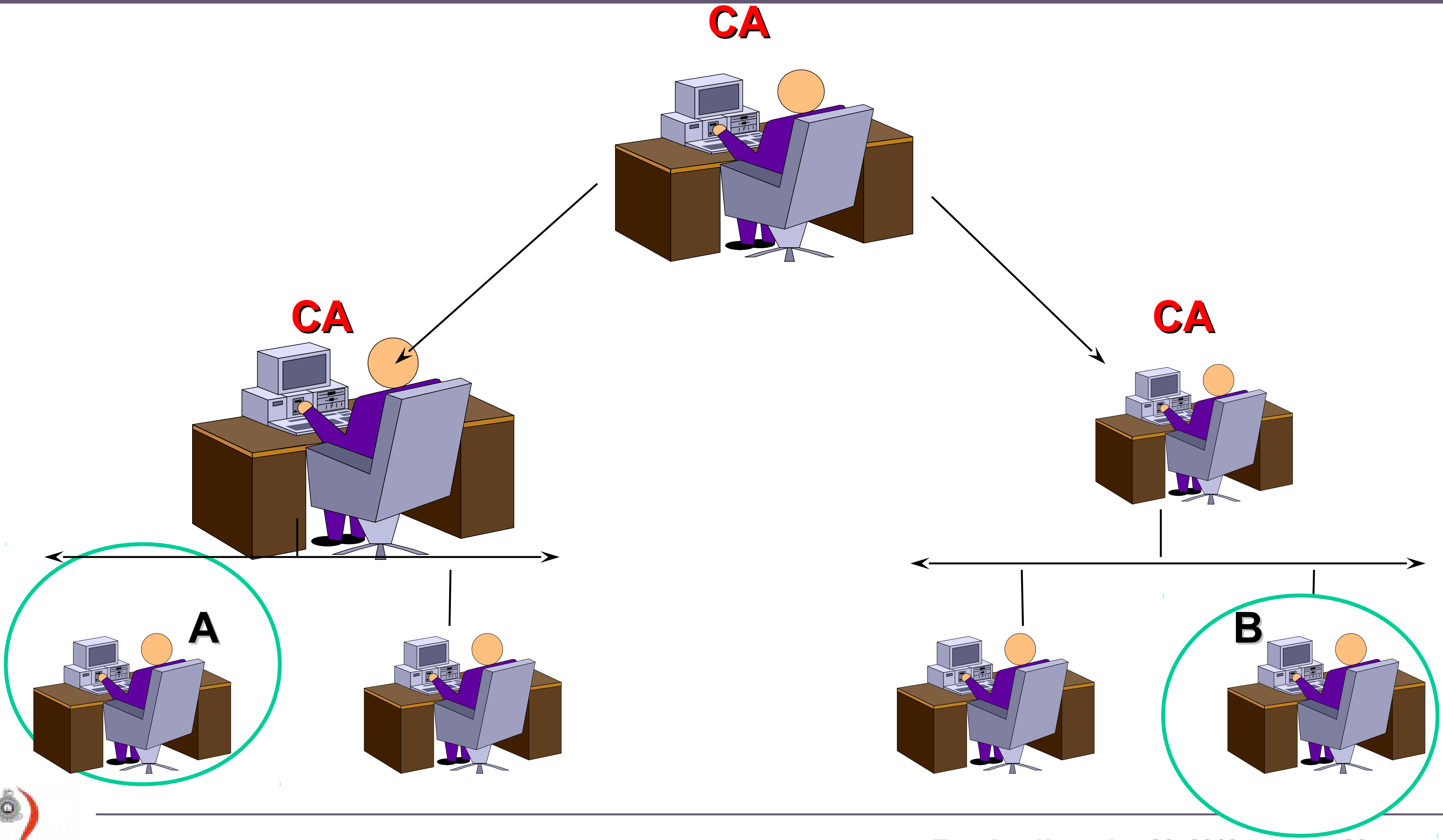
```
E:\JavaExamples\SSL>keytool -exportcert -keystore
Key -alias kasun -file cert.der
```

Public key infrastructure (PKI)

- Public key infrastructure (PKI) - provides the foundation necessary for secure e-business through the use of cryptographic keys and certificates
  - Enables secure electronic transactions
  - Enables the exchange of sensitive information

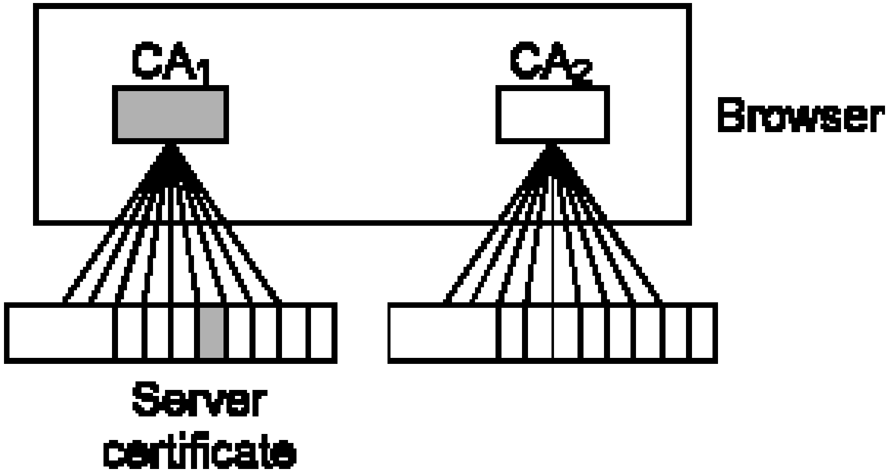
PKI

Certificate Hierarchy



CA Hierarchy in Practice

Flat or Clayton's hierarchy

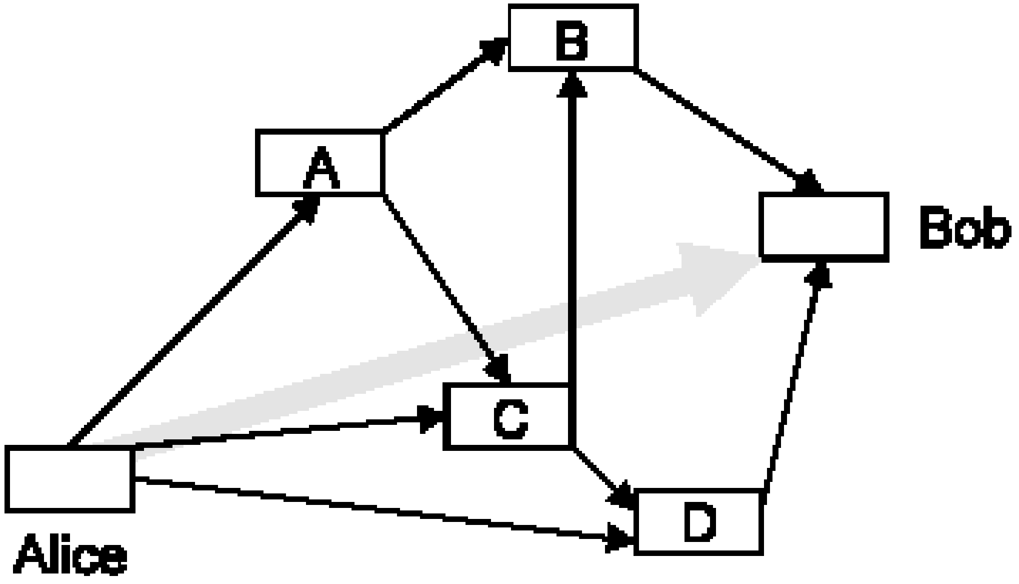


CA certificates are hard-coded into web browsers or email software

- Later software added the ability to add new CAs to the hardcoded initial set

Alternative Trust Hierarchies

PGP web of trust

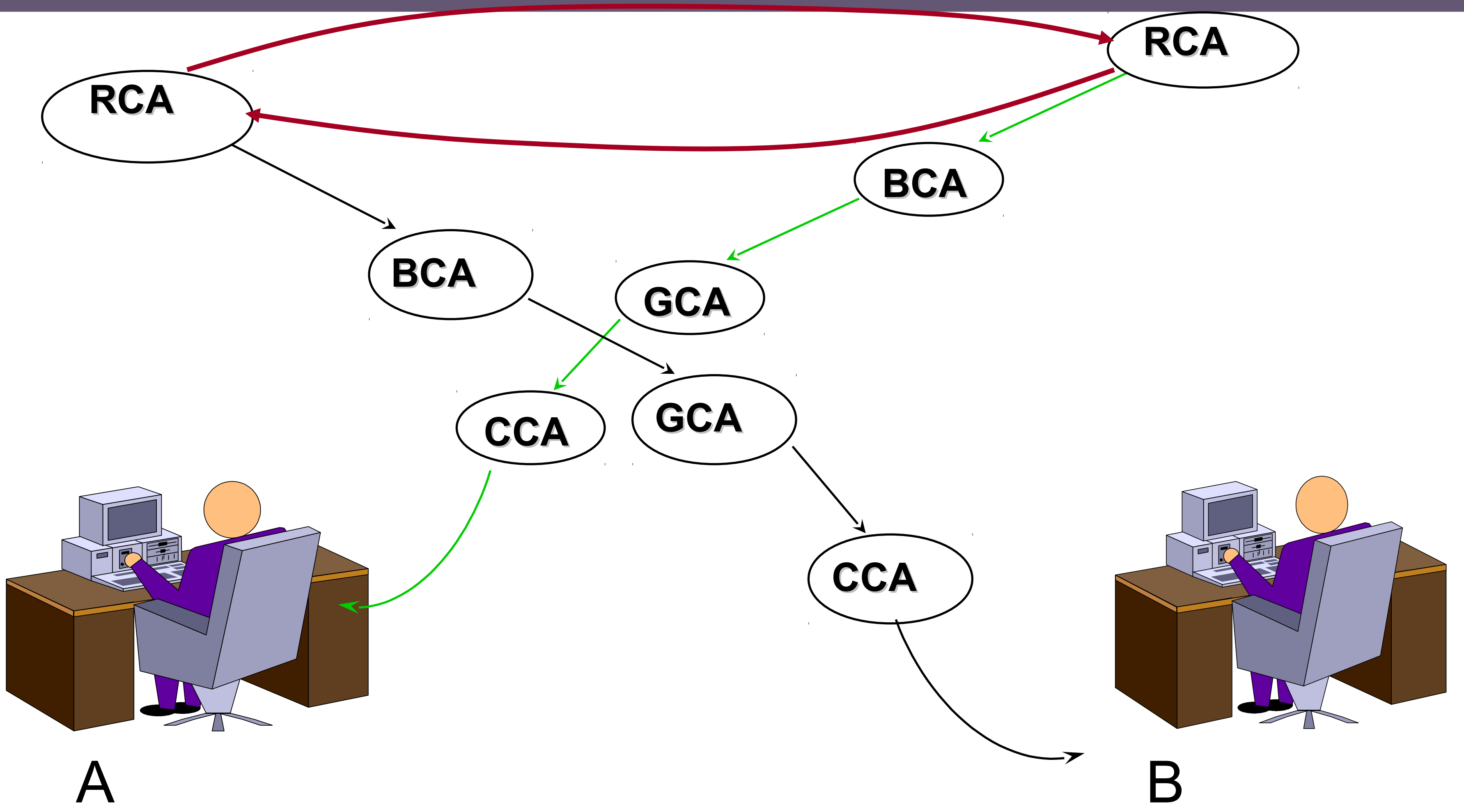


Bob knows B and D who know A and C who know Alice

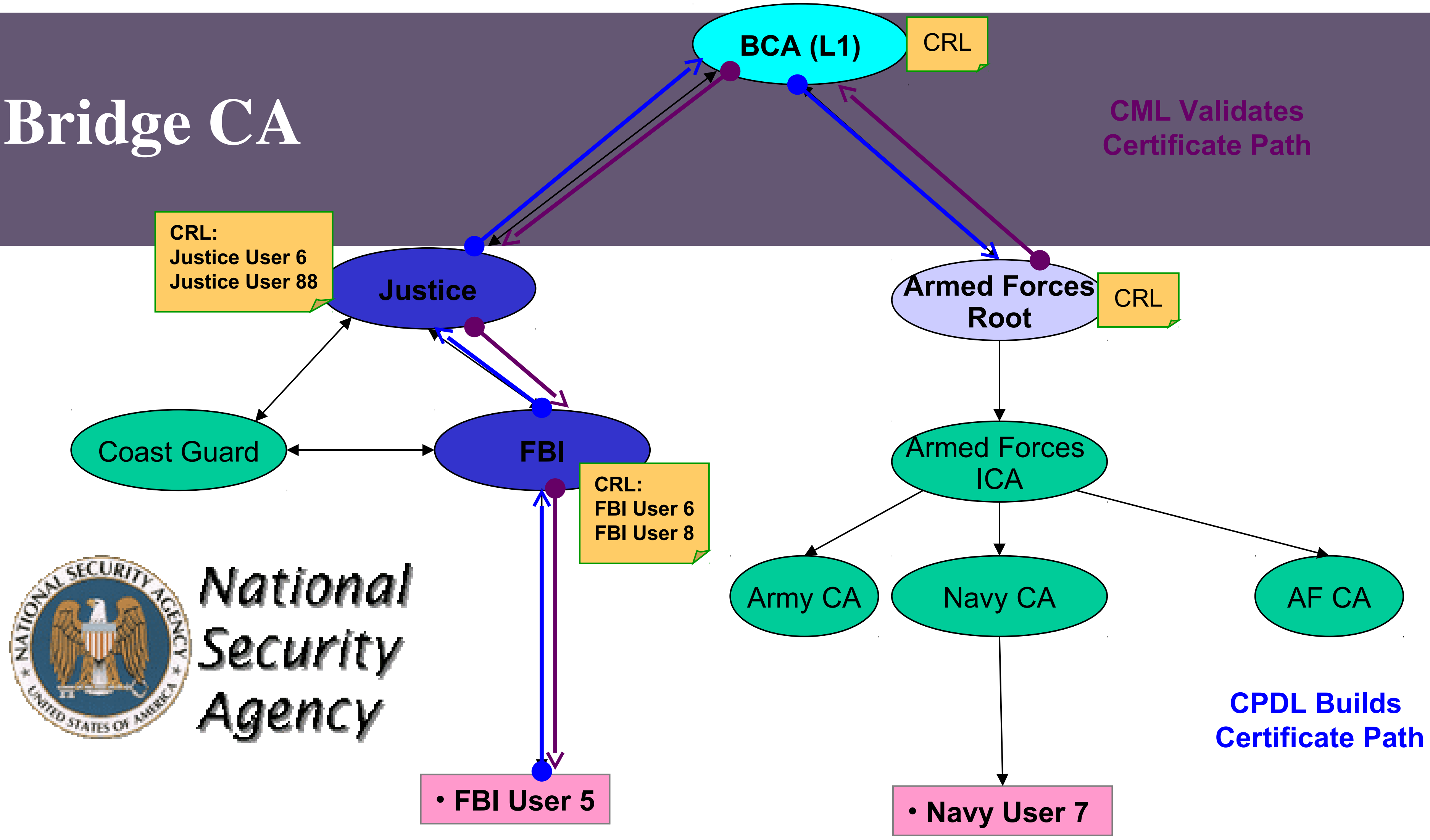
⇒ Bob knows the key came from Alice

Web of trust more closely reflects real-life trust models

Cross Certification



Bridge CA



Entrust User Signs and Transmits Encrypted Message to SPYRYUS User

✓ Original Message (Decrypted, Sig Verified)

SPYRUS User Verifies Entrust User Signature Cert, Verifies Signature, Decrypts and Displays Message

Certificate Revocation

- Revocation is managed with a Certificate Revocation List (CRL), a form of anti-certificate which cancels a certificate
- Equivalent to 1970s-era credit card blacklist booklets
- Relying parties are expected to check CRLs before using a certificate

– *“This certificate is valid unless you hear somewhere that it isn’t”*

CRL Distribution Problems

• CRLs have a fixed validity period
– Valid from *issue date* to *expiry date*
• At *expiry date*, all relying parties connect to the CA to fetch the
new CRL
– Massive peak loads when a CRL expires (DDOS attack)
• Issuing CRLs to provide timely revocation exacerbates the problem
– 10M clients download a 1MB CRL issued once a minute = ~150GB/s traffic
– Even per-minute CRLs aren’t timely enough for high-value transactions with interest calculated by the minute

Online Status Checking

•Online Certificate Status Protocol, **OCSP**

- Inquires of the issuing CA whether a given certificate is still valid
  - Acts as a simple responder for querying CRL’s
  - Still requires the use of a CRL to check validity
- OCSP acts as a selective CRL protocol

– Standard CRL process: “Send me a CRL for everything you’ve got”

– OCSP process: “Send me a pseudo-CRL/OCSP response for only these certs”

– Lightweight pseudo-CRL avoids CRL size problems

– Reply is created on the spot in response to the request

– Ephemeral pseudo-CRL avoids CRL validity period problems

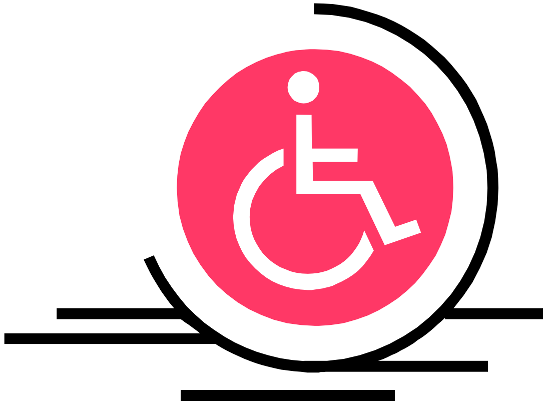
Online Certificate Status Protocol (OCSP)

- Returned status values are non-orthogonal

– Status = “good”, “revoked”, or “unknown”

– “Not revoked” doesn’t necessarily mean “good”

– “Unknown” could be anything from “Certificate was never issued” to “It was issued but I can’t find a CRL for it”



OCSP Problems

•Problems are due in some extent to the CRL-based origins of OCSP

– CRL can only report a negative result

– “Not revoked” doesn’t mean a cert was ever issued

– Some OCSP implementations will report “I can’t find a CRL” as “Good”

– Some relying party implementations will assume “revoked” “not good”, so any other status = “good”

– Much debate among implementors about OCSP semantics

Other Online Validation Protocols

- Simple Certificate Validation Protocol (SCVP)
  - Relying party submits a full chain of certificates
  - Server indicates whether the chain can be verified
  - Aimed mostly at thin clients
- Data Validation and Certification Server Protocols (DVCS)
  - Provides facilities similar to SCVP disguised as a general third-party data validation mechanism
- Integrated CA Services Protocol (ICAP)
- Real-time Certificate Status Protocol (RCSP)
- Web-based Certificate Access Protocol (WebCAP)
- Delegated Path Validation (DPV)

– Offshoot of the SCVP/DVCS debate and an OCSP alternative OCSP-X

Discussion