Security of Information System

Applied Cryptography Protocols and Practice

Nandika Kasun

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

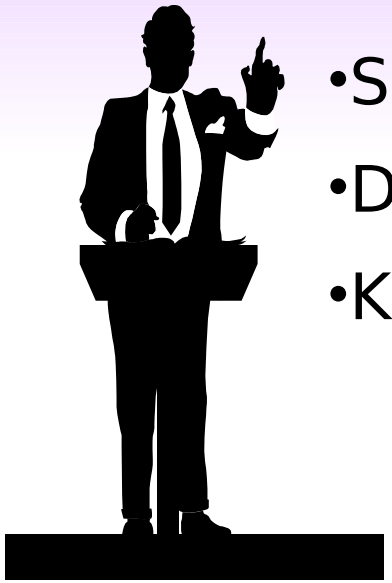
Objectives:

Applied Cryptography, Protocol and Practice

- Describe different key management protocols
- Understand the concept of public key infrastructure and related technologies
- Describe the advance cryptographic protocols
- Understand the legal issues related to security of information systems

kasun@cmb.ac.lk

Applied Cryptography Protocols and Practice



3.1 Key Management Protocols

- Solving Key Distribution Problem
- Diffie-Hellman Algorithm
- Key Exchange with Public Key Cryptography

kasun@cmb.ac.lk

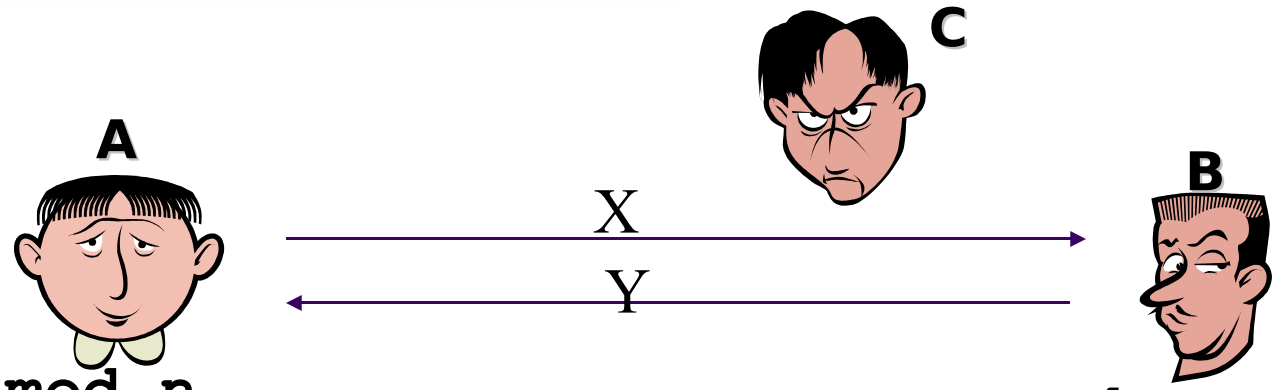
Key Distribution Problem

Kamla and Amal would like to communicate in absolute security in the presence of an eavesdropper, Nimal.

To do so, they need to share a common random string of number----key 

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



$X=g^x \bmod n$

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

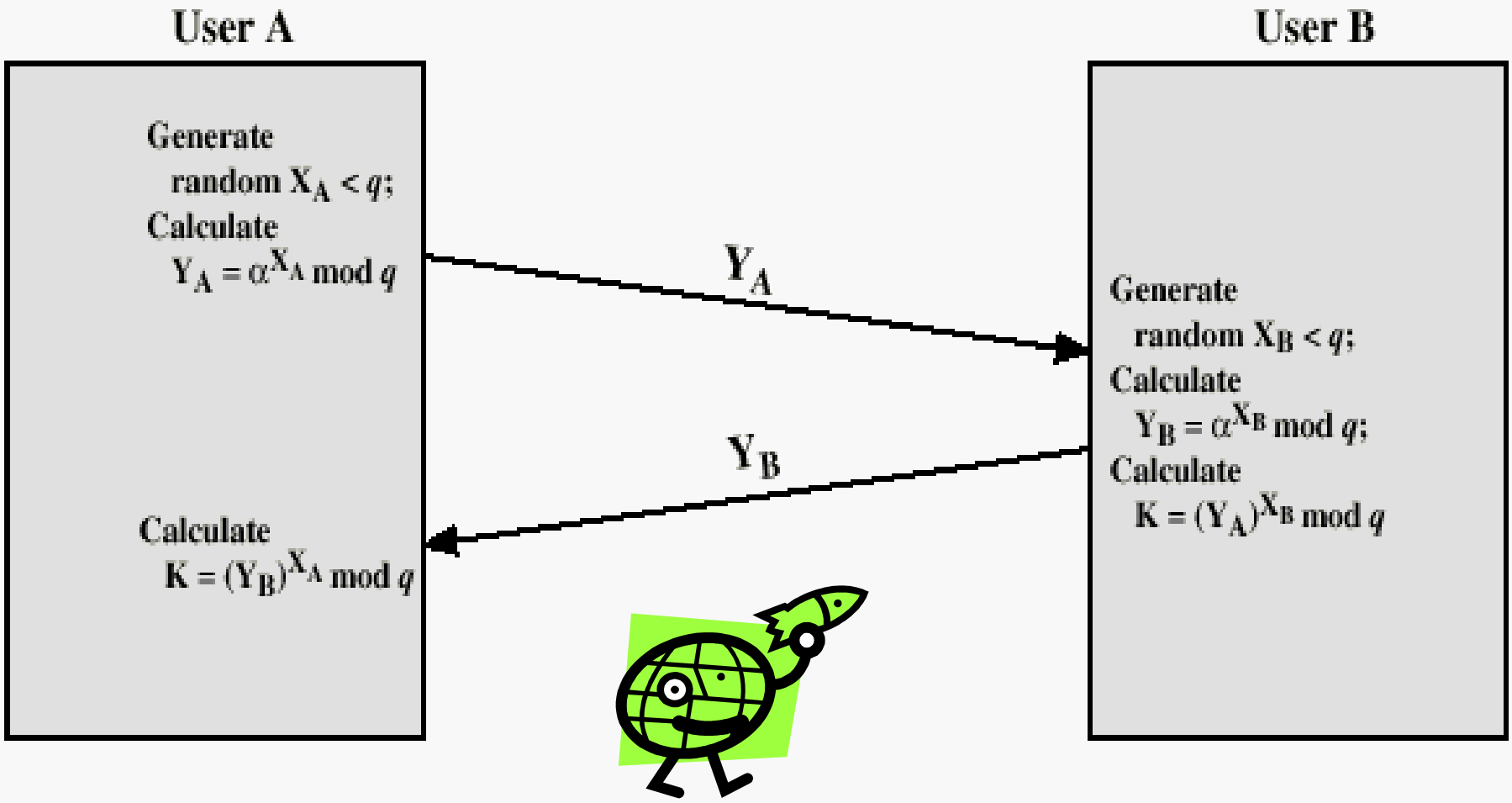
$Y=g^y \bmod n$

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

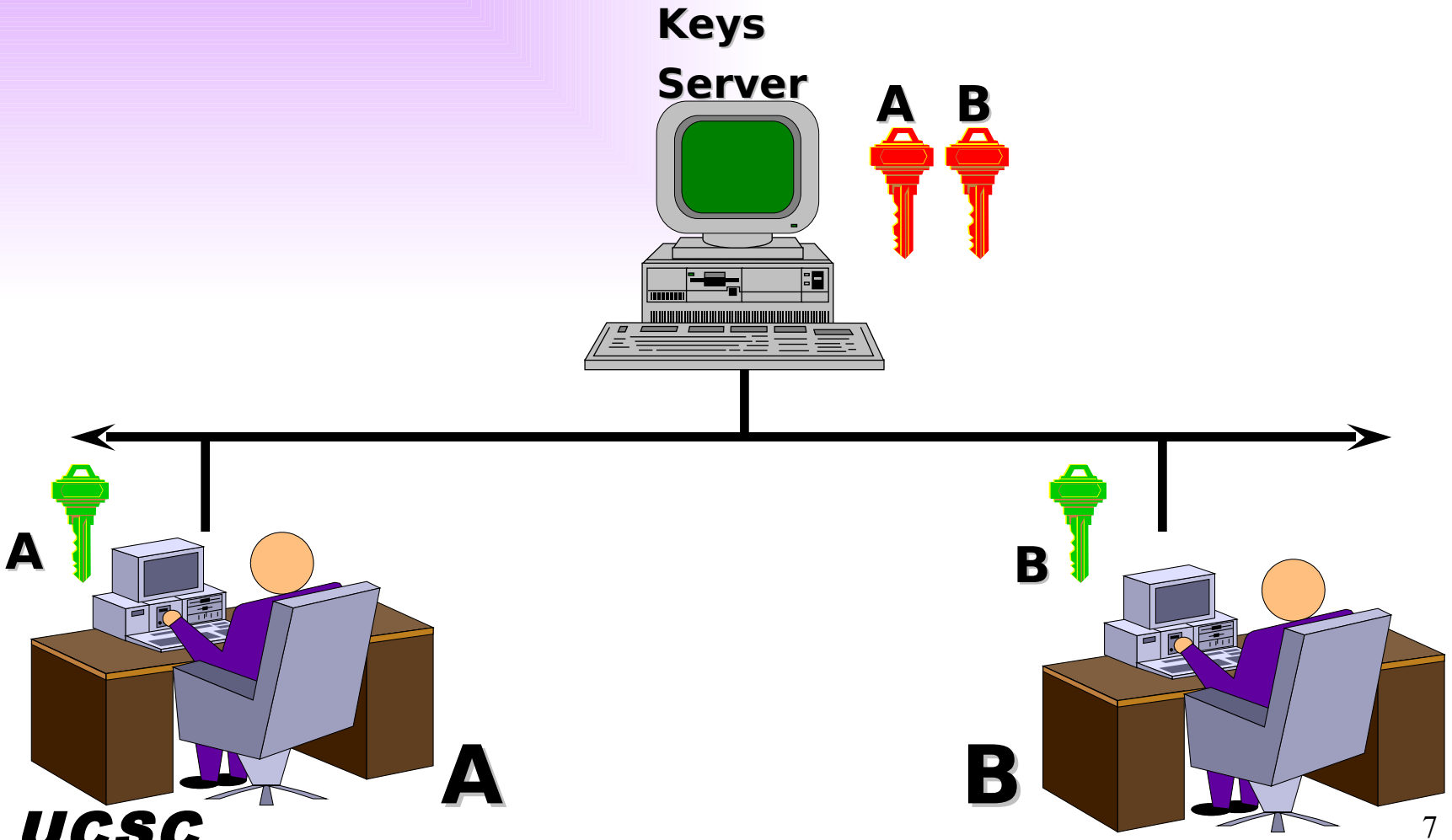
Possible to do man in the middle attack

kasun@cmb.ac.lk

Diffie-Hellman Key Exchange

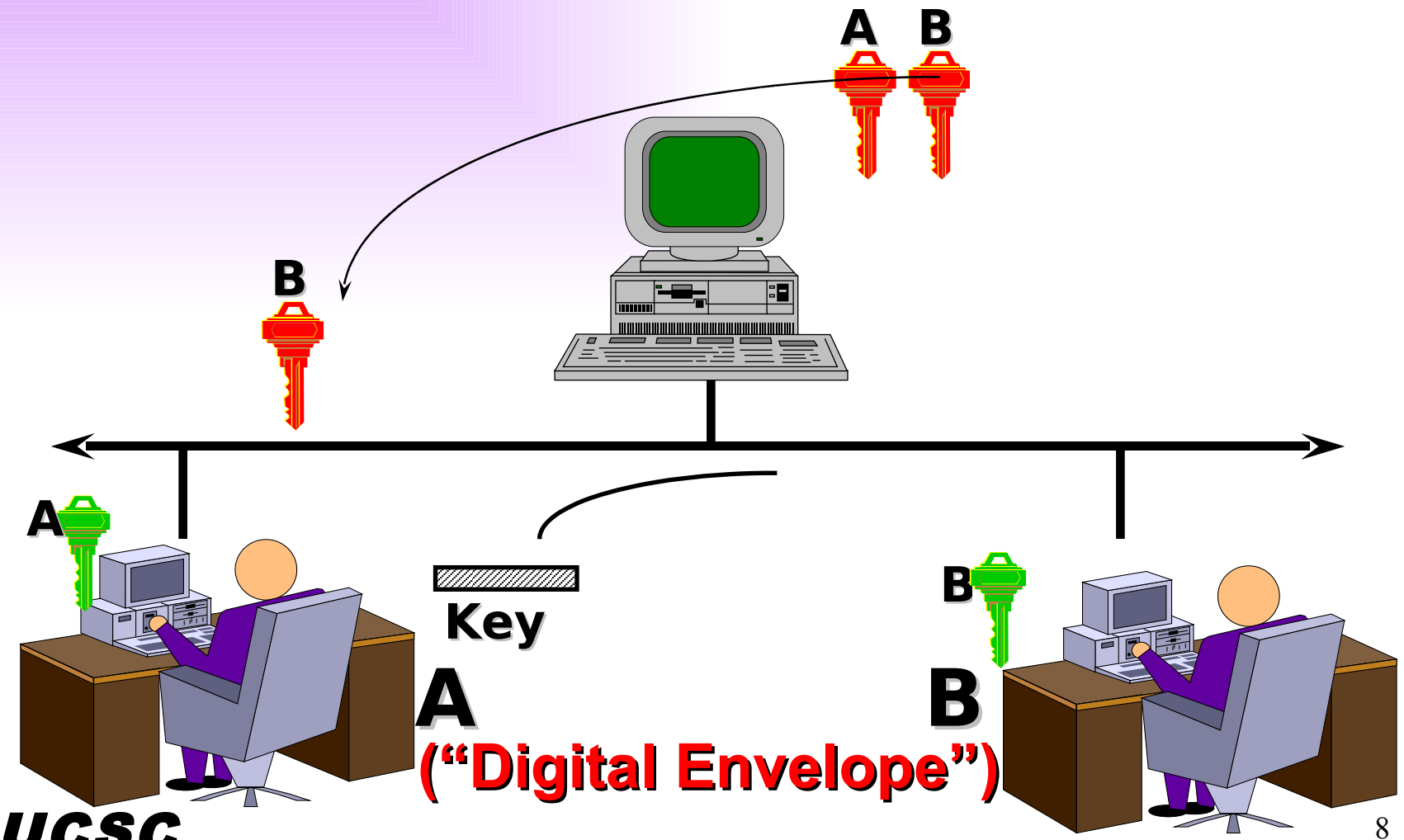


Storage and Handling Public Keys



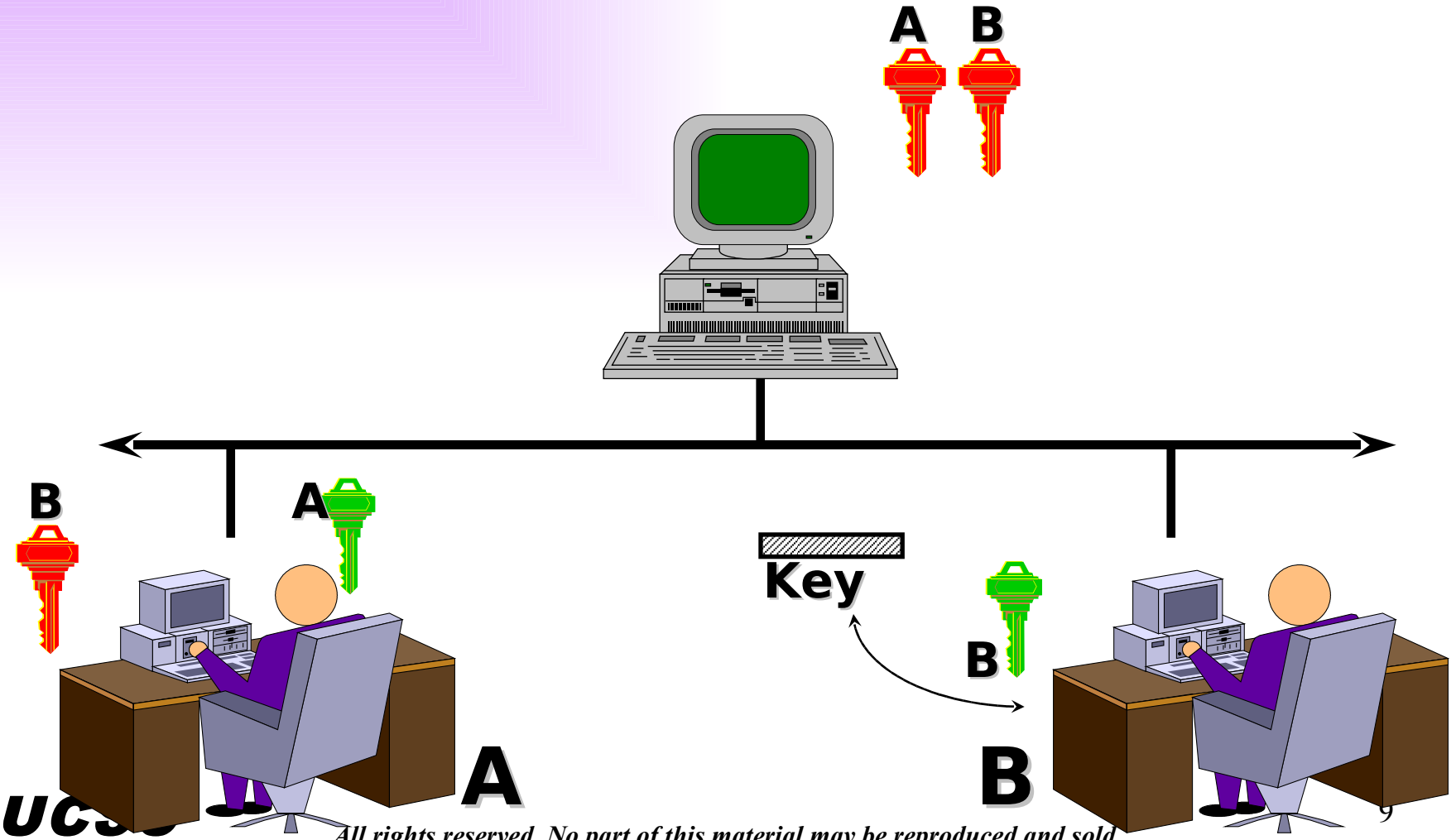
kasun@cmb.ac.lk

Secure Sending of secret key



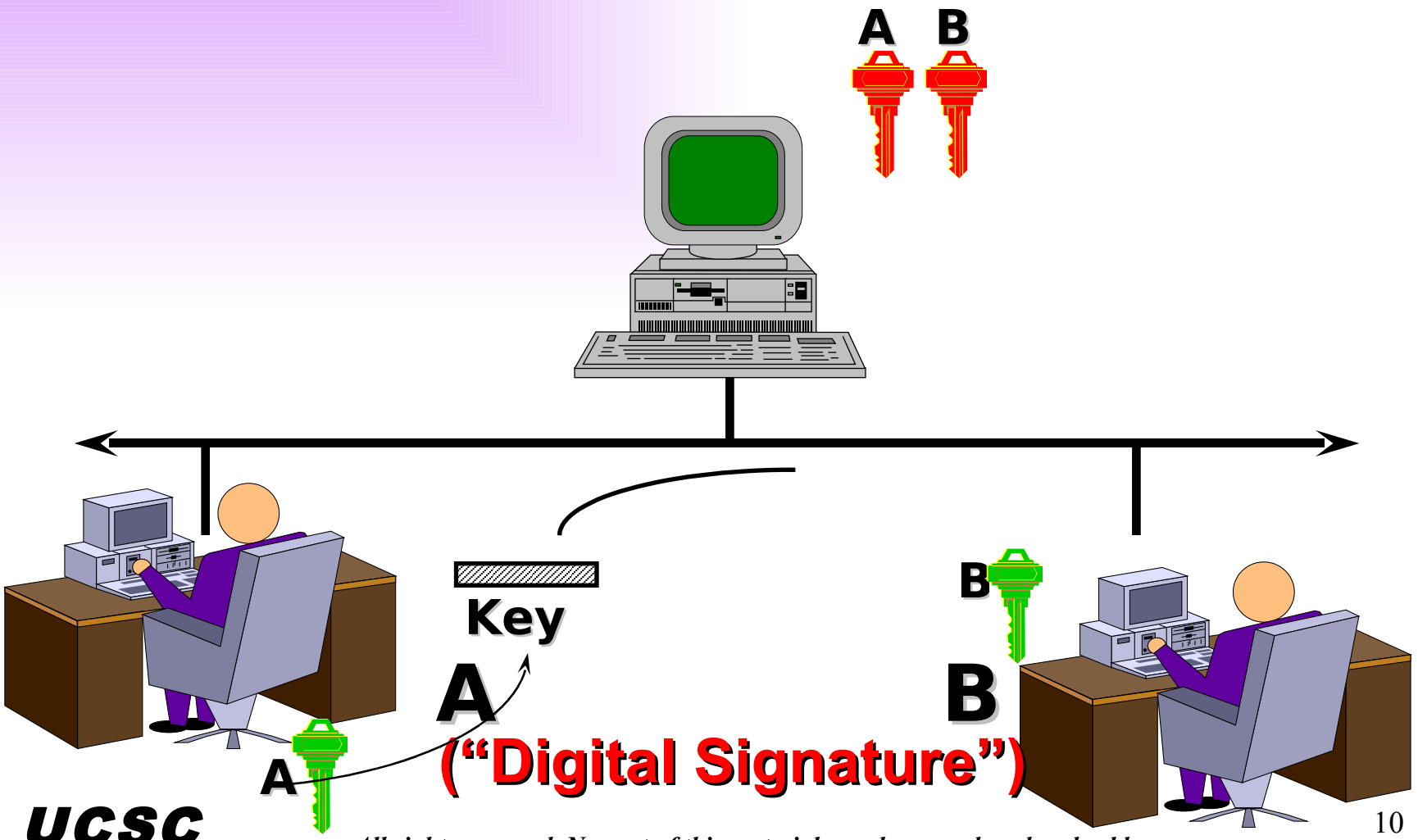
kasun@cmb.ac.lk

Recovery of Secret Key

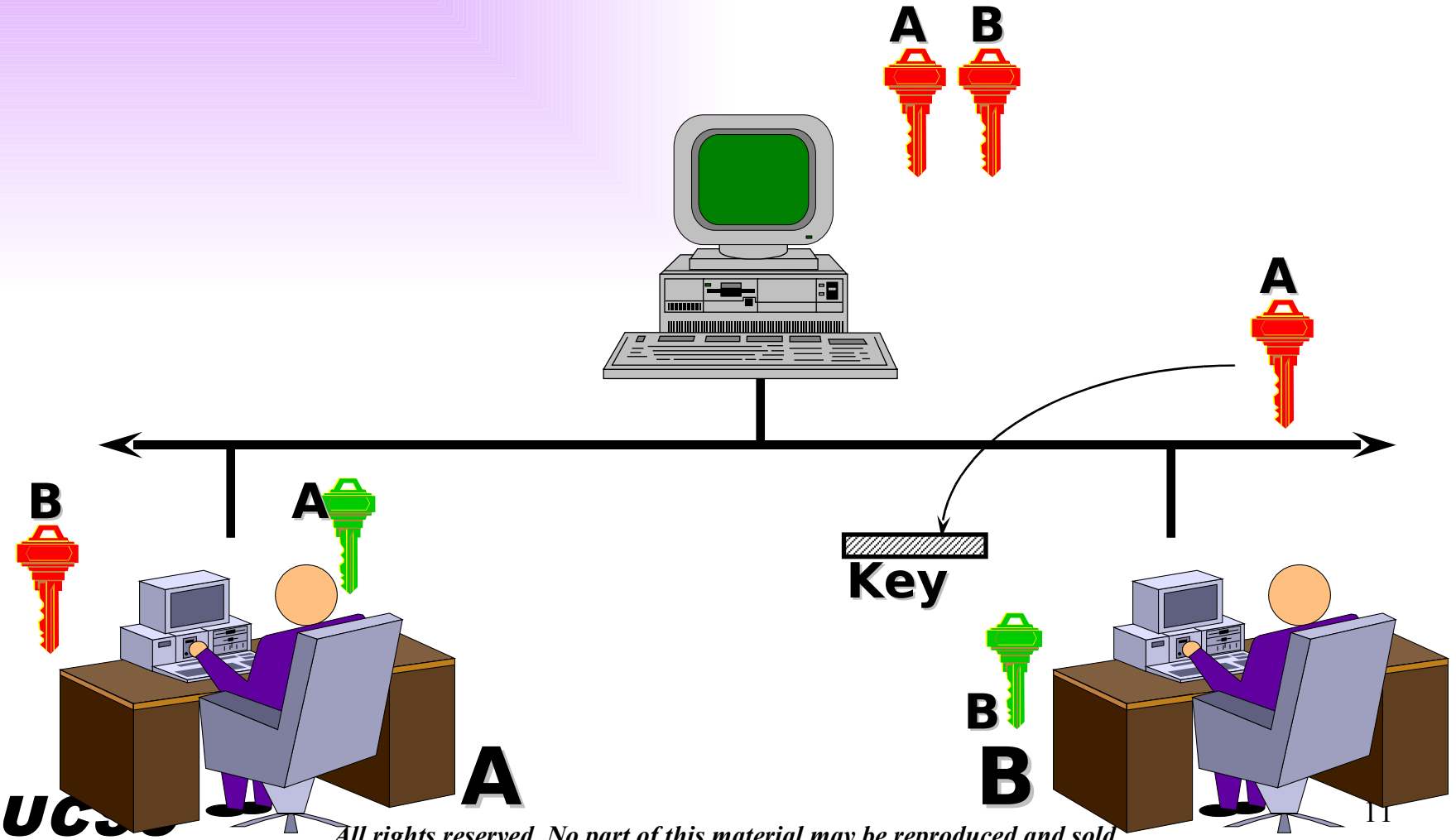


kasun@cmb.ac.lk

Authenticity of Sender

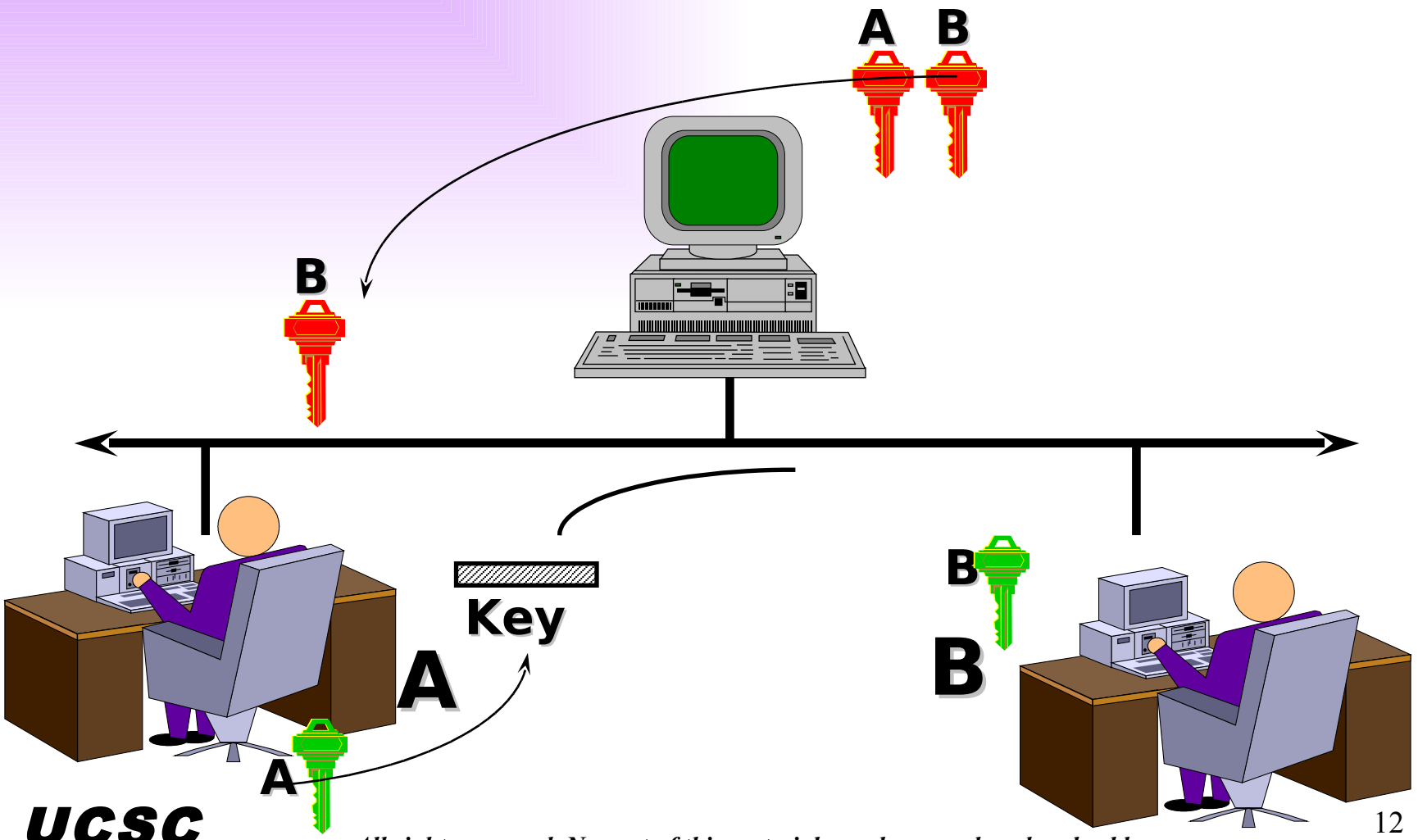


Verification of Signature



kasun@cmb.ac.lk

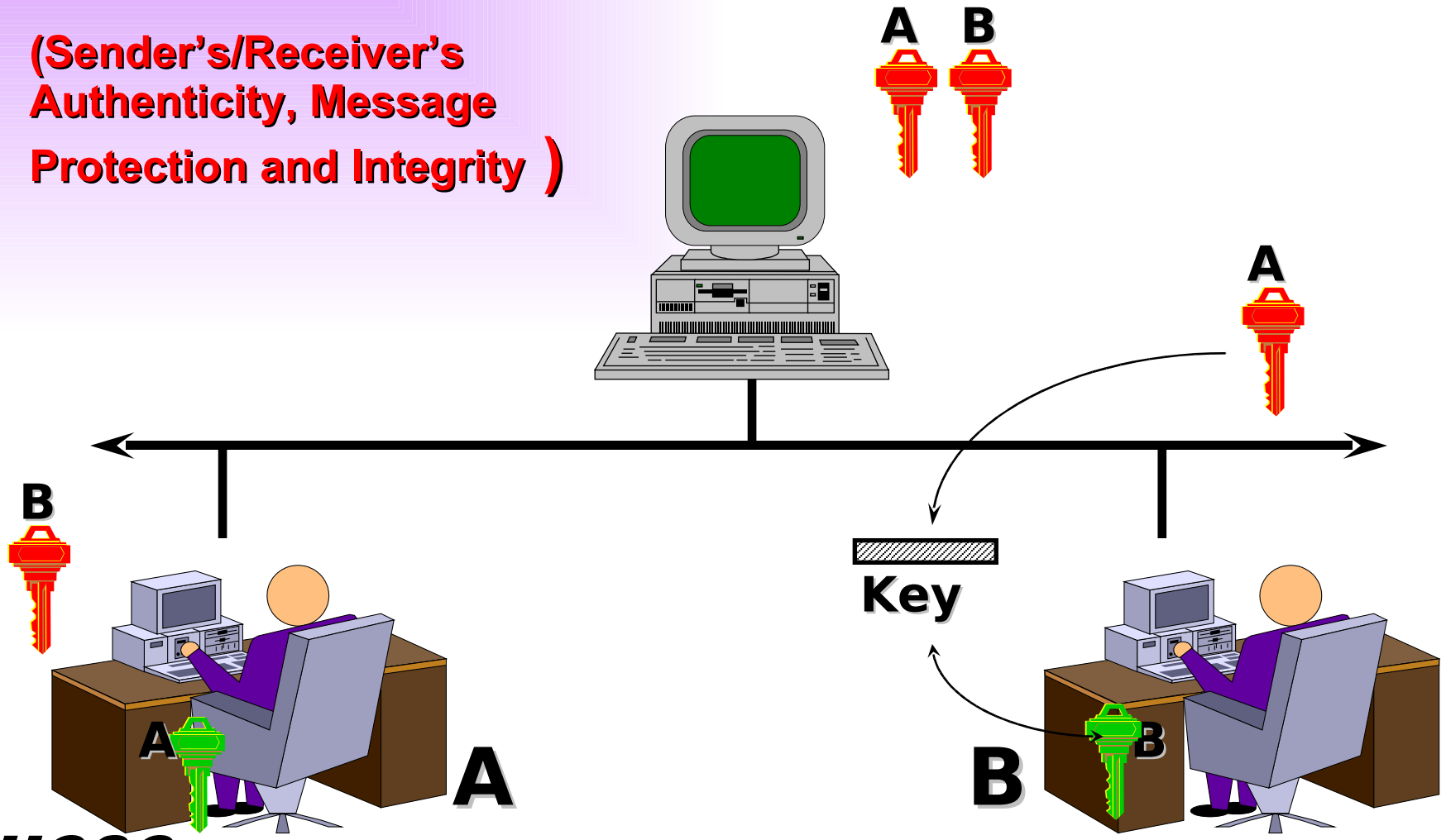
Authenticity of Sender and Receiver



UCSC
kasun@cmb.ac.lk

Full Verification

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



UCSC
kasun@cmb.ac.lk

Applied Cryptography Protocols and Practice

3.2 Public Key Infrastructure (PKI)

- Concept of Digital Certificate
- Certificate Authorities and it's roles
- Digital Certificates
- Types of Public Key Infrastructures

Public Key Infrastructure (PKI)

Main cryptographic tools, PKI

How to distribute public keys ?

⇒ Public Key Server (PKS), key exchange protocols

Public Key Infrastructure (PKI):

PKI = N x (Entities with private keys) + public key exchange system

REM: Public Key algorithms are slow

⇒ Need to use both Public & Secret Key Cryptography

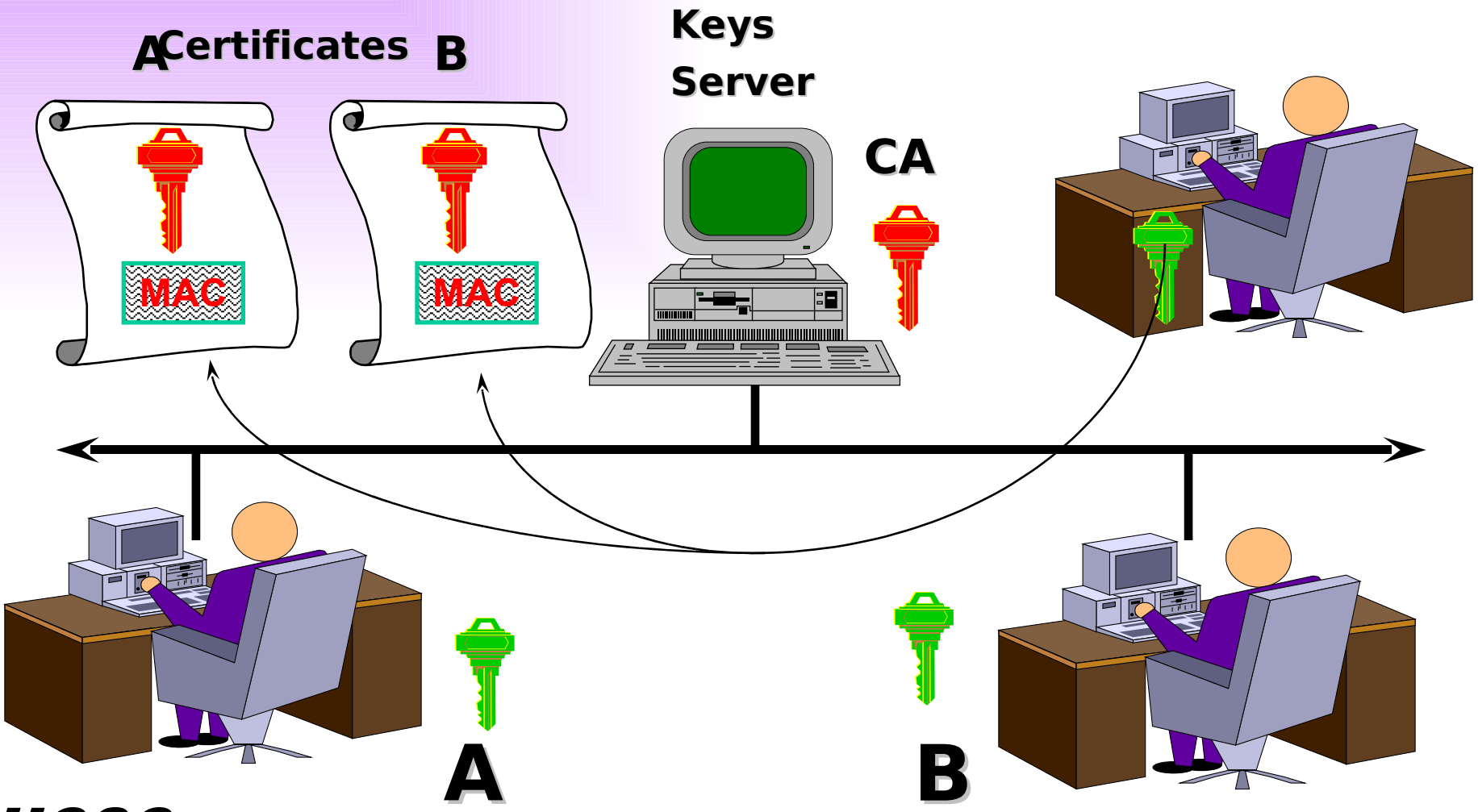
⇒ Public Key Protocols work in 3 phases

1. Authentication via Public Key Cryptography (challenge)
2. Exchange of a session Secret Key, encrypted with Public Key Crypto
3. Session encrypted with Symmetric Cryptography

ucsc

kasun@cmb.ac.lk

Certificate Authority



kasun@cmb.ac.lk

Certificates

A certificate binds an entity with its public key.
It's just a digitally signed piece of data.

⇒digital ID card

Certificate =

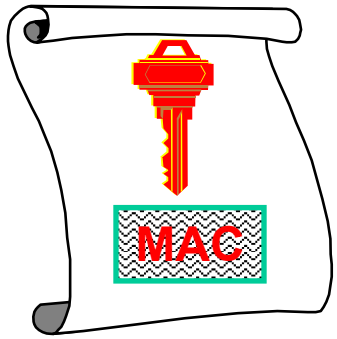
an **entity's description** (name, etc.)
+
entity's **public key**
+
expiration date, serial number, etc.
+
CA's name
+
a **signature issued by a CA**

The certificate is issued and signed by a **trusted** Certificate Authority (CA)

Digital signature:
CA signature = certificate hash, encrypted with CA's private key

Internal Structure of Certificate

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

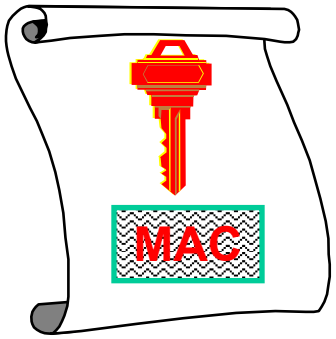


Structure of Distinguish Name

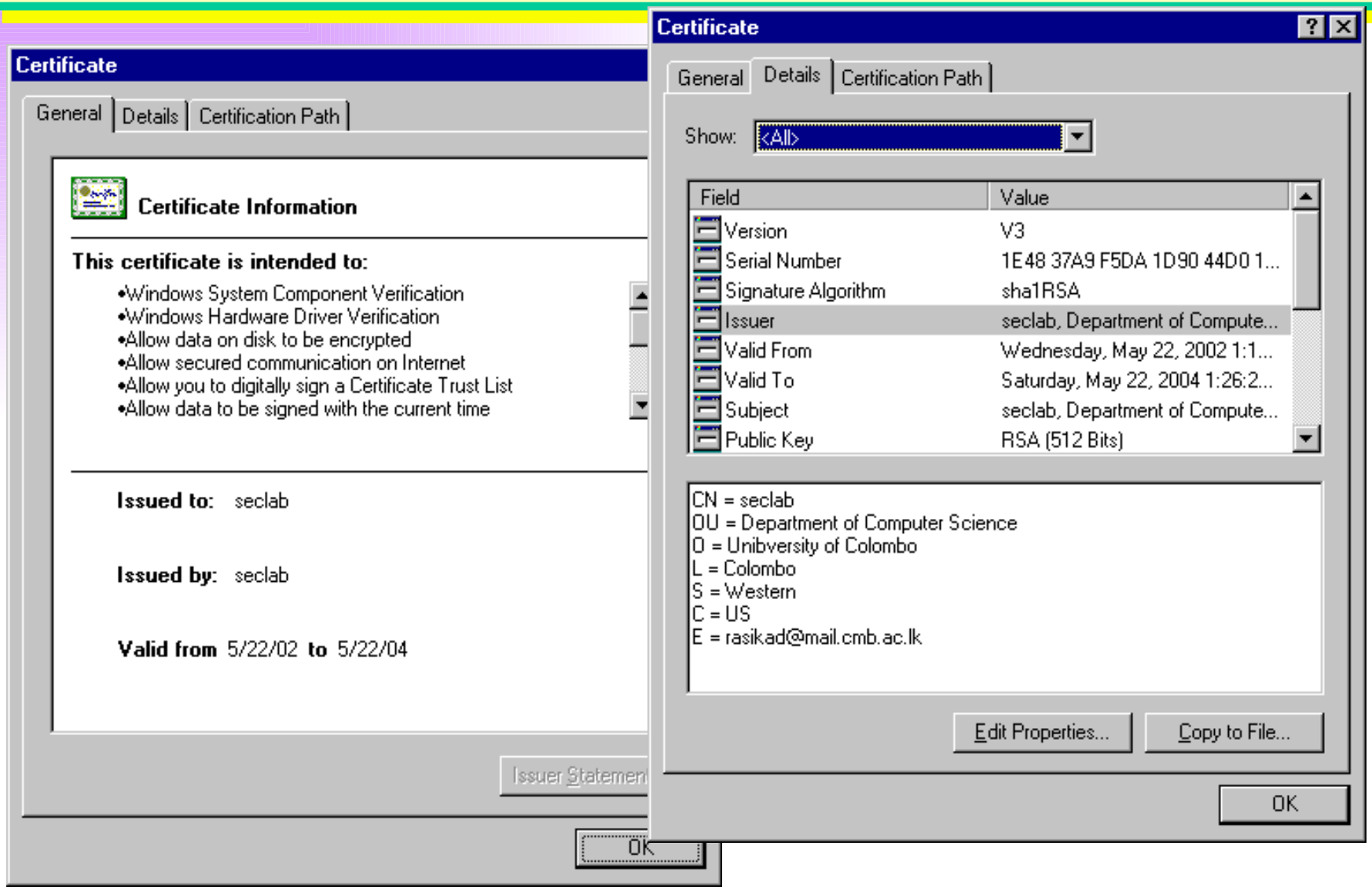
- Country Name
- State and Province Name
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- Email Address
- URL

Certificate Types

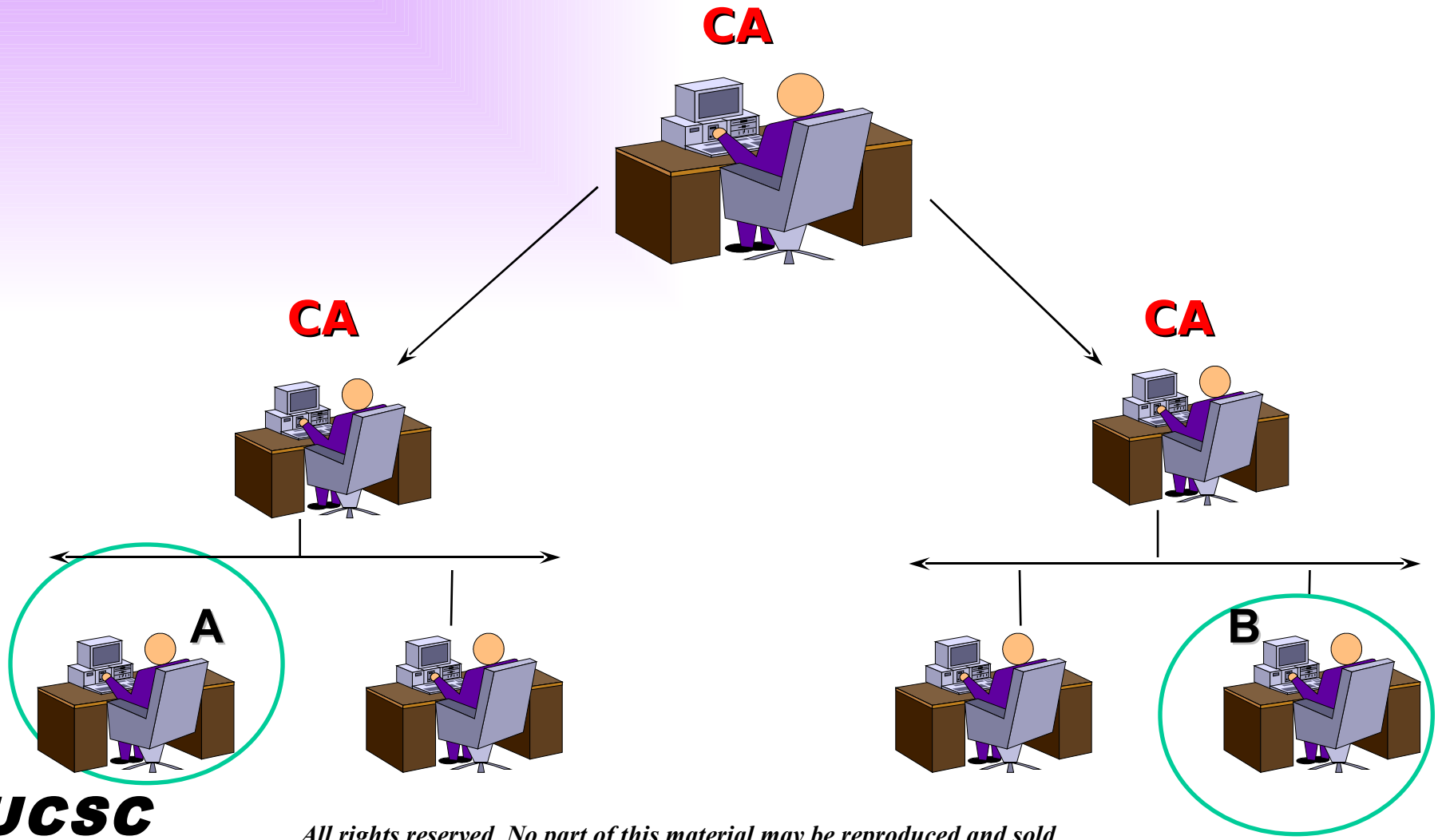
- Digital Signature
- Key Encipherment
- Data Encipherment
- Key Certificate Signature
- CRL Signature
- Object Signing



Root Certificate



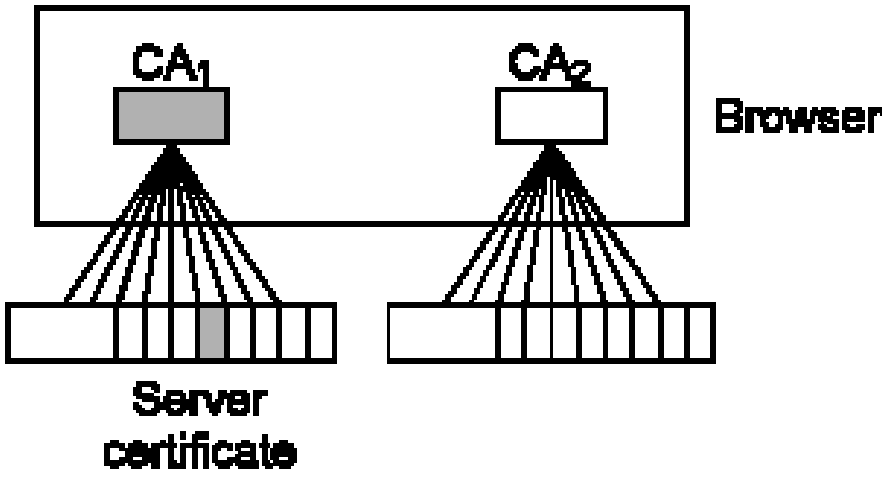
Certificate Hierarchy



kasun@cmb.ac.lk

CA Hierarchy in Practice

Flat or Clayton's hierarchy

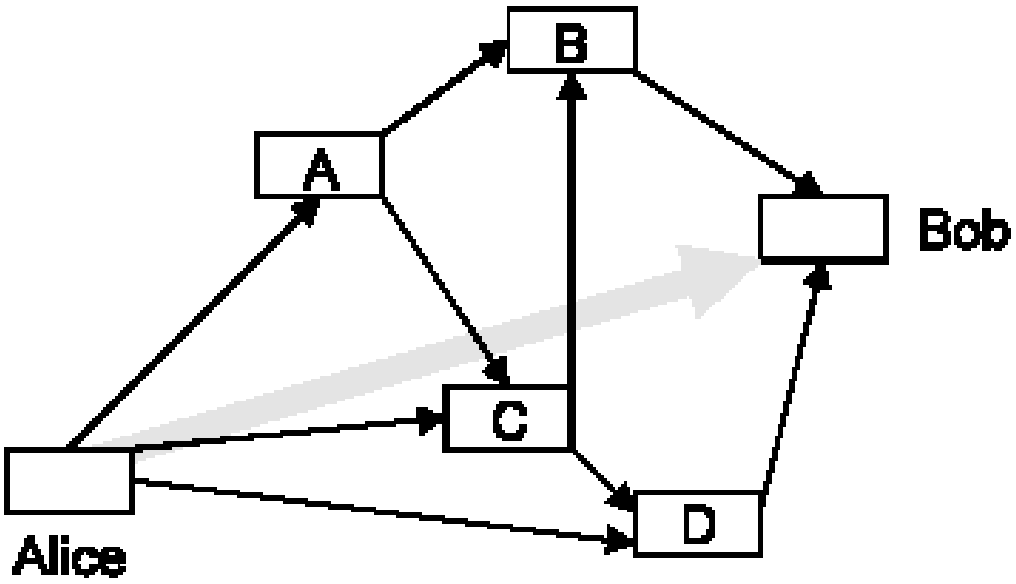


CA certificates are hard-coded into web browsers or email software

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

Alternative Trust Hierarchies

PGP web of trust



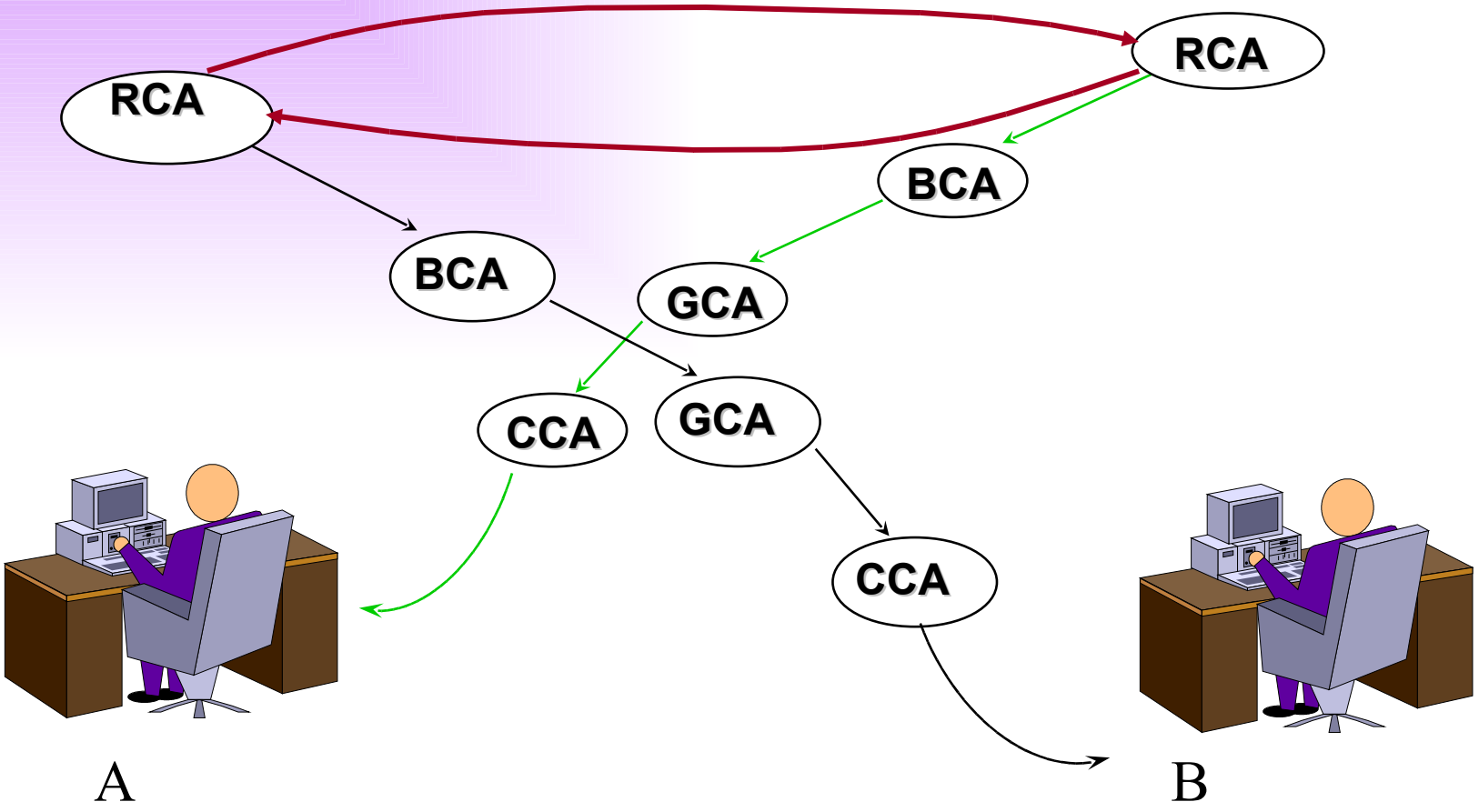
Bob knows B and D who know A and C who know Alice

$\Rightarrow$ Bob knows the key came from Alice

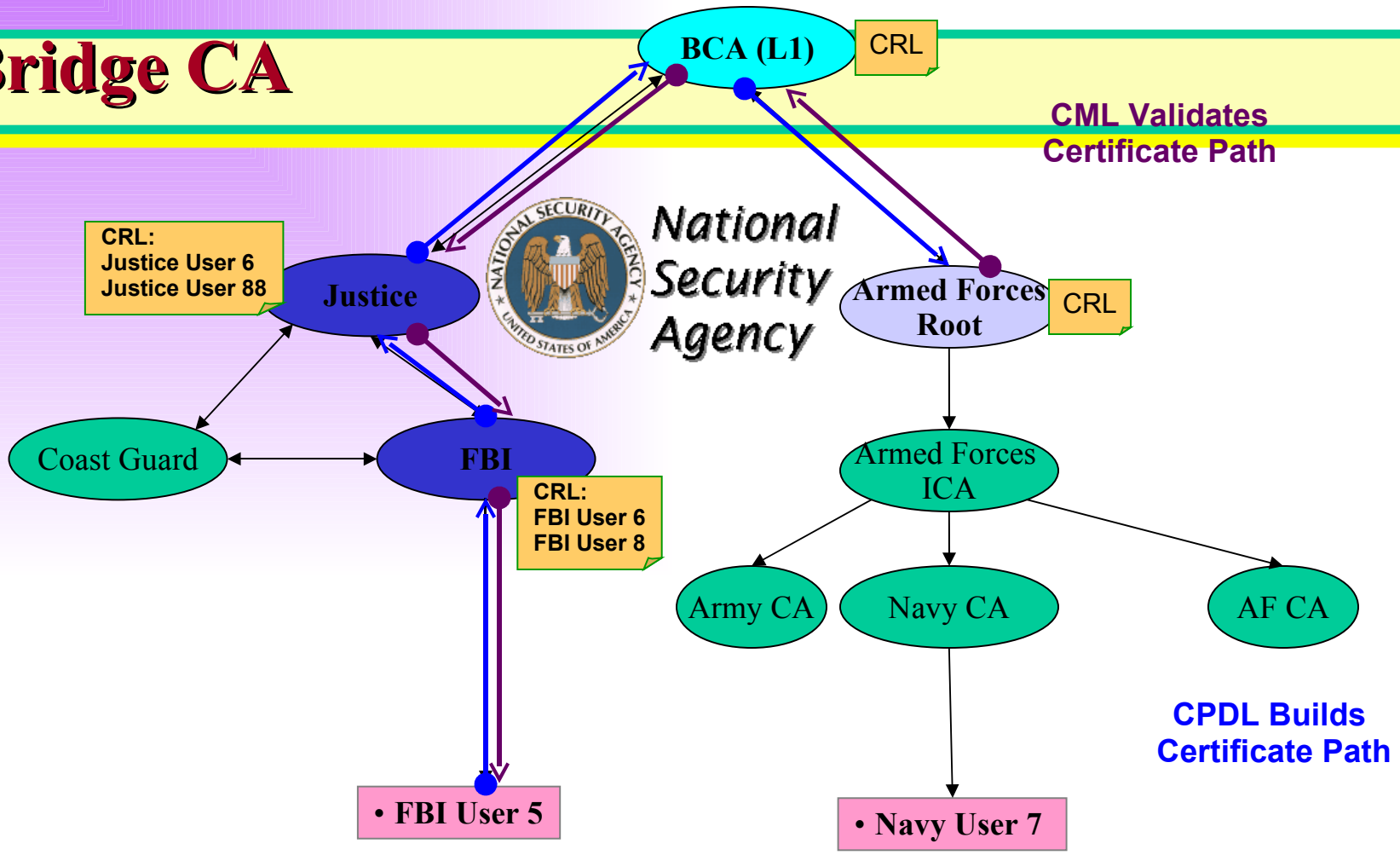
Web of trust more closely reflects real-life trust models

kasun@cmb.ac.lk

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

UCSC
kasun@cmb.ac.lk

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

kasun@cmb.ac.lk

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"

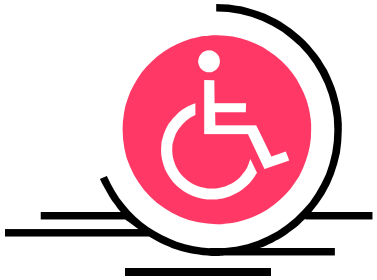
– Lightweight pseudo-CRL avoids CRL size problems

– 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"



kasun@cmb.ac.lk

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

Applied Cryptography Protocols and Practice

3.3 Legal Issues

- Copyrights
- Patents
- Trade Secrets
- Computer Crime
- Cryptography and the Law

kasun@cmb.ac.lk

Legal Issues

- Lawyers care about identity
- Signing ceremonies authenticate identities
- Dispute resolution typically requires validated information, including authenticated identification of parties
- Lawyers don't like ephemeral or ambiguous names

Why Laws? (1)

- **Laws and computer security are related in several ways.**
  - First, laws affect privacy and secrecy. These statutes often apply to the rights of individuals to keep personal matters private.
  - Second, laws regulate the use, development, and ownership of data and programs. Patents, copyrights, an trade secrets are legal devices to protect the rights of dev elopers and owners of the programs and data.
  - Third, laws affect actions that can be taken to protect the secrecy, integrity, and availability of computer information service.

Why Laws? (2)

- The laws of computer security affect programmers, designers, users, and maintainers of computing systems and computerised data banks.
- These laws provide protection, but they also regulate the behaviour of people who use computers.
- Before recommending change, however, professionals must understand the current state of computers and th e law.

Protecting Programs and Data

- There are three common used ways to provide protections by laws:
  - **Copyright**
  - **Patent**
  - **Trade Secret**

Copyrights

- Copyrights are designed to protect the expression of ideas. Thus, a copyright applies to a creative work, such as a story, photograph, song, or pencil sketch. The right to copy an expression of an idea is protected by a copyright.

- Copyright gives the author/programmer exclusive right to make copies of the expression and sell them to the public. That is, only the author can sell copies of the author's book (except, of course, for booksellers or others working as the agents of the author).

Copyrights - Originality of Work

- The work being copyrighted must be original to the author. A work can be copyrighted even if it contains so me public domain material, as long as there is some origi nality, too.
- For example, a music historian could copyright a collection of folksongs even if some are in the public dom ain. In order to be subject to copyright, something *in* or *a bout* the collection would have to be original. The historia n might argue that collecting the songs, selecting which o nes to include, and putting them in order was the original part. In this case, the copyright law would not protect the folk songs, but the specific selection and organisation.

kasun@cmb.ac.lk

Copyright - Fair Use of Material

- **The copyright law indicates that the copyrighted object is subject to "*fair use*".**
- **Specifically, the law allows *"fair use of a copyrighted work, including such use by reproductio n in copies, … for purposes such as criticism, comme nt, news reporting, teaching (including multiple copi es for classroom use), scholarship and research*".**
- **The copyright law usually upholds the author's right to a fair return for the work, while encouragi ng others to use the underlying ideas.**

Copyright - Infringement

- The infringement must be substantial, and it must be copying, not independent work.
- In theory, two people might write identically the same song independently, neither knowing the othe r. These two people would *both* be entitled to copyr ight protection for their work.

kasun@cmb.ac.lk

Copyrights for Computer Works

- **Can a computer program be copyrighted?**

  YES. The algorithm is the idea, and the statements of the programming language are the expression of the idea.

- **Therefore, protection is allowed for the program statements themselves, but not for the design: copy ing the code intact is prohibited, but reimplementi ng the algorithm is permitted.**

Patents

- **Patents are unlike copyrights in that they protect inventions, not works of the mind.**
- **The distinction between patents and copyrights is that patents were intended to apply to the results of science, technology, and engineering, whereas copy rights were meant to cover works in the arts, literat ure, and written scholarship.**
- **The patents law excludes *newly discovered laws of nature … [and] mental processes*.**

kasun@cmb.ac.lk

Patents - Requirement of Novelty

- If two composers happen to compose the same song independently at different times, copyright law would allow both of them to have copyright.
- If two inventors devised the same invention, the patent goes to the person who invented it first, rega rdless of who filed the patent first.

Patent - Infringement (1)

- A patent holder must oppose all infringement.
- With a copyright, the holder can choose which cases to prosecute, ignoring small infringements and waiting for serious infractions where the infringeme nt is great enough to ensure success in court or to ju stify the cost of the court case.
- However, failing to sue a patent infringement - even a small one or the patent holder does not know abo ut - can mean losing the patent rights entirely.

Patent - Infringement (1)

- But, unlike copyright infringement, a patent holder does not have to prove that the infringer copied the i nvention;
- a patent infringement occurs even if someone independently invents the same thing, without know ledge of the patented invention.

Patents - Computer Objects

- The patent has not encouraged patents of computer software.
- For a long time, computer programs were seen as the representation of an algorithm was a fact of nature, which is not subject to patent.
- There was a case on a request to patent a process for converting decimal numbers into binary. The S upreme Court rejected the claim, saying it seemed to attempt to patent an abstract idea, in short, an a lgorithm. But the underlying algorithm is precisely what most software developers would like to protec t.

Trade Secret

- A *trade secret* is information that gives one company a competitive edge over others. For example, the formula for a soft drink is a trade secret, as is a mailing list of customers, or information about a product due to be announced in a few months.
- The distinguishing characteristic of a trade secret is that it must always be kept secret. The owner must take precautions to protect the secret, such as storing it in a safe, encrypting it in a computer file, or making employees sign a statement that they will not disclose the secret.

Trade Secret - Computer Objects (1)

- Trade secret protection applies very well to computer software.
- The underlying algorithm of a computer program is novel, but its novelty depends on nobody else's knowing it.
- Trade secret protection allows distribution of the result of a secret (the executable program) while still keeping the program design hidden.

kasun@cmb.ac.lk

Trade Secret - Computer Objects (2)

- Trade secret protection does not cover copying a product (specifically a computer program), so that it cannot protect against a pirate who sells copies of so meone else's program without permission.
- However, trade secret protection makes it illegal to steal a secret algorithm and use it in another produc t.

Comparisons

	Copyright	Patent	Trade Secret
Protects	Expression of idea, not idea itself	Invention; the way something works	A secret competive advantage
Protected object made public	Yes; intention is to promote publication	Design filed ar patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years for a company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue of secret improperly obtained

Rights of Employees and Employers

- Employers hire employees to generate ideas and make products. Thus, the protection offered by cop yrights, patents, and trade secrets applies to the ide a and products.
- However, considering the issue of who owns the ideas and products is much more complex.
- Ownership is an issue of computer security because it relates to the rights of an employer to protect the secrecy and integrity of works produced by the employees.

Ownership of the Products (1)

- *Ownership of a patent* - The person who owns a work under patent or copyright law is the inventor.
- Therefore, employee can has the right of the patent.
- However, in a patent law, it is important to know who files the patent. If an employee lets an employer patent an invention, the employer is deemed to own t he patent and , therefore, the right to the invention.
- The employer also has the right to patent if the employee's job functions included inventing the product.

Ownership of the Products (2)

- *Ownership of a copyright* - Ownership of a copy right is similar to ownership of a patent.
- The author (programmer) is the presumed owner of the work.
- Normally, the owner has all rights to an object.
- However, a special situation known as work for hire applies to many copyrights for development of software or other products.

Ownership of the Products (3)

- *Trade secret protection* - In the event a trade secret is revealed, the owner can prosecute the revealer fo r damages suffered.
- But first, ownership must be established because only the owner can be harmed.
- A company owns the trade secrets of its business as confidential data. As soon as a secret is developed, the company becomes the owner.

Ownership of the Products (4)

- *Employment contracts* - Sometimes there is no contract between the software developer and a possible employer. However, commonly an employment contract will spell out rights of ownership. Having a contract is desirable both for employees and employers so that both will understand their rights and responsibilities.

Why Computer Crime is Hard to Define? (1)

- **Understanding**

  Neither courts, lawyers, police agents, nor jurors necessarily understand computers.

- **Fingerprints**

  Polices and courts for years depended on tangible evidence, such as fingerprints. But with many computer crimes there simply are no fingerprints, n o physical clues.

Why Computer Crime is Hard to Define? (2)

- **Form of Assets**

  We know what cash is, or diamonds, or even negotiable securities. But are 20 invisible magnetic spots really equivalent to a million dollars?

- **Juveniles**

  Many computer crimes involve juveniles. Society understands immaturity and can treat even very se rious crimes by juveniles as being done with less un derstanding than when the same crime is committe d by an adult.

Type of Crimes Committed (1)

- **Telecommunications Fraud**

  It is defined as avoiding paying telephone charges by misrepresentation as a legitimate user.

- **Embezzlement**

  It involves using the computer to steal or divert funds illegally.

- **Hacking**

  It denotes a compulsive programmer or user who explores, tests, and pushes computers and communicati ons system to their limits - often illegal activities.

Type of Crimes Committed (2)

- **Automatic Teller Machine Fraud**

  It involves using an ATM machine for a fraudulent activity - faking deposits, erasing withdrawals, divertin g funds from another person's account through stolen PIN numbers.

- **Records Tampering**

  It involves the alteration, loss, or destruction of computerised records.

- **Acts of Disgruntled Employees**

  They often use a computer for revenge against their employer.

Type of Crimes Committed (3)

- **Child Pornography and Abuse**

  They are illegal or inappropriate arts of a sexual nature committed with a minor or child, such as photographing or videotaping.

- **Drug Crimes**

  Drug dealers use computers to communicate anonymously with each other and to keep records of dr ug deals.

- **Organised Crime**

  For all kinds of crime, the computer system may be used as their tools.

Cryptography and the Law

- Cryptography is a regulated activity, but the issues are a little less clear-cut, in part because there is little open discussion of the subject.
- Everybody wants cryptography e.g. business, individual, criminal, bankers, and government.
- France prohibits use of encryption by individuals, asserting that in order to control terrorism, it must have access to communications of suspected terrori sts.

Questions?