Distributed Systems: **Security**

Dr Soumyabrata DEV
https://soumyabrata.dev/

School of Computer Science and Informatics
University College Dublin
Ireland

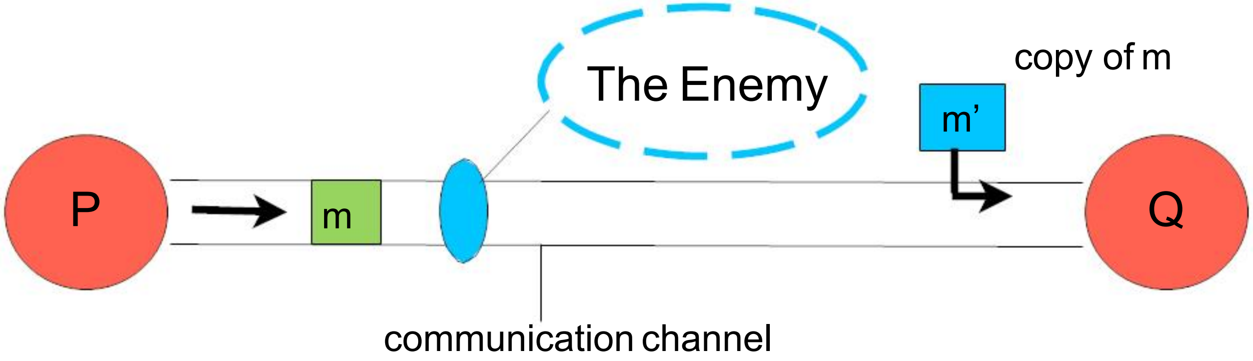
These course slides are adapted from the original course slides prepared by Dr Anca Jurcut, University College Dublin.

Security in Distributed Systems

- Why are distributed systems vulnerable to security attacks?
  - promote the sharing of resources - open to external access
  - Exposed interfaces to services offered by the distributed system
  - Insecure networks
  - Hackers likely to have knowledge of the algorithms used to deploy services in distributed systems

Protecting Resources

- Access to shared resources managed by processes
- processes outline how you interact with the resource
- need to protect processes that
  - execute shared objects
  - communicate with shared processes



Security Policy v/s Mechanisms

- Security Mechanisms: techniques used to protect a shared resource
  - e.g. lock used to lock a door
- Security Policies: rules which govern the use of security mechanisms
  - e.g. rule which says the door must be locked when it is not guarded
- policies are independent of the mechanism used but are just as vital
  - i.e. provision of a lock does not ensure a door is secure unless there is a policy for it’s use

Security Mechanisms

- Goal of security mechanisms: to protect shared resources from:
  - Unauthorized access (hackers)
  - Malicious attacks (viruses)
  - Incorrect Usage (mistakes by valid users)
- Today we examine mechanisms for the protection of data and other resources in a distributed system
  - whilst allowing interactions between computers implied by security policies
- A key technique that underpins security is cryptography
  - “*The* art of encoding information in a format that only the intended recipients can *access.”*

3 Security Threats

λLeakage - the acquisition of information by unauthorized recipients.

  λ Choicepoint, the leading US provider of identification and credential verification services with a turnover of $1.1bn, leaked 163,000 private records in 2004/05 resulting in costs of over $55m (to date).

λTampering – the unauthorized alteration of information.

  λ E-Trade, an online stock-broker, lost $18m in 3 months due to hackers who snagged banking credentials which they used to transfer money to personal accounts.

λVandalism – interference with the proper operation of a system without gain to the perpetrator.

  λ Pakistani hackers recently vandalized the website of Mitnick Security Consulting, the company formed by Kevin Mitnick

Methods of Attack

- In order to attack any system, attackers need to either
  - access an existing communication channel OR
  - establish a new channel that looks like an authorized one

- Methods of attack can be further classified by the way in which the channel is misused...

channel = communication mechanism between processes

5 Methods of Attack

- 1. Eavesdropping – obtaining copies of messages without authority.
  - October 2007, a German security expert presented a SMS-based Trojan that copied all SMS messages on a mobile phone and created conference calls to allow monitoring of all phone calls.
- 2. Masquerading – sending or receiving messages using the identity of another principal without their authority.
  - E.g. e-mails claiming to be from banks that contain links to fake login pages.
- 3. Message Tampering – intercepting messages and altering their contents before passing them on to the intended recipient.
  - Man-in-the middle attacks, such as fake web sites that mimic bank web-sites, where users to interact as normal with the bank website, but do so via an intermediary website that records all transmitted information.

5 Methods of Attack

- 4. Replaying – storing intercepted messages and sending them at a later date.
  - Type of man-in-the-middle attack that is often used to maintain credentials.
  - e.g. a customer accesses their online bank account, without realizing that the HTTP requests are being recorded. At a later date, the hacker can use the record to log in to the customers bank account.

- 5. Denial of Service – flooding a channel or other resource with messages in order to deny access to others.
  - On its launch March 2006, Sun Grid, which offered a sample text-to-speech service, suffered a denial of service attack.
  - In February 2000, Yahoo, Amazon, and eBay were hit by repeated distributed denial of service attacks that repeatedly made the sites inaccessible over a two day period.

Designing Secure Systems

- Worst case assumptions:
  - Exposed interfaces
  - Insecure networks.
    - fake messages, spoofed host addresses, etc.
  - Algorithms and program code available to attackers.
    - Best practice: publish, scrutinize, and rely on the keys
  - Attackers may have access to large resources.
    - Hardware is cheaper so design for the future.
- Guidelines:
  - Limit Lifetime and Scope of Secrets.
    - Limit life of passwords and secret keys
  - Minimize the Trusted Base.
    - Keep the number of trusted components to a minimum.
    - Try to separate applications from data and protect the data.

trusted base = portion of the system that is responsible for the implementation of it's security (including all hardware and software components that they rely on)

What Is Cryptography ?

Cryptography —— making "secret codes"

is the study of mathematical techniques related to aspects of information security.

Cryptanalysis: —— breaking "secret codes"

the study of mathematical techniques for attempting to defeat information security services.

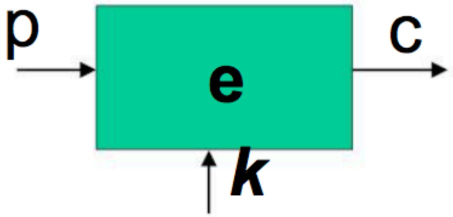
Cryptology: —— The art & science of making + breaking "secret codes"

the study of cryptography and cryptanalysis.

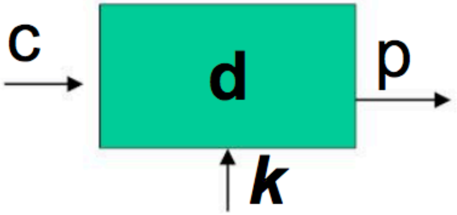
What is a Cryptosystem?

- A *cipher* or *cryptosystem* is used to *encrypt* (e) the *plaintext* (p)
- The result of encryption is *ciphertext* (c)
- We *decrypt* (d) ciphertext to recover plaintext
- A *key* (k) is used to configure a cryptosystem
- $d_K(e_K(p)) = p$

encryption



decryption



Cryptosystem

- **Basic assumptions**
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms (ciphers) are not secret
- This is known as **Kerckhoffs' Principle**
- **Why do we make such an assumption?**
  - Experience has shown that secret algorithms tend to be weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Characteristics of a Good Cipher

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

Types of Cryptography

- ❑ **Symmetric Key**
  - o Same key for encryption and decryption
  - o Modern types: Stream ciphers, Block ciphers
- ❑ **Public Key** (or “asymmetric” crypto)

o Two keys, one for encryption (public), and one for decryption (private)

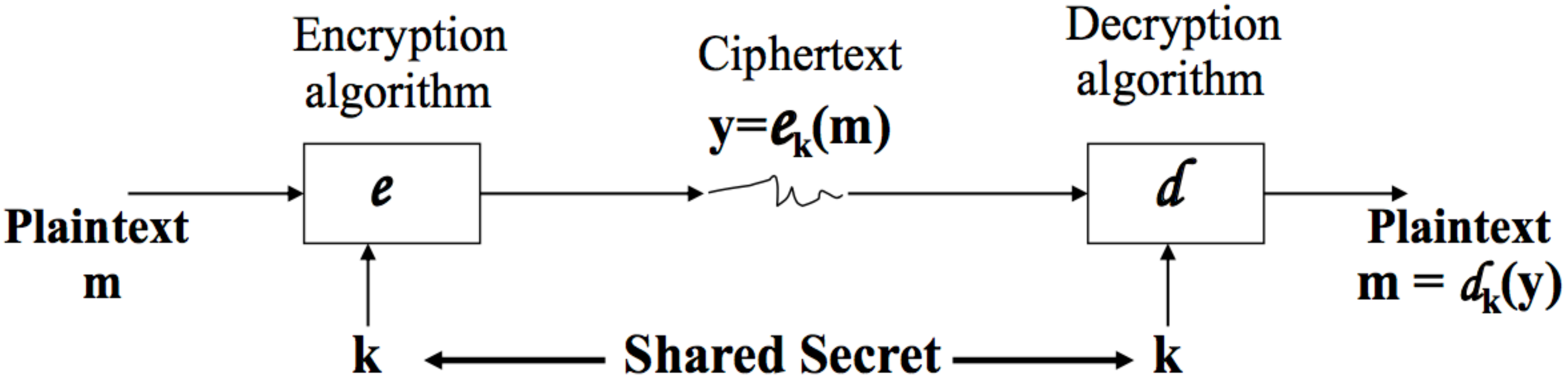
o Example: digital signatures — The private key used for signing is referred to as the signature key and the public key as the verification key.

- ❑ **Hash algorithms**
  - o Can be viewed as “one way” crypto

Symmetric key (Conventional) Crypto

- Unique key (k) for correspondence
- In a network, the transmitter and receiver share a common key
- Keys must be delivered/distributed in a secure manner

Symmetric key (Conventional) Crypto



- Communicating parties share a secret key (k)
- Encryption followed by decryption, using the same key, causes the original message to be recovered [$m = d_k(e_k(m))$]
- For secrecy/confidentiality between A and B, only A and B must know the shared key (k).

Symmetric Key Crypto

2 Types:

- **Stream cipher** — generalize one-time pad
  - Except that key is relatively short
  - Key is stretched into a long **keystream**
  - Keystream is used just like a one-time pad
- **Block cipher** — generalized codebook
  - Block cipher key determines a codebook
  - Each key yields a different codebook
  - Employs both “confusion” and “diffusion”

Confusion and Diffusion

- In cryptography, confusion and diffusion are two properties of the operation of a secure cipher identified by Claude Shannon in his 1945 classified report A Mathematical Theory of Cryptography.

- Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

- Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.

Public Key Cryptography (PKC)

- Probably most significant advance in the history of cryptography

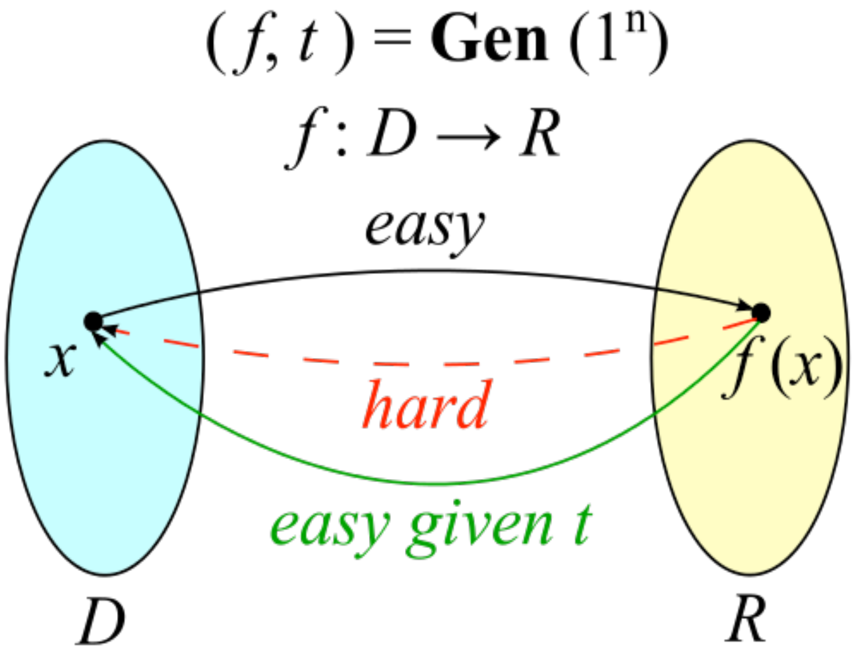
- Developed to address two main issues:
  - **Key Distribution** – how to have secure communications in general without having to trust a Key Distribution Centre with your secret key
  - **Digital Signatures** – how to verify a message comes intact from the claimed sender

Public Key Cryptography(PKC)

- **Two keys, one to encrypt, another to decrypt**
  - Alice uses Bob’s **public key** to encrypt
  - Only Bob’s **private key** decrypts the message
- **Based on** “trapdoor, **one way** function”
  - “One way” means easy to compute in one direction, but hard to compute in other direction
  - Example: Given p and q, product N = pq easy to compute, but hard to find p and q from N
  - “Trapdoor” is used when creating key pairs

Trapdoor function

- A **trapdoor function** is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are widely used in cryptography.



A trapdoor function **f** with its trapdoor **t** can be generated by an algorithm **Gen.** **f** can be efficiently computed, *i.e.*, in polynomial time. However, the computation of the inverse of **f** is generally hard, unless the trapdoor **t** is given.

Public Key Cryptography (PKC)

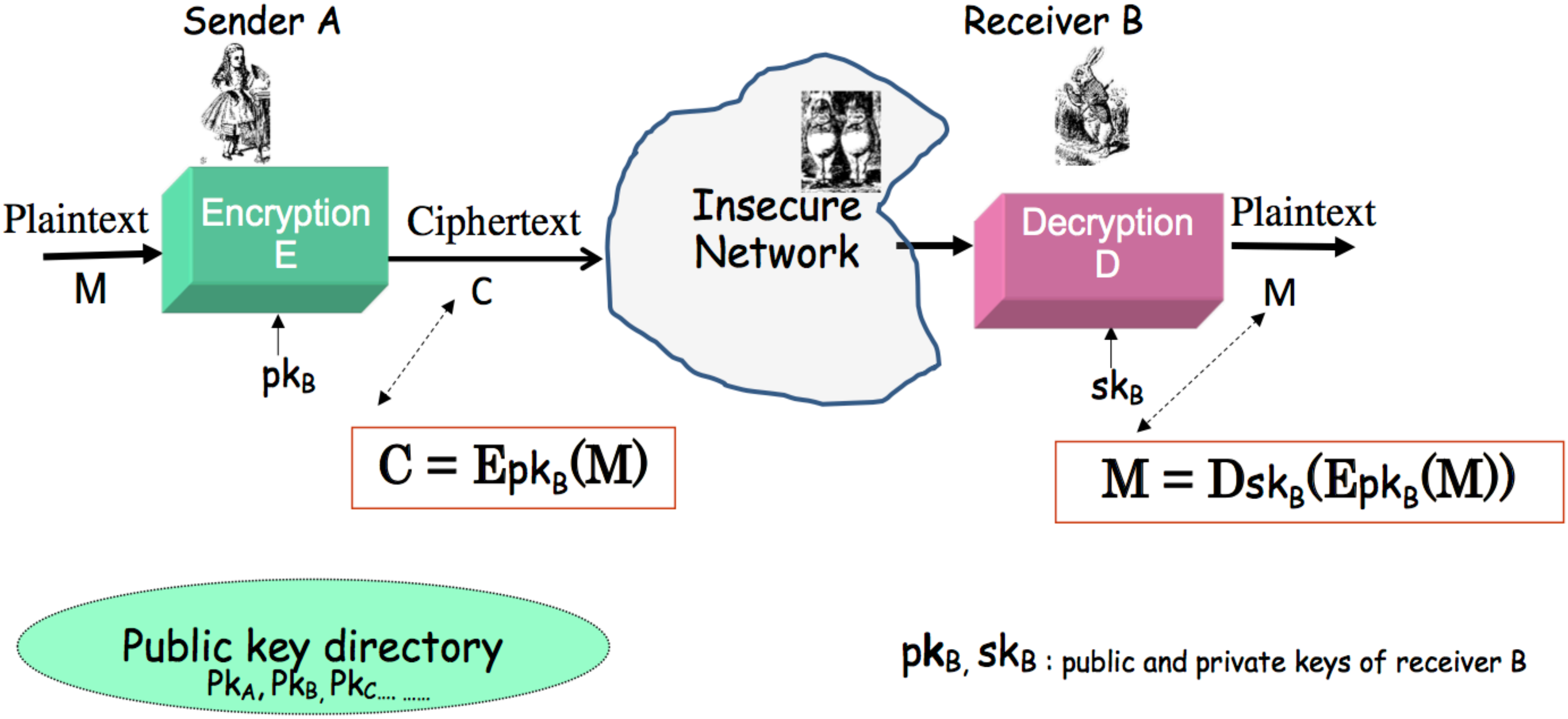
- Each user has 2 keys, public key (**pk**) and private key **(sk)**
  - **Public key pk**
    - used to **encrypt messages**
    - used to **verify signatures**
  - **Private key sk**
    - only known by the owner
    - used to **decrypt messages**
    - used to **create signatures**

Public Key Cryptography (PKC)

- Encryption
  - Suppose we **encrypt** M with Bob’s public key
  - Bob’s private key can **decrypt** C to recover M
- Digital Signature
  - Bob **signs** by “encrypting” with his private key
  - Anyone can **verify** signature by “decrypting” with Bob’s public key
  - But only Bob could have signed
  - Like a handwritten signature, but much better…

Using PKC: Confidentiality/Secrecy

- Sender encrypts the message using the receiver's public key



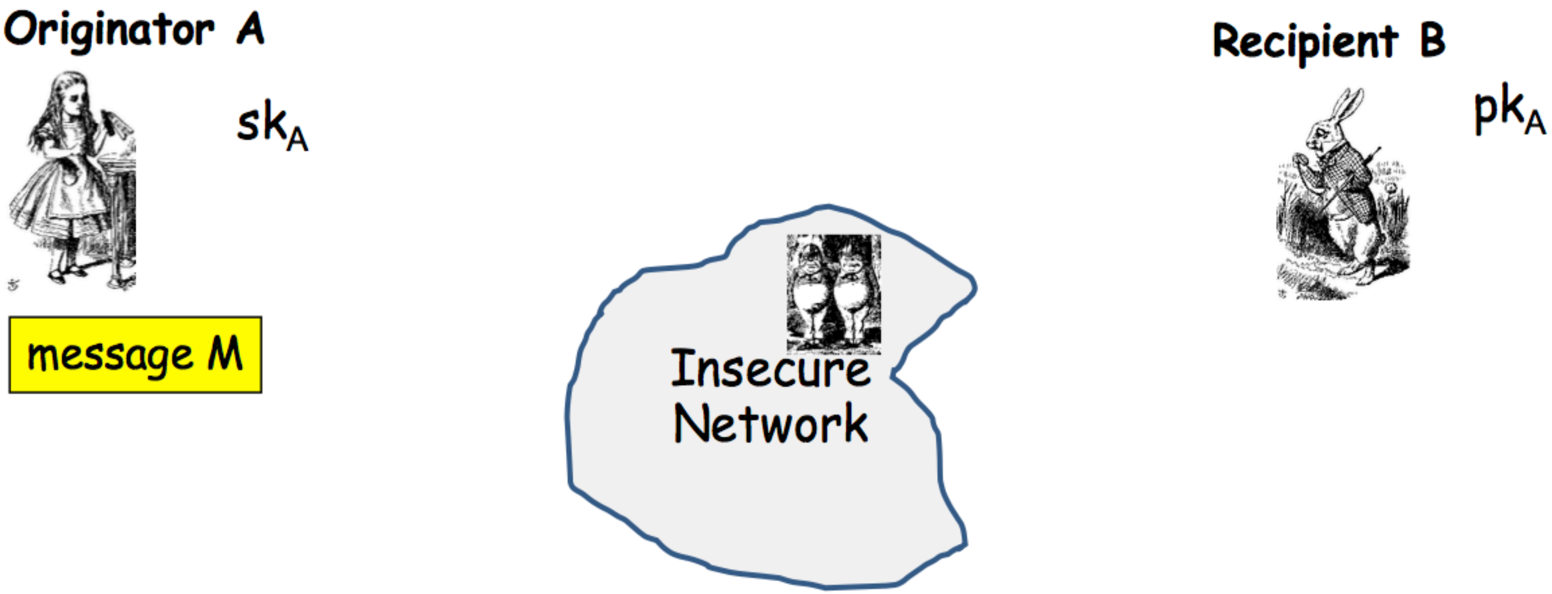
$$C = E_{pk_B}(M)$$

$$M = D_{sk_B}(E_{pk_B}(M))$$

Public key directory
Pk_A, Pk_B, Pk_C.... ......

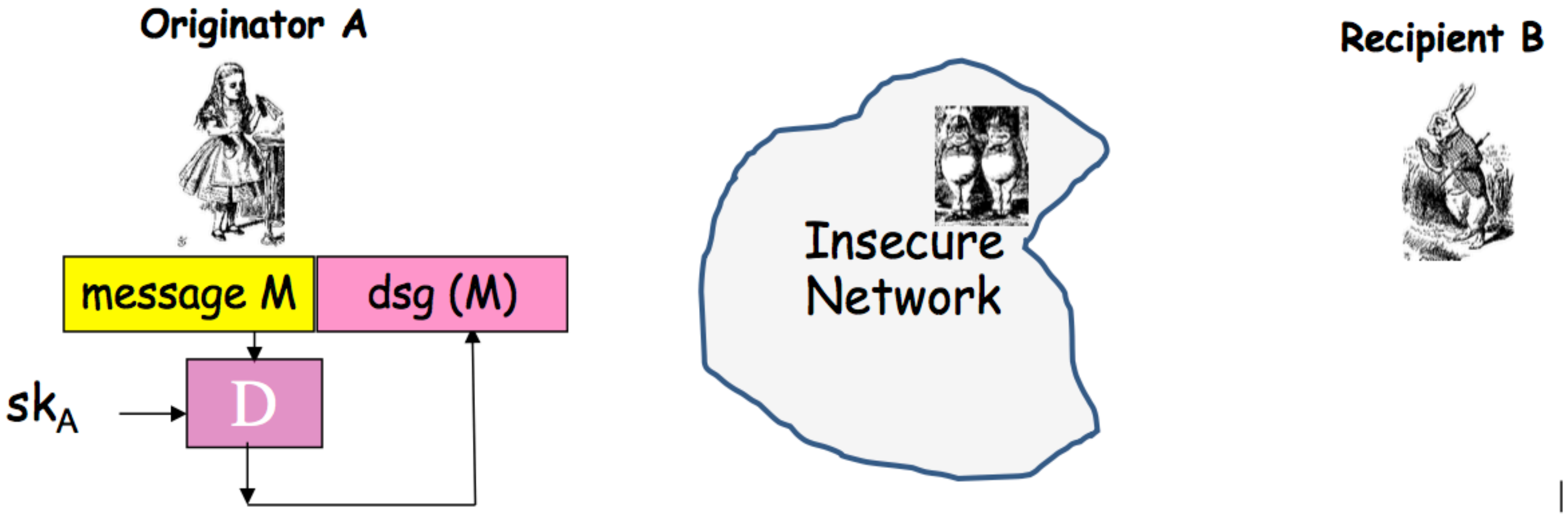
pk_B, sk_B : public and private keys of receiver B

Using PKC: Message Authentication using Digital Signatures



- ❑ A wishes to send a signed message M to B
- ❑ On receipt B wants to verify the integrity and the originator of the message M

Using PKC: Message Authentication using Digital Signatures



$$dsg(M) = Dsk_A(M)$$

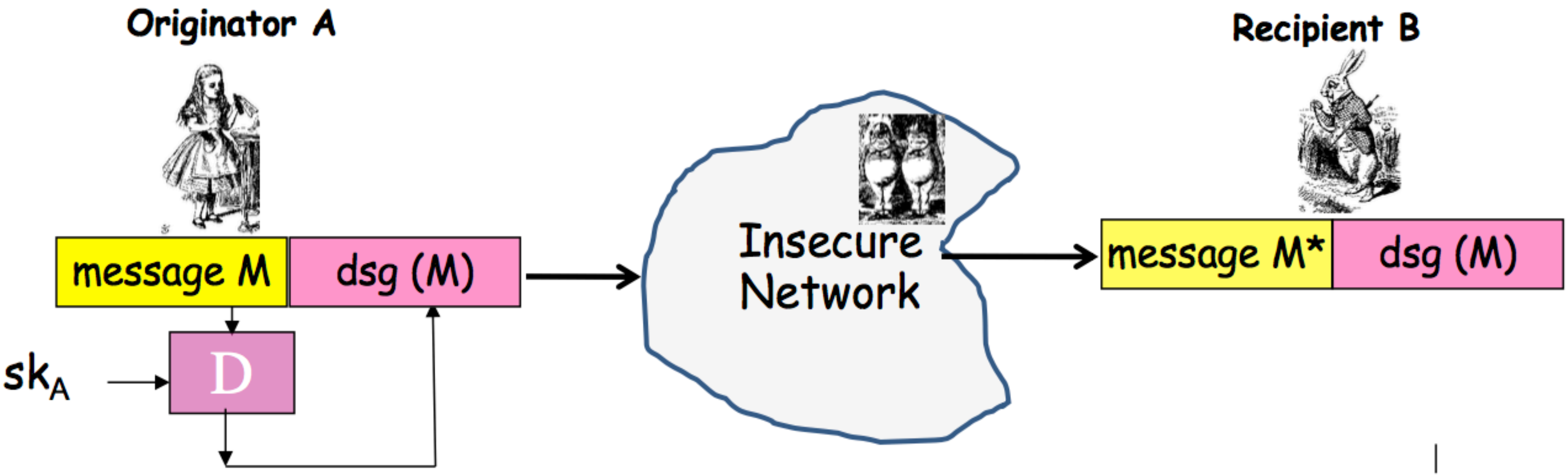
pk_A, sk_A : public and private keys of originator A

Signature Generation

$$\boxed{M,\ Dsk_A(M)}$$

- ❑ A signs message M using her private key sk_A

Using PKC: Message Authentication using Digital Signatures



$$dsg(M) = Dsk_A(M)$$

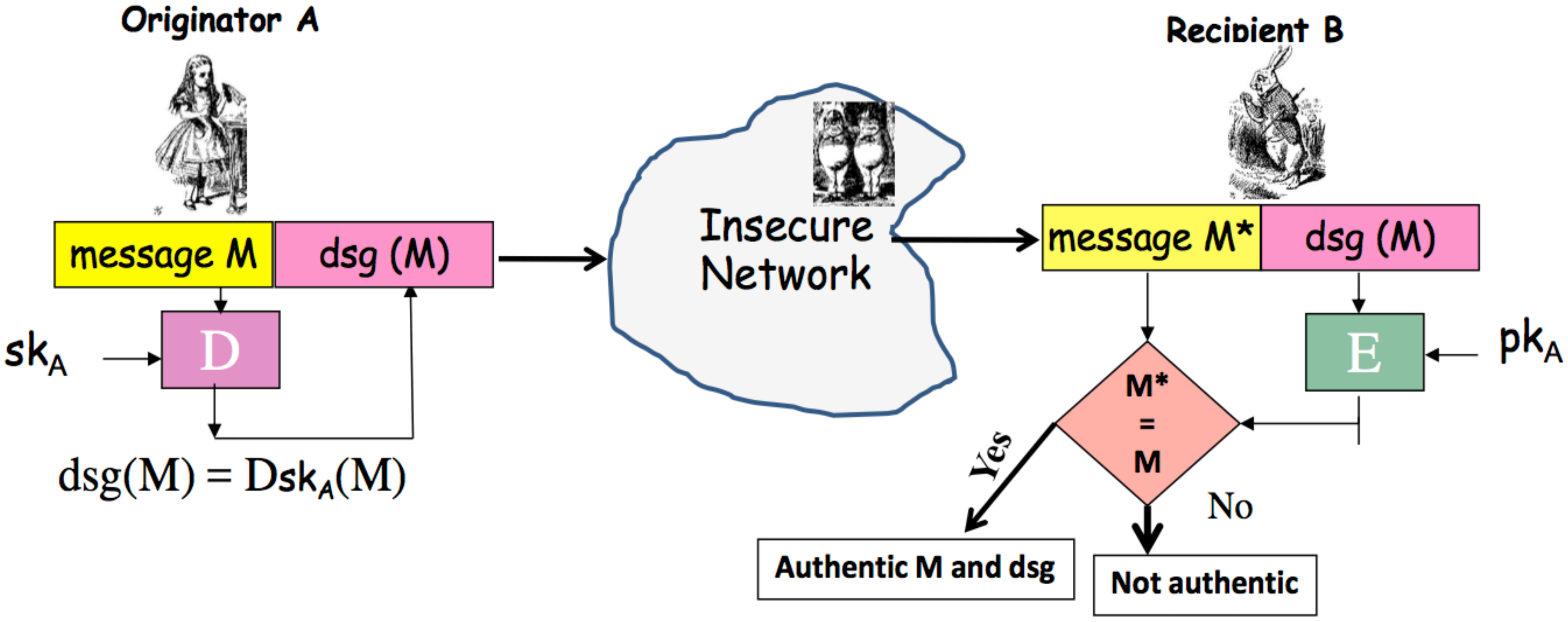
pk_A, sk_A : public and private keys of originator A

Signature Generation

$$\boxed{M,\ Dsk_A(M)}$$

- A sends signed message to B

Using PKC: Message Authentication using Digital Signatures



Signature Generation

$M, \; Dsk_A(M)$

Signature Verification

verify $M = M^*$,

where $M = Epk_A(Dsk_A(M))$

pk_A, sk_A : public and private keys of originator A

Uses of Cryptography

- Secrecy and Integrity
- Authentication
- Digital Signatures

Secrecy and Integrity

- Ensuring the safety and correctness of information of transmitted over networks.
  - Relies on the fact that an encrypted message can only be decrypted by someone that has the corresponding decryption key.
  - Secrecy is maintained so long as the decryption key is not compromised.
  - Encryption maintains data integrity so long as some form of checksum is also provided.

- Issues:

  How do we transmit the keys securely?

  - How do we know that the message isn't a copy of an earlier message?

Authentication

- Supporting communication between pairs of principals:
  - The receipt of secure message implies that the sender must have the corresponding encryption key - hence deduce identity of sender (if key is only known to two the parties)
  - If the key is known to only one recipient, then that recipient is uniquely identified by the decryption key
- Example 1: Authenticated Communication with a Server
  - Let A and B be two principles, S is a third party server
  - A wishes to access file located on file server B
  - S is authenticating server that is securely managed
    - issues passwords and holds secret key for all principles in the system
  - Ticket: is an encrypted item issues by authentication server containing the identity of a principle to who it is issued and a shared key that has been generated for a new communication session

E.g. Ticket = $\{K_{AB}, Alice\}_{KA}$

Summary

- Essential to protect communication channels and interfaces of systems with shared resources - hold information that might be subject to attack
  - E.g. e-mail, financial transactions

- Security protocols, policies and mechanisms are designed to protect such resources

- Two kinds of Security mechanisms:
  - Shared key/Secret key cryptography
  - Public key cryptography

Summary

- Secret key cryptography - symmetric - same key used for encryption and decryption
  - A and B share same key - can exchange encrypted information without risk
  - problem: how to exchange keys?
- Public key cryptography - asymmetric - different keys used for encryption and decryption - knowledge of one does not reveal the other
  - one key made public, anyone can send messages to the holder of corresponding private key - holder of private key can sign messages and certificates

Thank you

For general enquries, contact:

Please contact the Head Teaching Assistant: Xingyu Pan (Star), Xingyu.Pan@ucdconnect.ie