Week 1

Overview Lecture

Subject Overview

Lecture 1

Introduction to cryptography.

Lecture 2

Introduction to Numbers

Workshops start from Week 2

Quiz 1

Introduction to cryptography

COMP90043

Lecture 1

Udaya Parampalli

Introduction to cryptography

Lecture 1

1.1 Information Security

- Definitions, Role of Cryptography, Cyber Security
- Story of Cryptography since ancient times
- A story of Alice and Bob: terms and notations

1.2 Motivating Examples

- Practical Banking
- A Communication Game:

1.3 Classical example

- Diffie-Hellman Protocol

1.4 Basic Security Objectives

1.1 Information Security

COMP90043

Lecture 1

Information Security

Definitions, Role of Cryptography, Cyber Security

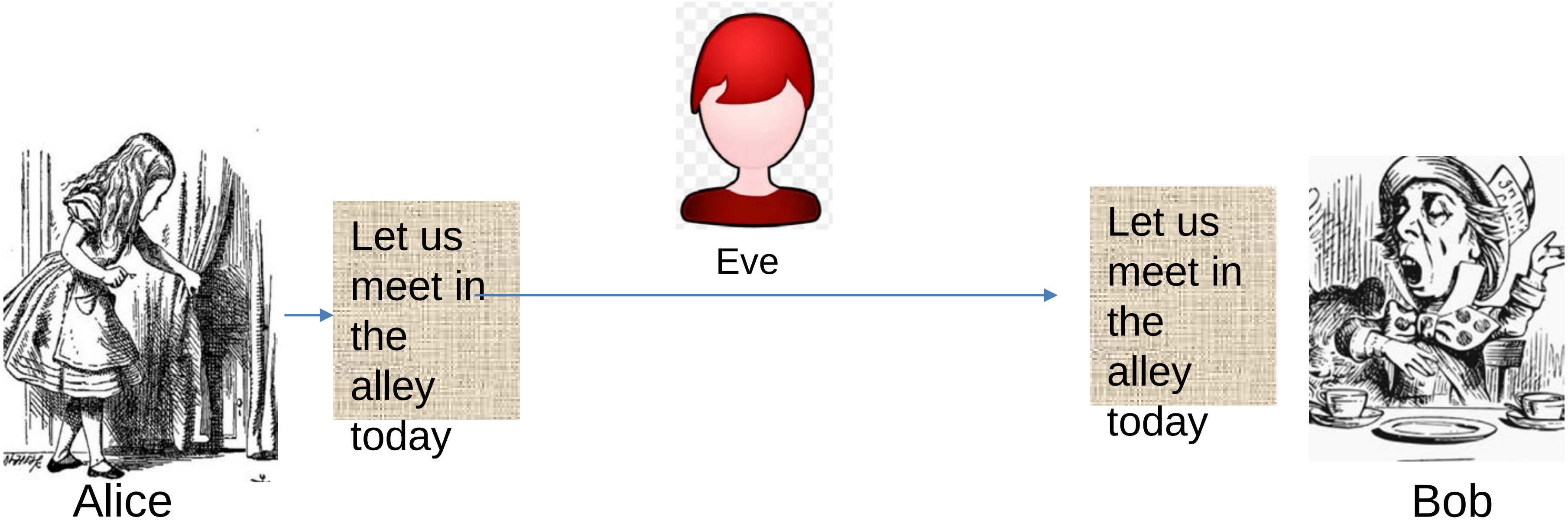
- What is Cryptography?
  - “Secret Writing”
  - Refers to the techniques required for protecting data between authorized parties on information communication technologies in the presence of potentially malicious elements.
  - Refers to a range of techniques such as Encryption, Signature, Hash functions, assuring Privacy, Integrity, and Authentication of data in the digital world.
- What is Information Security?
  - A broad topic of exchange and processing of information on modern computers and networks.
  - Confidentiality, Integrity, and Availability.
- What is Cyber Security?
  - Refers to management of attacks and risks by adversarial and malicious elements on computers and networks that support modern businesses and economy involving business, government, and community.

Information Security

The field of Network and Internet security

- Stallings Take:
  - The field of network and Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.
- Our Approach:
  - Is to study certain basic cryptographic primitives such as symmetric and public key cryptography, hash functions, message authentication and signatures, and use them explore the field of network and Internet security protocols.

Story of Cryptography since ancient times



Eve

Let us meet in the alley today

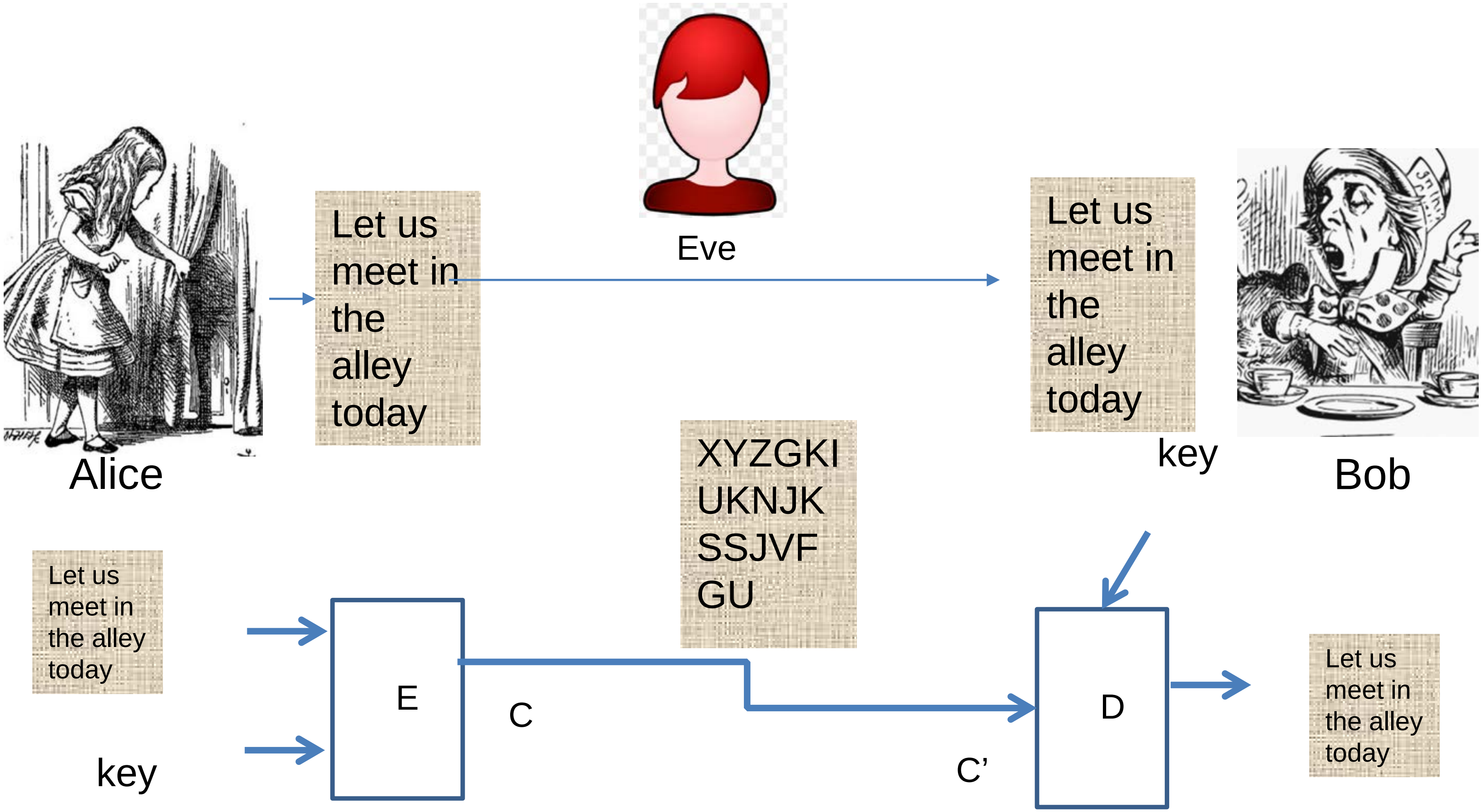
Let us meet in the alley today

Alice

Bob

Images: General Internet resources

Story of Cryptography since ancient times



Eve

Alice

Let us meet in the alley today

Let us meet in the alley today

Bob

key

XYZGKI UKNJK SSJVF GU

Let us meet in the alley today

key

E

C

C’

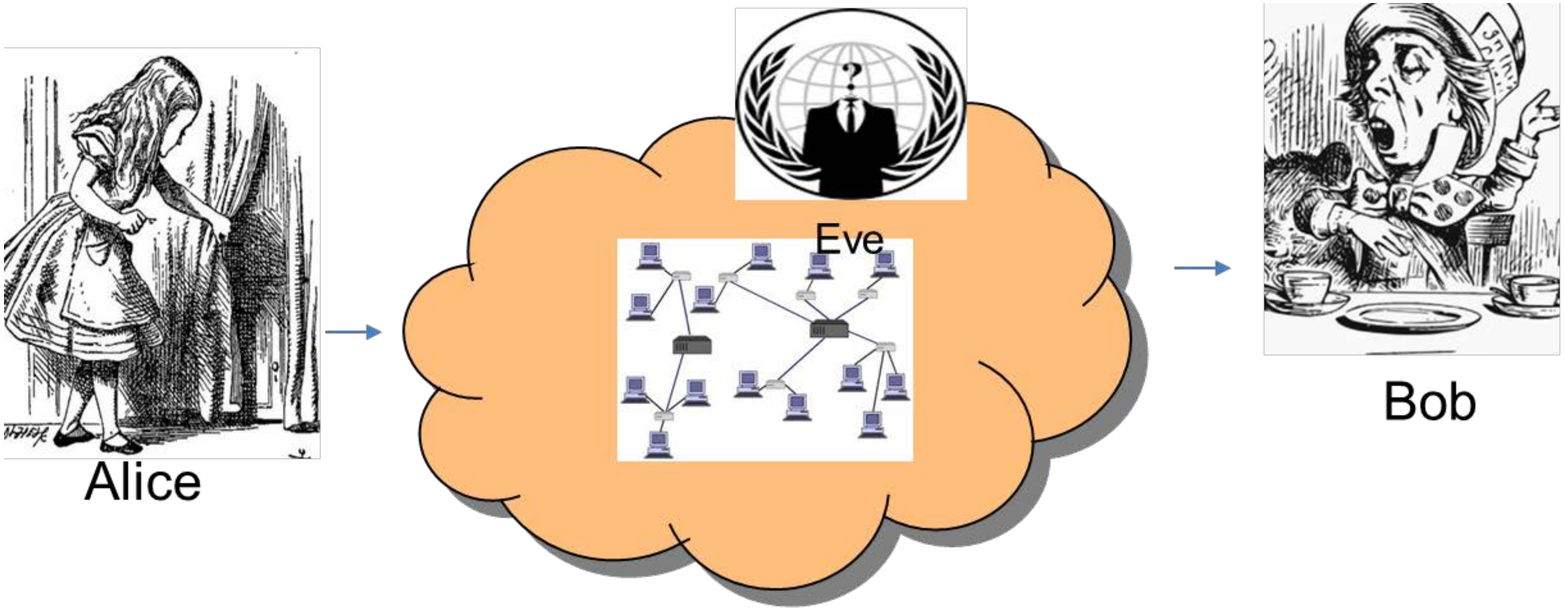
D

Let us meet in the alley today

How do they agree on the “key”? -Chicken and Egg Problem

Images: General Internet resources

Fast forward: In Modern times



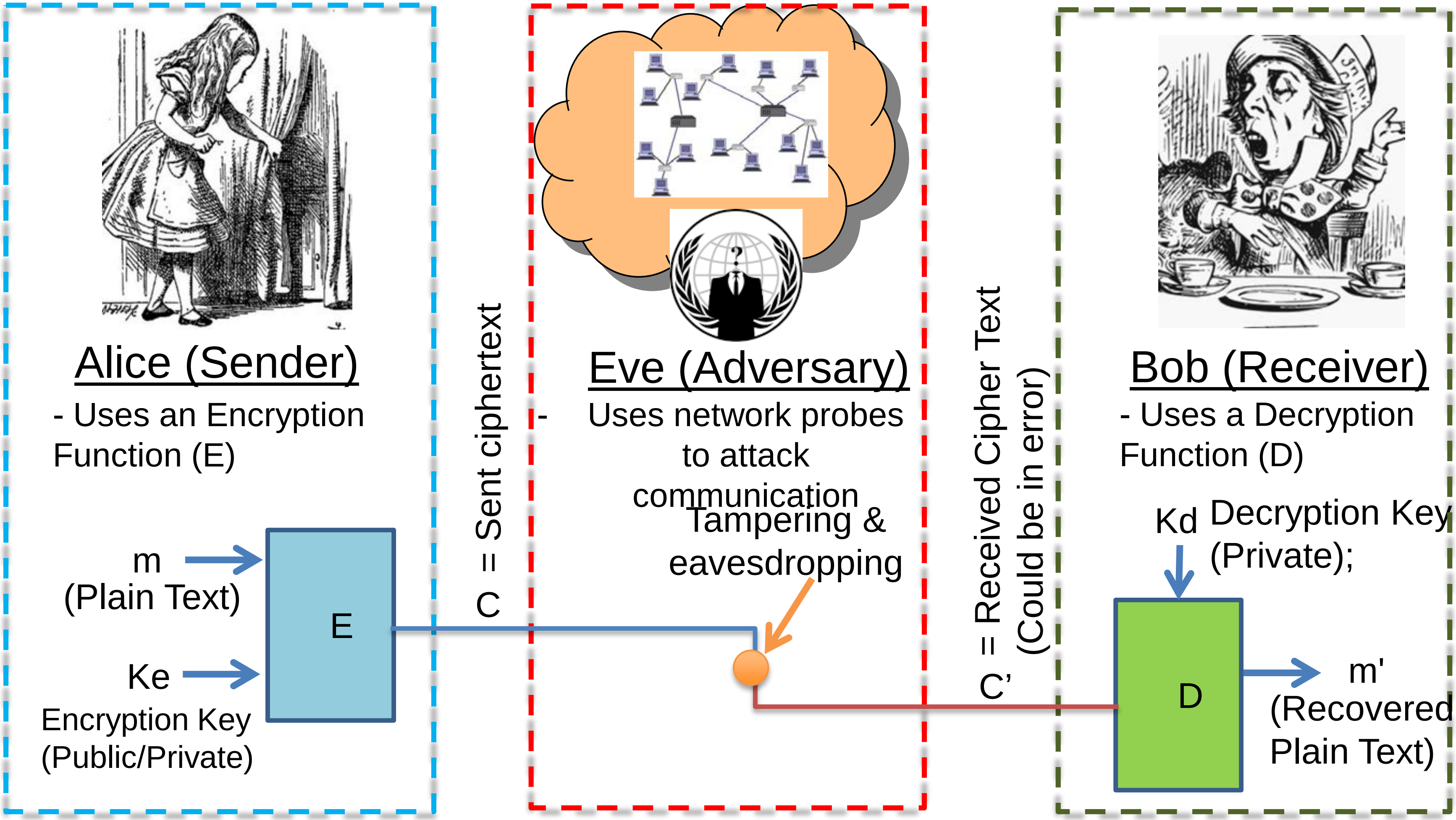
Alice and Bob cannot meet in advance for every situation

Can Mathematics come to their aid?

The magic tool is the One Way function.
We will consider many such functions based on numbers in the subject

Images: General Internet resources

Story of Alice and Bob terms and notations



E, D are public; c is the ciphertext, c' is received ciphertext; ideally m=m';

Cryptography involves many conceptual ideas, we look at the basic functions

Images: General Internet resources

Differences

- $Ke = Kd$:Symmetric key also sometimes referred as private key. But we shall call always symmetric key-
  - Known since antiquity.
- $Ke \neq Kd$: Asymmetric or Public Key Cryptography –
  - Fairly recent- since 1974 after the celebrated paper by Diffie-Hellman.
  - Please read this paper. I have added a link to this page in LMS.

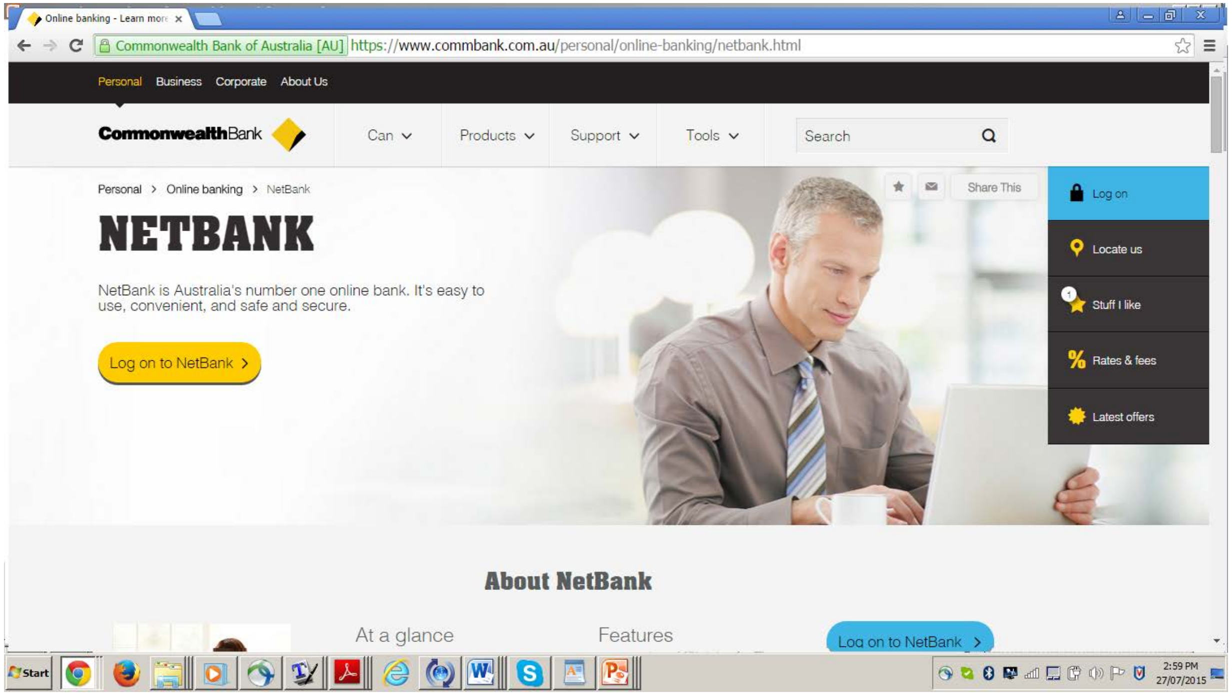
1.2 Motivating Examples

COMP90043

Lecture 1

Udaya Parampalli

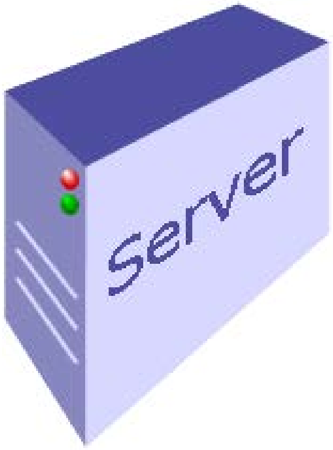
Motivating examples



NETBANK

NetBank is Australia's number one online bank. It's easy to use, convenient, and safe and secure.

Comm bank Server



Issues in getting your money from the bank.
Should work over Internet
Think, who is Alice, Bob and Eve here.
What tools Cryptography can provide here?

A Communication Game

Alice

Dating Problem!

Bob

Alice and Bob want to spend an evening together.

They want to decide whether to go to Music concert or Cinema

They can resolve either way by tossing a coin.

If they can meet together, it is a simple task.

However, they are in different offices connected by a telephone.

They need to book the program in advance and want to make decision over the phone.

Can you help them?

A Cryptographic Solution Using Mathematics!

- Assume we have a magic function with

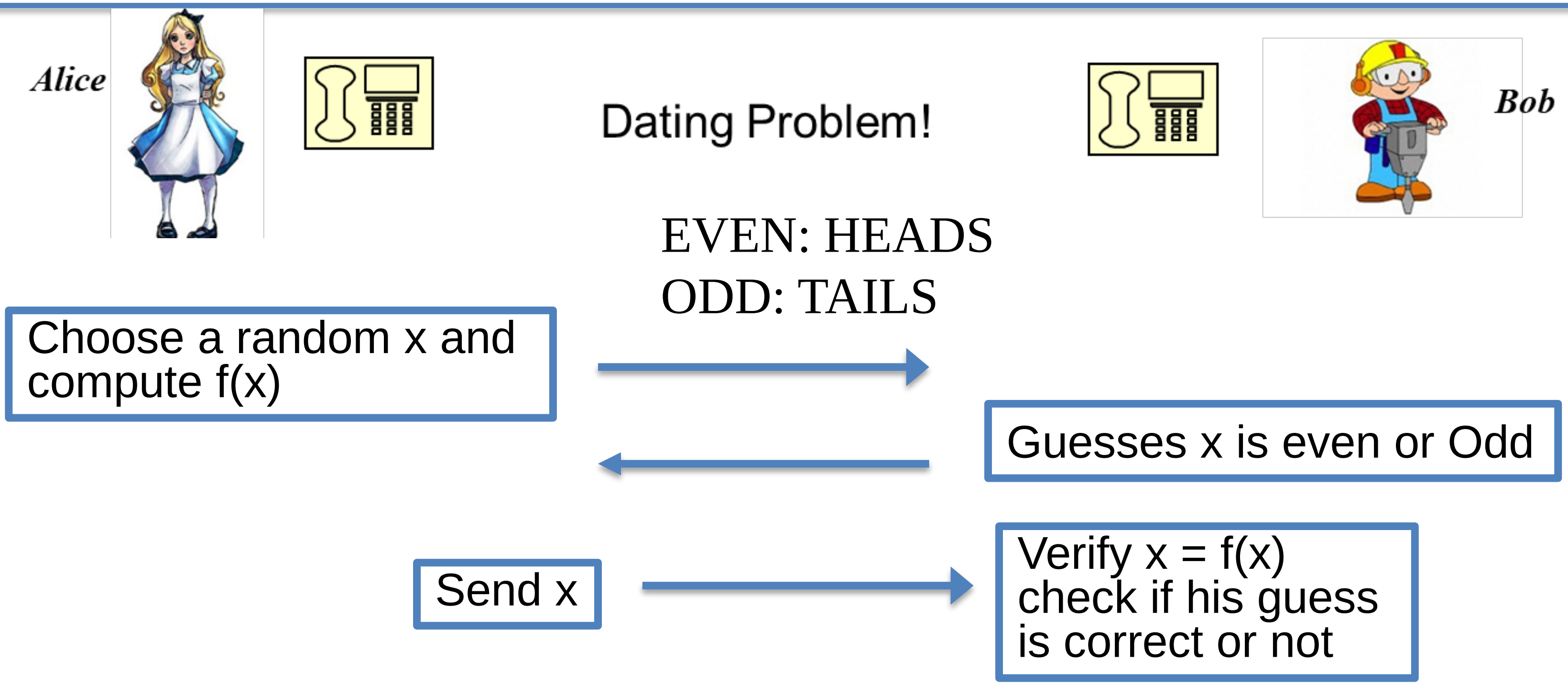
A. For every integer x, it is EASY to compute f(x) from x, however given a value for f(x) it is impossible to find x which is the pre-image of f(x), eg. To decide if x is odd or even

A. It is impossible to find a pair of integers with

x not equal to y and f(x) = f(y)

- Even number x in f(x) denotes EVEN and the other case denotes ODD.

A protocol



Dating Problem!

EVEN: HEADS
ODD: TAILS

Choose a random x and compute f(x)

Guesses x is even or Odd

Send x

Verify x = f(x) check if his guess is correct or not

Whoever wins the game decides the venue of the meeting!

Is this protocol correct and fair (unbiased)? Can you modify so that both Alice and Bob

If the line is not secure: Some questions

- They need to introduce traditional cryptography to secure the line
- Symmetric key or Asymmetric key?

- Or Use Different methods of communication where intruder cannot read the channel.
- We will discuss cryptographic solutions.

Models for Information Security

- Traditional Communication Model:
  - Alice and Bob is connected by insecure channel. Marvin, an adversary can listen to their conversation and modify if needed.
- Modern Network Model:
  - Network itself is an adversary. More than two participants. A valid participant also can be an adversary to others. Many models exist.

If the line is not secure: Some questions

- They need to introduce traditional cryptography to secure the line
- Symmetric key or Asymmetric key?

- Or Use Different methods of communication where intruder cannot read the channel.
- We will discuss cryptographic solutions.

If the line is not secure: Some questions

- They need to introduce traditional cryptography to secure the line
- Symmetric key or Asymmetric key?

- Or Use Different methods of communication where intruder cannot read the channel.
- We will discuss cryptographic solutions.

One-Way functions

- Does One Way functions exist?
- This simple question rises lots of philosophical issues. Cryptographers would like believe that they exist and have come up with many practical one-way functions.
- Do they have a clear cut proof for these claims?
- On the other hand, cryptanalysts believe in the opposite and work towards breaking the claims of cryptographers.

1.3 Classical example

COMP90043

Lecture 1

Diffie-Hellman Idea: Basics

- Two users want to share a common secret over a public network, Is this possible? Think!

- For a moment assume that we have a one way function.

- What is one way function?
  - Given x in domain it is easy to compute f(x)
  - Given y in range, it is difficult find x in domain such that f(x)=y

DH Continued

- Alice can create x in a domain (agreed in advance) –keep it secret,
- Compute f(x)– Send it to Bob over public channel
- Bob can create secret y in the domain and he also computes f(y) – Send it back to Alice
- Now both of them have f(x) and f(y)-
- If f is such that they can workout a common function of their secrets which others who observed f(x) and f(y) cannot compute, then one can attempt to have a solution to this problem.
- Diffie-Hellman in their 1974 paper give one such concrete solution! Please read it, you will love the idea.

Prime Numbers

- A number is said to be a prime number if p > 1 and p has no positive divisors except 1 and p.
- Example: $p = 2,3,5,7,11,13$
- The numbers which are not prime numbers are referred as composite numbers.
- For any integer n, $n > 1$, let $Z_n = \{0, 1, 2, \ldots, n\text{-}1\}$ be a set of numbers. This set is called the set of residues *modulo n*, as the elements are remainders of integers divided by the number *n*.
- We define the following operations on the set Z_n using the modulo operation.

$$x \oplus_n y = (x + y) \ mod \ n.$$

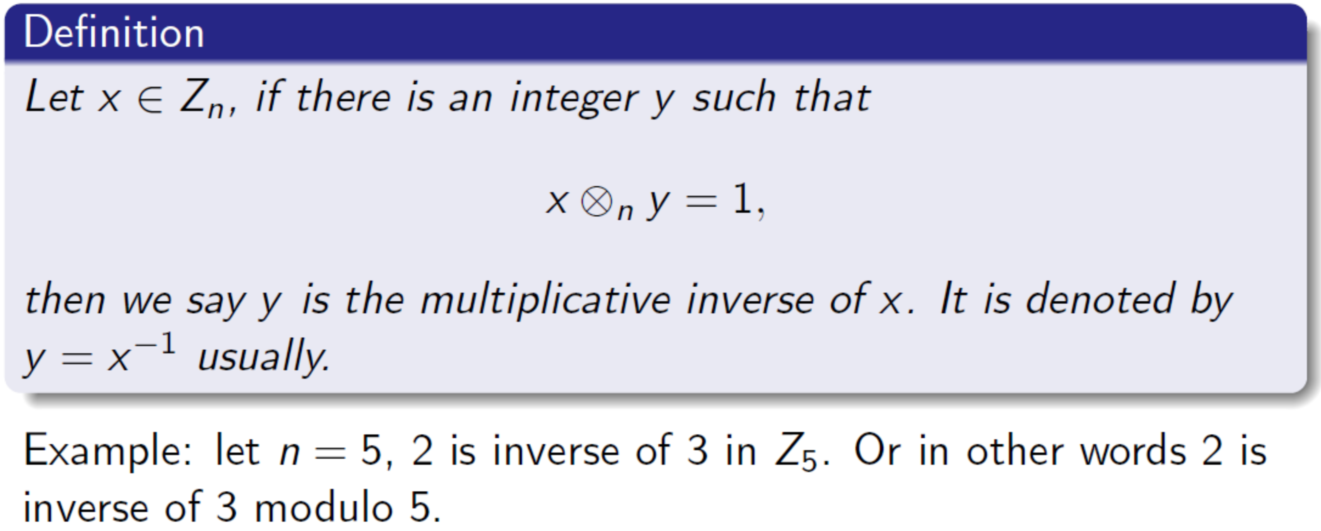
$$x \otimes_n y = (xy) \ mod \ n$$

Clock Arithmetic

- Example: $(6 + 7) \ mod \ 12 = 1$; $5 \times 4 \ mod \ 12 = 8;$
- In this lecture, *n* will only be a prime number.

Udaya Parampalli

Modular Inverse



Definition

Let $x \in Z_n$, if there is an integer y such that

$$x \otimes_n y = 1,$$

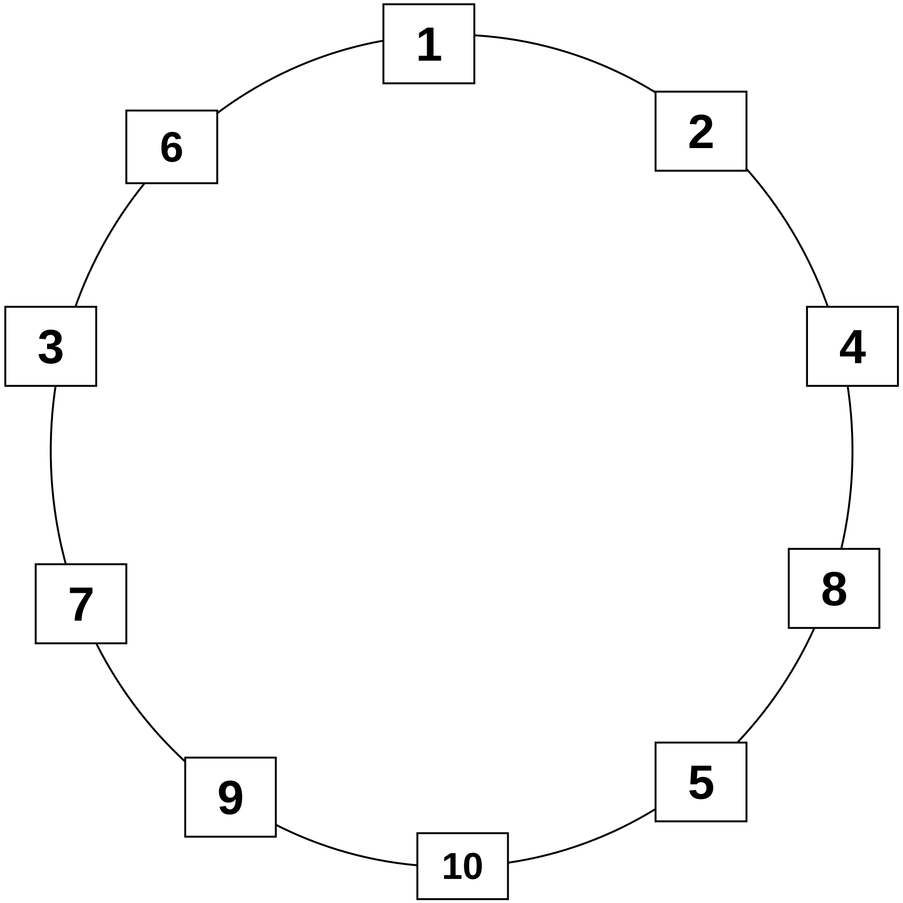
then we say y is the multiplicative inverse of x. It is denoted by $y = x^{-1}$ usually.

Example: let $n = 5$, 2 is inverse of 3 in Z_5. Or in other words 2 is inverse of 3 modulo 5.

We can now define a cyclic group over nonzero elements of Z_p when p is prime.
Let $Z^*_p = \{1, 2, 3, \ldots, (p-1)\}$. Let g be an element of Z^*_p such that
$Z^*_p = \{g, g^2, g^3, \ldots, g^{p-1}=1\}$, (*you can always find such an element g)

*We do not cover this idea here, it requires more study; those interested can see the textbook

An example



g^i	$g^i \bmod p$	$Dlog(g^i)$
2^1	2	1
2^2	4	2
2^3	8	3
2^4	5	4
2^5	10	5
2^6	9	6
2^7	7	7
2^8	3	8
2^9	6	9
2^{10}	1	10

Example of a Cyclic group modulo $p = 11$

g : generator = 2

Order(size) of G = 10

What power of 2 is 3?

The Example of One Way Function

X	2^x mod 11
0	1
1	2
2	4
3	8
4	5
5	10 Or -1
6	9
7	7
8	3
9	6
10	1
11	2

Discrete Logarithm Problem (DLP)

Let ‘*g*’ and ‘*h*’ be elements of the group G. Then the discrete logarithm (DL) problem is the problem of finding ‘*x* ’ such that $g^x = h$.

For example, the solution to *x* in the problem:

$3^x = 13 \pmod{17}$ -> $x = 4$, because $3^4 = 81 = 13 \ (mod\ 17)$.

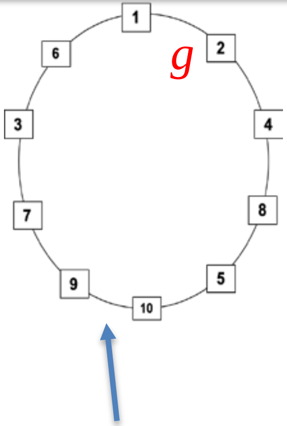
- o The discrete log problem is believed to be hard. Therefore it has become the basis of several public key schemes, for example: El-Gamal.
- o Next, we will consider the Diffie-Hellman protocol, the first public key algorithm.
- o The protocol is defined over a cyclic group: $Z^*_p = \{g, g^2, g^3, \ldots, g^{p-1}=1\}$,

Udaya Parampalli

Diffie-Hellman Key Establishment Protocol

- Alice Bob
- Choose Na=2 → Choose Nb=6
- $g^{Na} = 2^2 = 4 = Ma$
- ← $g^{Nb} = 2^6 = 9 = Mb$
- Compute
- $K_{ab} = Mb^{Na}$
- $= 9^2 = 4$
- Compute
- $K_{ba} = Ma^{Nb} = 4^6 = 4$
- $K_{ab} = K_{ba} = 4$

Diffie-Hellman Protocol



All arithmetic under *mod* $p=11$

Alice $p=11, g=2$ **Bob**

Choose Na=2 Eve

Choose Nb=6

$g^{Na} = 2^2 = 4 = Ma$ $g^{Nb} =$

$2^6 = 9 = Mb$

Compute

$K_{ab} = Mb^{Na} = (g^{Nb})^{Na}$

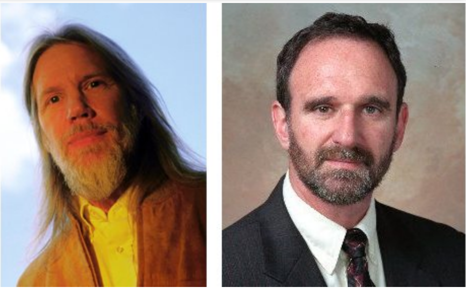
$= 9^2 = 4$

Compute

$K_{ba} = Ma^{Nb} = (g^{Na})^{Nb}$

$= 4^6 = 4$

$K_{ab} = K_{ba} = 4 = (g^{NaNb})$



Whitfield Diffie
and
Martin Hellman

Image from Wikimedia Commons

Clearly a solution to DL implies a solution to CDH

Is the converse True?*

* Open Problem

CDH PROBLEM → Problem for Eve in the above protocol

Let G be a cyclic group of size q and g be a generator of the group G. Given g^a and g^b, two arbitrary elements of the group G for some integers a and b in the range: $0 \leq a, b \leq q$, then find g^{ab}

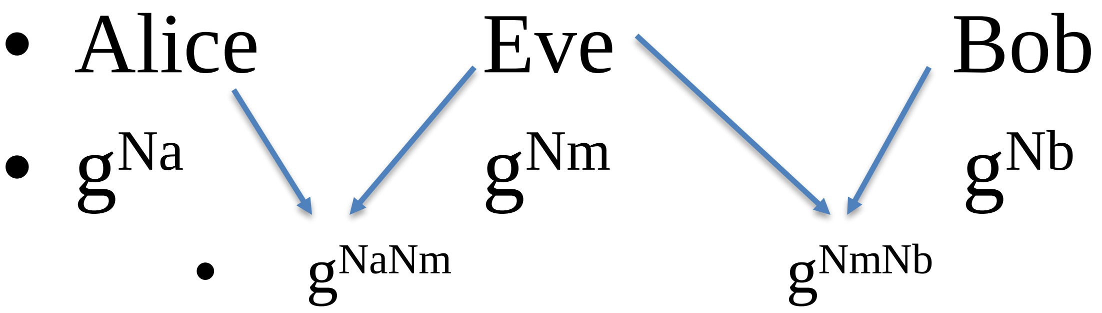
Normally G is a multiplicative group in a suitable finite field.

New directions in Cryptography, IEEE Trans. Inf. Theory 22(6): 644-654 (1976)

Issues wit this Protocol: Secure?

- Exchanged data -only g^{Na} and g^{Nb}
- So Alice cannot guess N_b nor Bob can guess N_a
- So their secrets are safe from each other
- But also none can guess Na and Nb for the same reason
- Both Alice and Bob can compute common secret g^{NaNb}
- It is also believed that g^{NaNb} cannot be computed by others who can only see g^{Na} and g^{Nb}
- The later problem is known as Computational Diffie-Hellman problem (Hard!)

Man in the Middle Attack

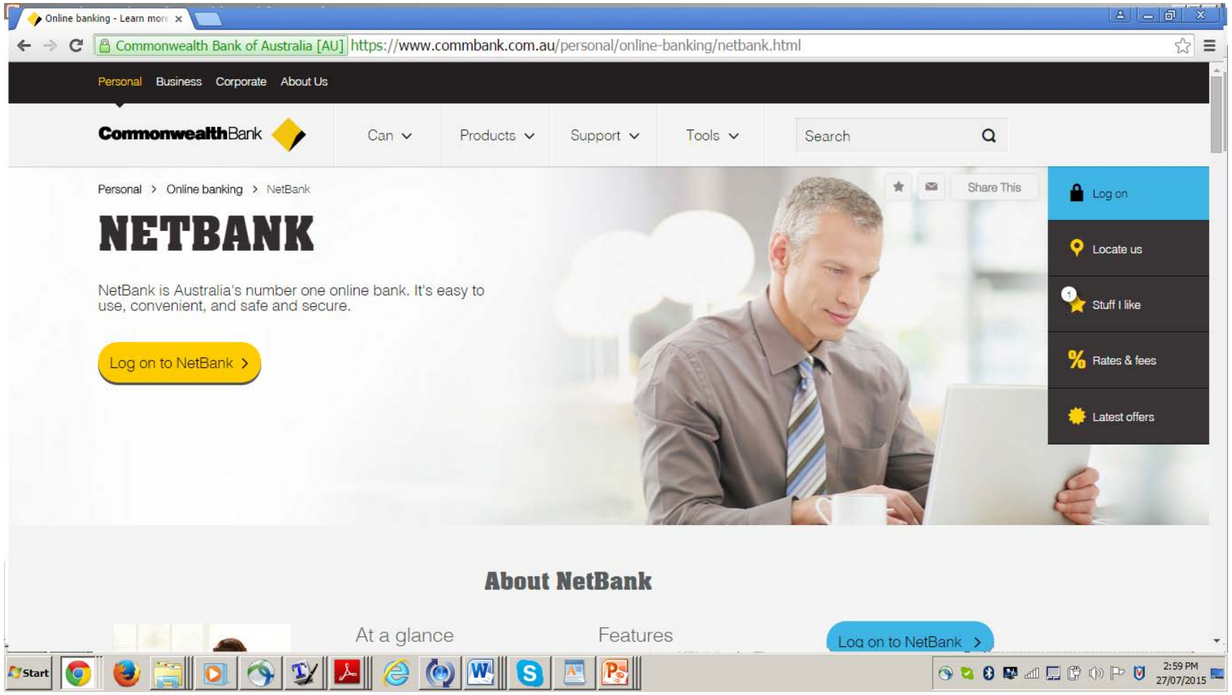


- Alice Eve Bob
- g^{Na} g^{Nm} g^{Nb}
  - g^{NaNm} g^{NmNb}

- Marvin comes in between Alice and Bob, and he can create two secrets one with Alice and the other with Bob.
- This is possible because when Bob receives communication from Alice, there is no way for him to determine if it indeed come from Alice, in other words, the messages are not authenticated.
- A way to solve this problem is by using digital signatures! –We will revisit these ideas when we visit Public Key topics later in the semester.

In Practice

Comm bank Server



Online banking - Learn more ×

Commonwealth Bank of Australia [AU] https://www.commbank.com.au/personal/online-banking/netbank.html

Personal Business Corporate About Us

CommonwealthBank Can Products Support Tools Search

Personal > Online banking > NetBank

Share This

NETBANK

NetBank is Australia's number one online bank. It's easy to use, convenient, and safe and secure.

Log on to NetBank >

Log on

Locate us

Stuff I like

Rates & fees

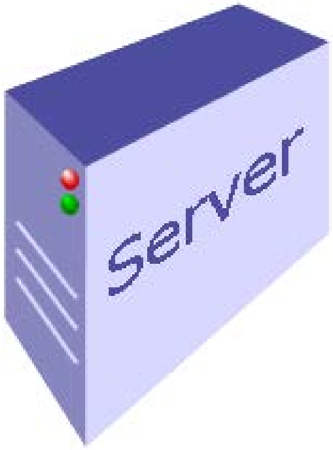
Latest offers

About NetBank

At a glance Features Log on to NetBank >

Start

2:59 PM 27/07/2015



© University of Melbourne, 2020
Udaya Parampalli

1.4 Basic Security Objectives

COMP90043

Lecture 1

Three important concerns of Information security

- Confidentiality
  - In simple terms, confidentiality of information or data ensures that the access is given only to authorized individuals.
- Integrity
  - Information integrity ensures that enough safe guarding mechanisms exists so that authorized individuals get the **right** information and any changes to the information by intentional and un intentional means will be detected.
- Availability
  - Information or data availability ensures that the information is authorized available to the users.

From the textbook definitions

OSI Security Architecture

- How to define the requirements for security in networked world and characterizing the approaches to satisfy those requirements?

- Refer to ITU-T X.800 “Security Architecture for OSI”
  - It defines a systematic way of defining and providing security requirements

- Three main aspects:
  - Security attacks
  - Security Mechanisms.
  - Security services.

Security Attack

- *Attack* is any action that compromises the security of information owned by an organization
- *Threat* is a possible potential for violation of security,

- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing (threat is attack in waiting)
- Generally we have a wide range of attacks:
- Some generic types of attacks:
  - passive
  - active

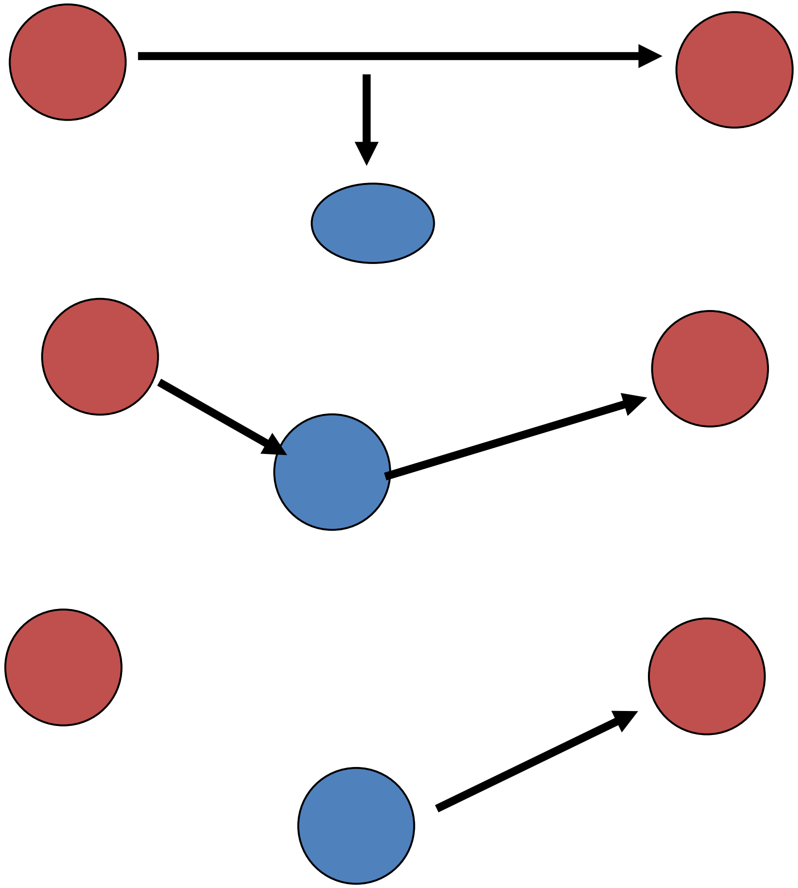
Basics Security Services

We concentrate on Implementation and Mechanism aspects of Information Security.

- Authentication
- Confidentiality
- Integrity
- Nonrepudiation
- Availability

Security Threats in Networked World

- Security services are defined to address or withstand threats



Interception

Confidentiality

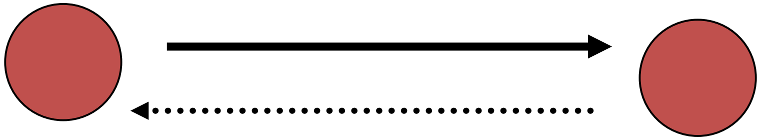
Modification

Integrity

Fabrication

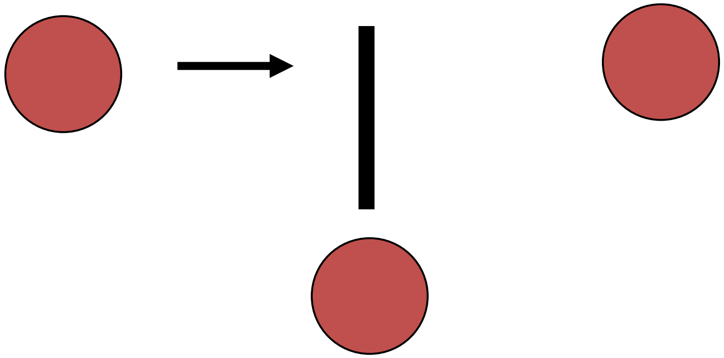
Confidentiality
Authentication

Security Threats in Networked World



Non-Repudiation

Source Authentication



Interruption

Network QOS

Model for Network Security (Textbook)

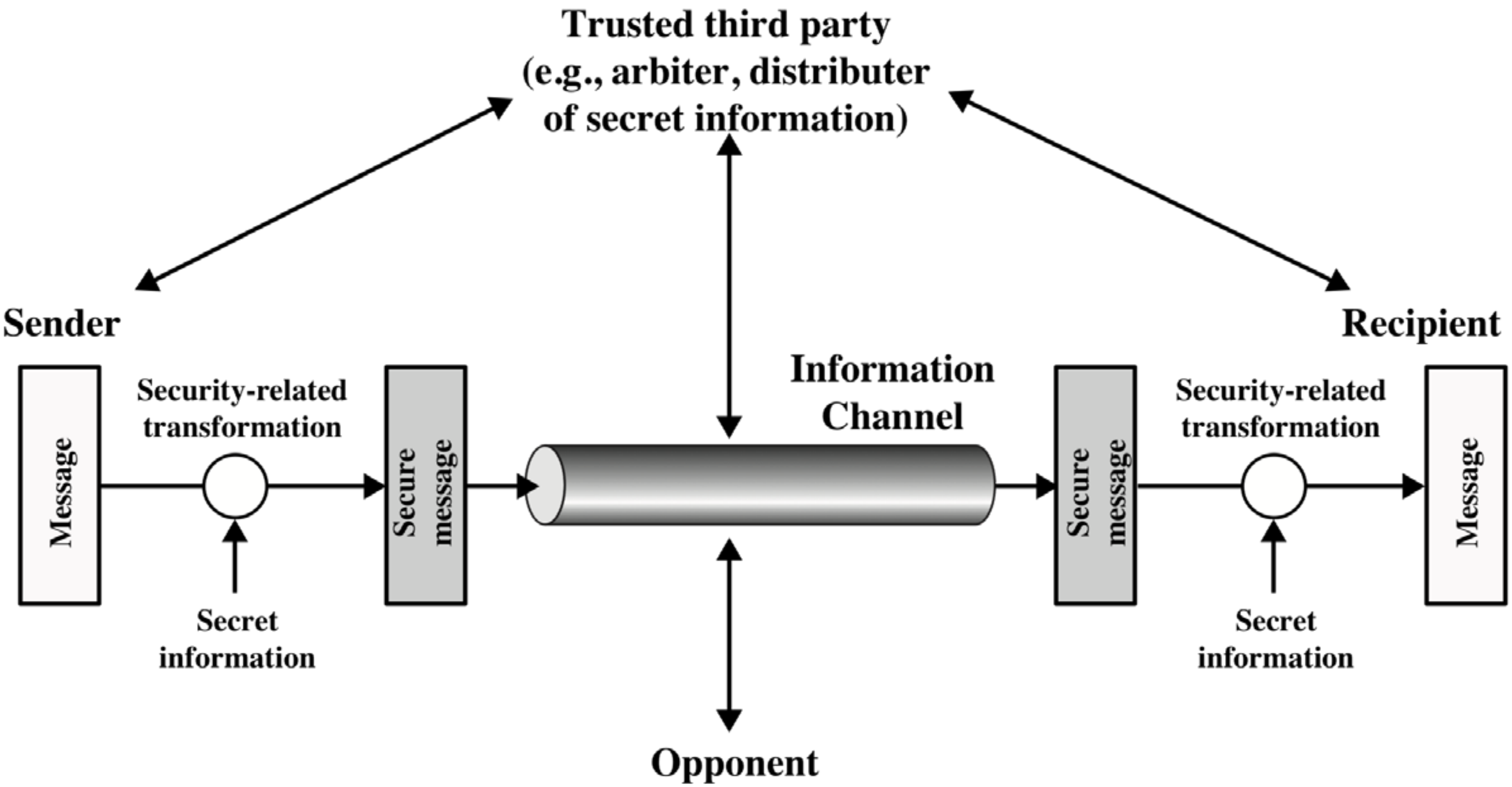
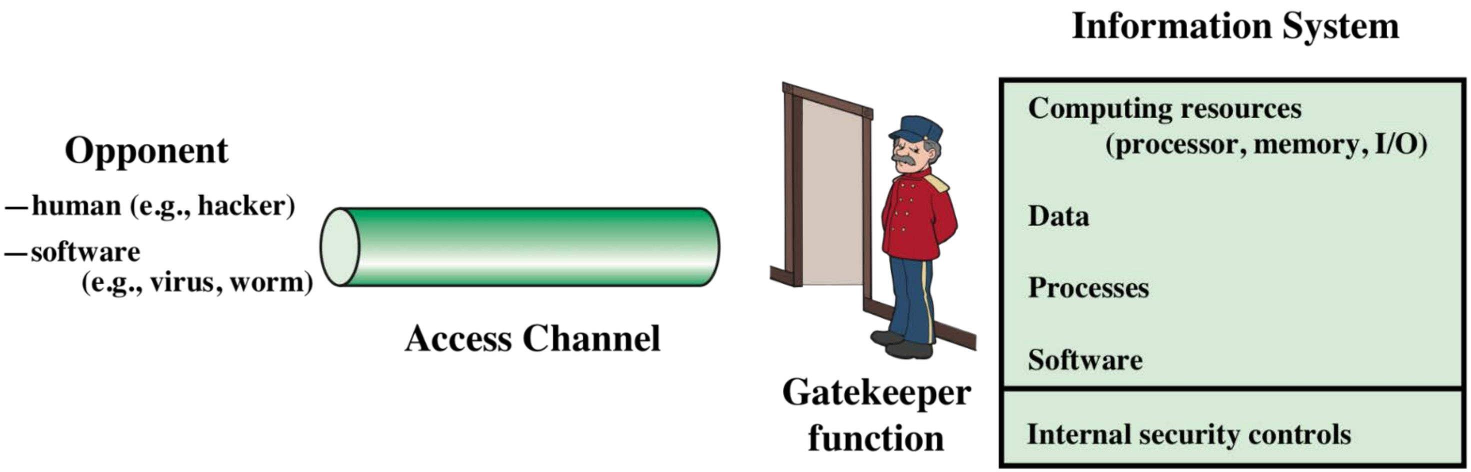


Figure 1.2 Model for Network Security

Source: WilliamStallings, Cryptograph and Security

Network Access Security Model



Information System

Opponent

—human (e.g., hacker)

—software
(e.g., virus, worm)

Access Channel

Gatekeeper function

Computing resources
(processor, memory, I/O)

Data

Processes

Software

Internal security controls

Figure 1.3 Network Access Security Model

Source: WilliamStallings, Cryptograph and Security

Week 1

Overview Lecture

Subject Overview

Lecture 1

Introduction to cryptography.

Lecture 2

Workshops start from Week 2

Quiz 1