Introduction

- **Role of Cryptography in Information Security**
  - **Definitions, A story of Alice and Bob, terms and notations**
- **Motivating Examples**
- New view point: A Communication Game
- Diffie-Hellman Protocol
- Basic Security Objectives

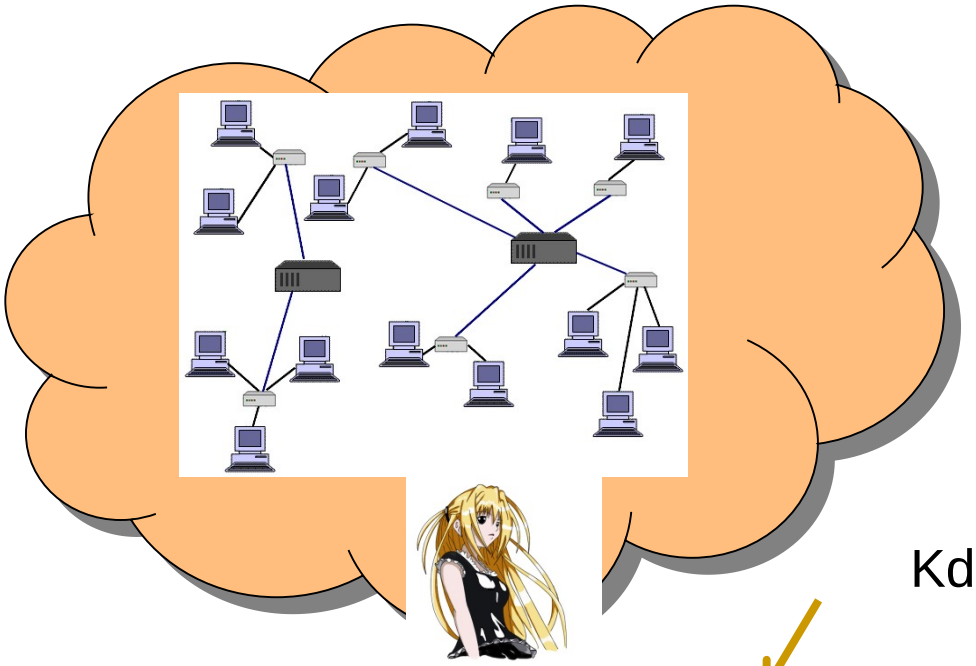
Information Security

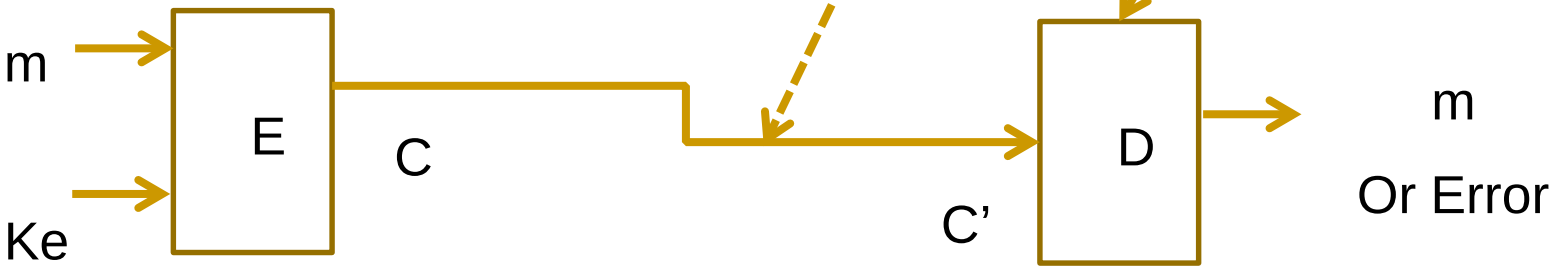
- What is Cryptography
  - “Secret Writing”
  - Refers to the techniques required for protecting data between authorized parties on information communication technologies in the presence of potentially malicious elements.
  - Refers to a range of techniques such as Encryption, Signature, Hash functions, 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.

What does the field of network and Internet security Consists of?

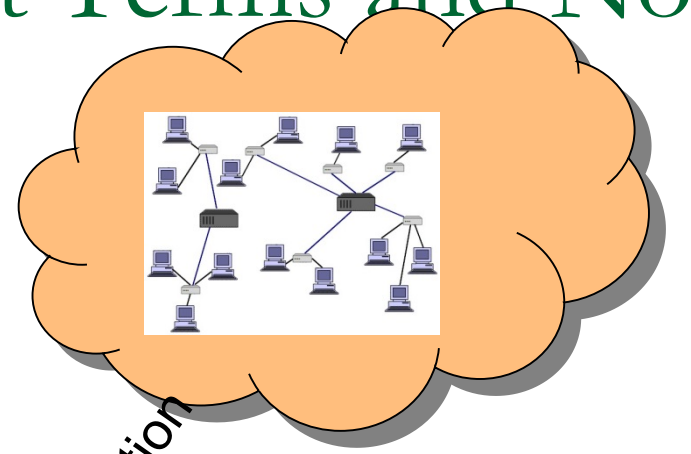
- Stallings Take:
  - The field of network and Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.
- Our approach is to some study basic cryptographic primitives such as symmetric and public key cryptography,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

A story of Alice and Bob





Important Terms and Notations



Bob

Alice

Encryption Function

Decryption Key
(Private)

Kd

Plain Text

m

Ke

E

C

tampering

Eve

eavesdropping

C'

D

m

Or Error

Encryption Key
(Public/Private)

Received Cipher Text
(Could be in error)

Decryption Function

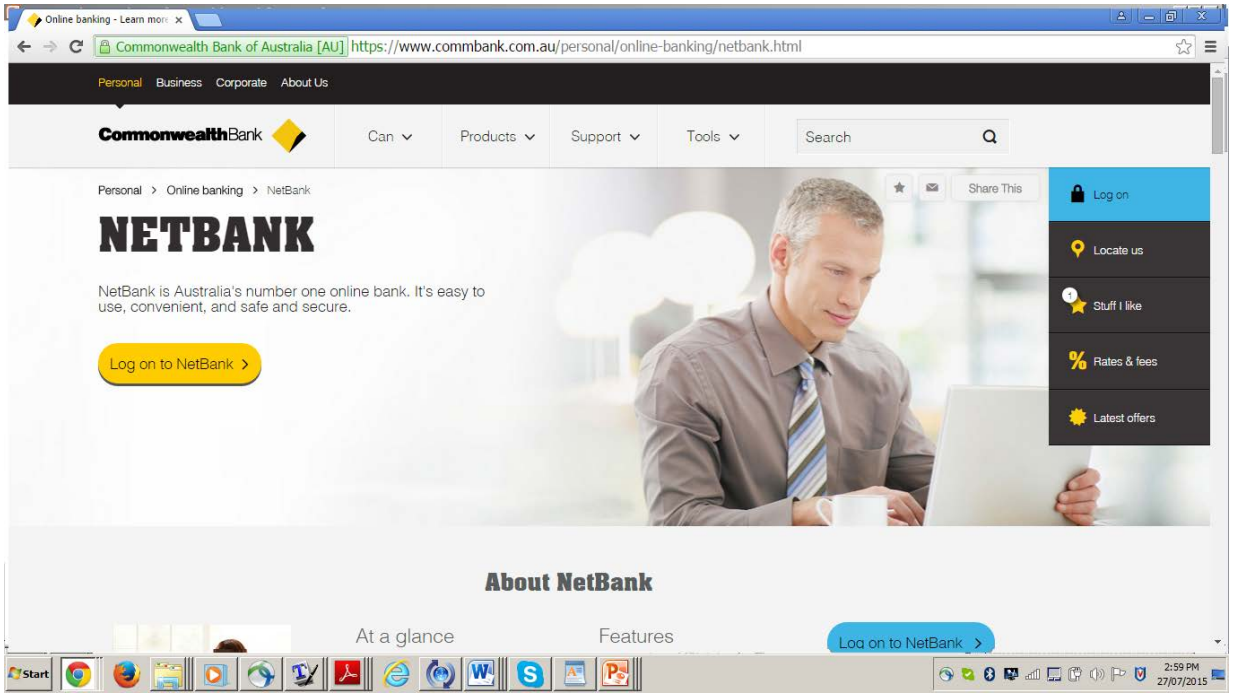
E, D are public;

Keys determine security

Differences

- Ke = Kd → Symmetric key also sometimes referred as private key. But we shall call always symmetric key-
  - Known since antiquity.
- Ke ≠ 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.

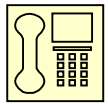
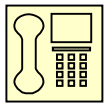
Motivating example: In Practice



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


- Dating Problem!
- 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. They are in different offices connected by a telephone.
- They need to book the program in advance and want to make a decision over the phone.
- Can you help them?

A Cryptographic Solution Using Mathematics!

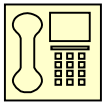
- Assume we have a magic function with

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

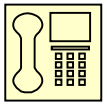
B. It is impossible to find a pair of integers with x not equal to y and f(x) = f(y)

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

A protocol



Alice



Bob

EVEN: HEADS
ODD: TAILS

Choose a random x and
compute f(x) ----------→

←----------Guesses x is even or Odd

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

Whoever wins the game decides the venue of the meeting!

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

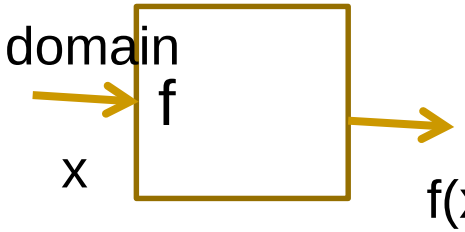
- Traditional Communication Model: Alice and Bob is connected by insecure channel. Marvin, an adversary can listen to their conversation and modify if needed.

- 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.

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.

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

Easy and Difficult! – not easy ☺

DH Continued

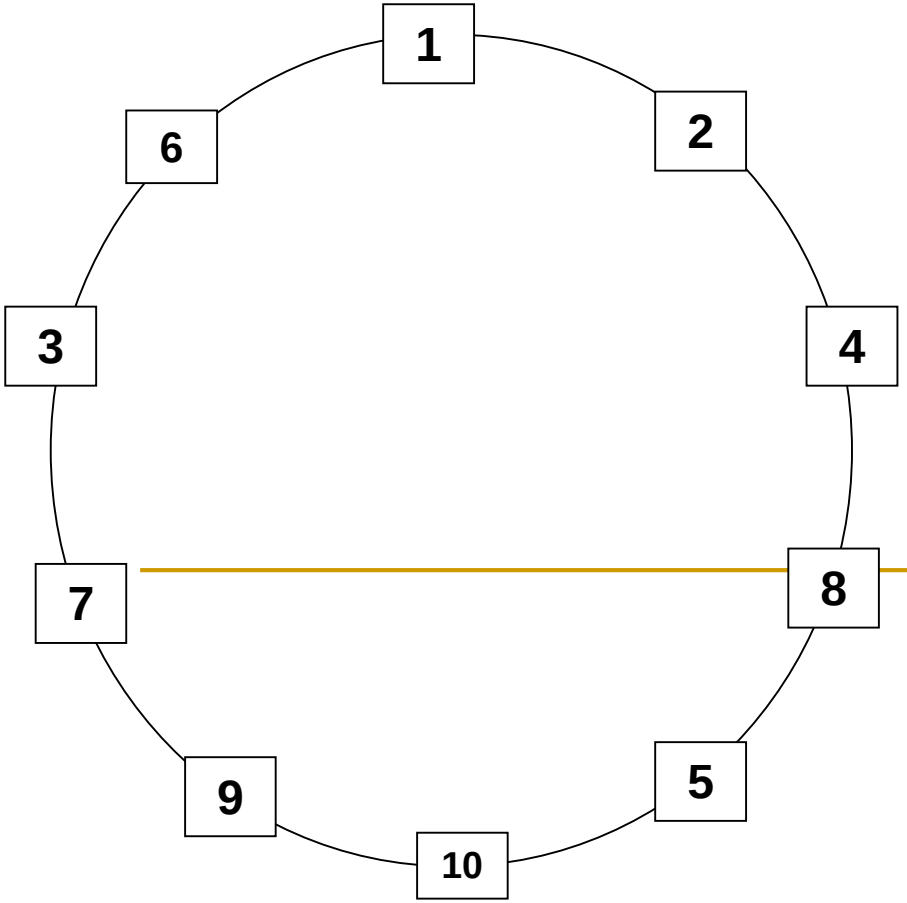
- Alice can create x in a domain (agreed in advance) –keep it secret,
- Compute f(x)– Send it to Bob over public channel
- Bob can create secret y in the domain and he also computes f(y) – Send it back to Alice
- Now both of them have f(x) and f(y)-
- If f is such that they can workout a common function 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.

Discrete Logarithm Problem

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

  $3^x = 13 \pmod{17}$ is 4, because

  $3^4 = 81 = 13 \pmod{17}$.
- The discrete log problem is believed to be difficult.
- Now note that given g and h, computing g^h, exponentiation is easy (polynomial in no of bits in h).
- The inverse is believed to be hard in certain groups.



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

One Way Function Example

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

Diffie-Hellman Key Establishment Protocol

p=11, g =2: Public

- Alice
- Choose Na=2
- $g^{Na} = 2^2 = 4 = Ma$

Bob

Choose Nb=6

$g^{Nb} = 2^6 = 9 = Mb$

- Compute
- $K_{ab} = Mb^{Na}$
- $= 9^2 = 4$

Compute

$K_{ba} = Ma^{Nb} = 4^6 = 4$

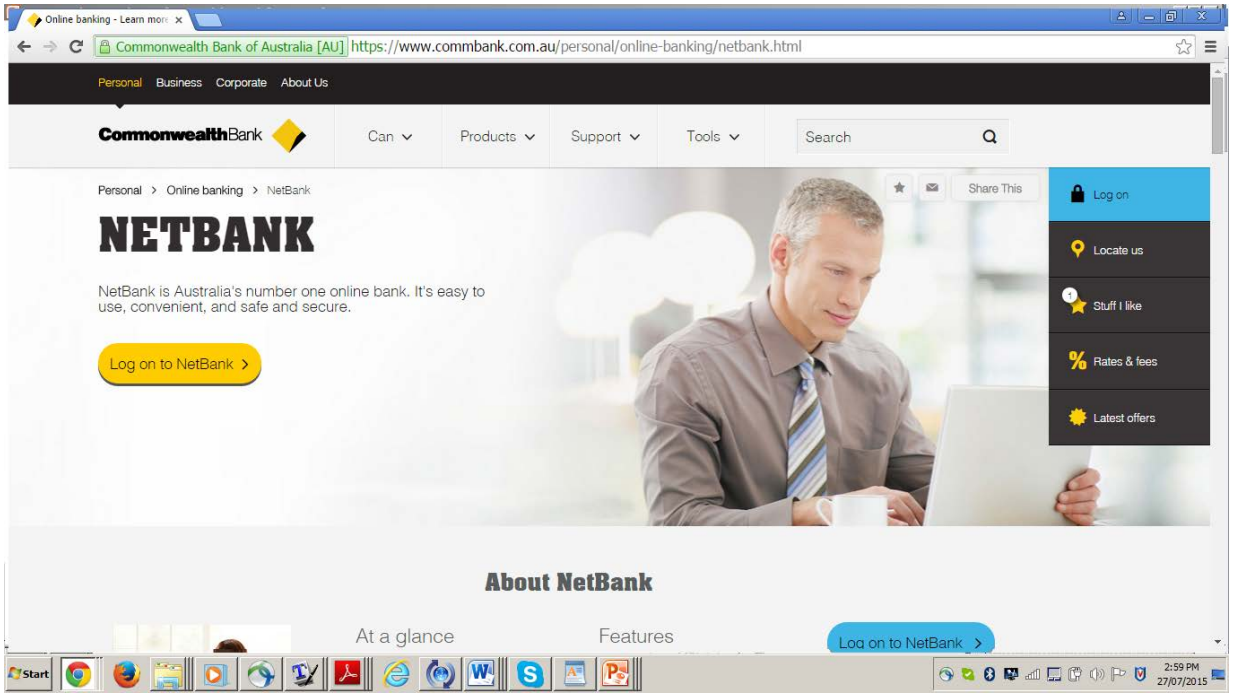
$K_{ab} = K_{ba} = 4$

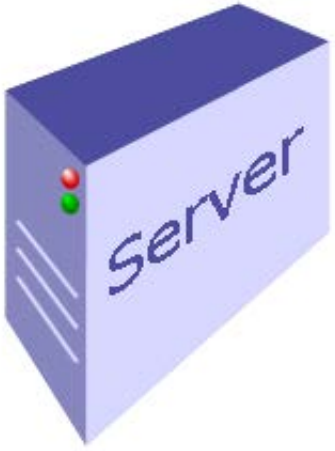
Issues wit this Protocol: Secure?

- 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!)

In Practice

Comm bank Server





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.

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

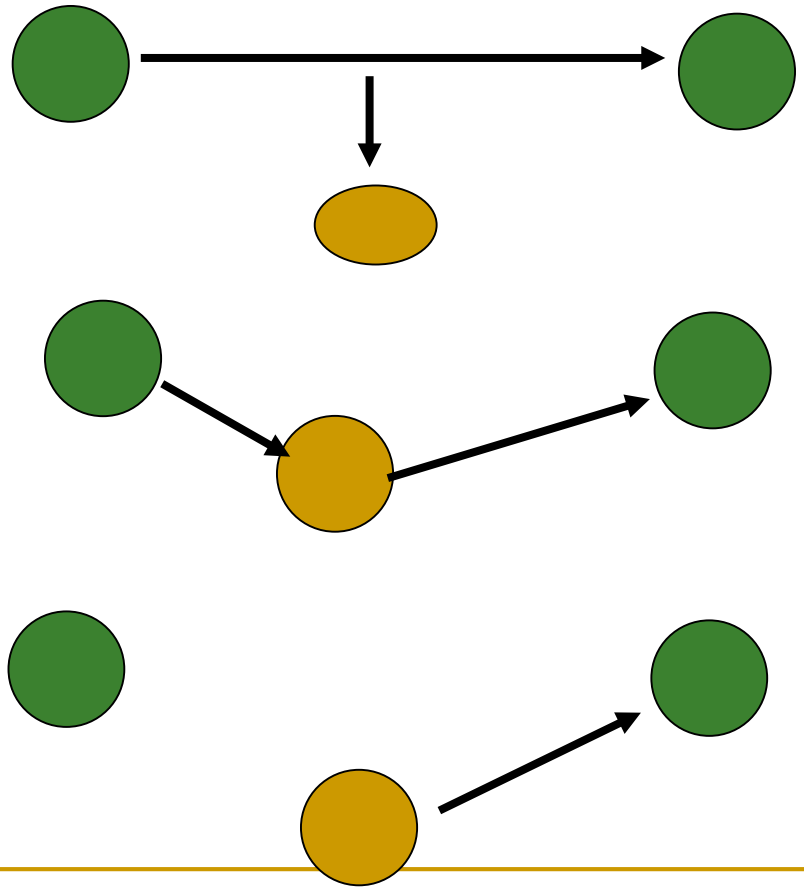
- Attack is any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing (threat is attack in waiting)
- Generally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

Basics Security Services

- Authentication
- Confidentiality
- Integrity
- Nonrepudiation
- Availability

Security Threats

Security services are defined to address or withstand threats



Interception

Confidentiality

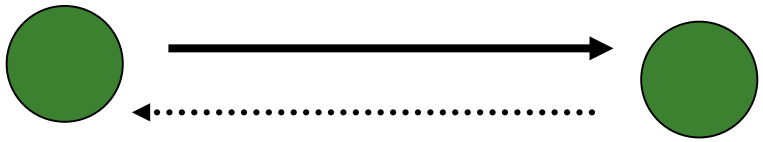
Modification

Integrity

Fabrication

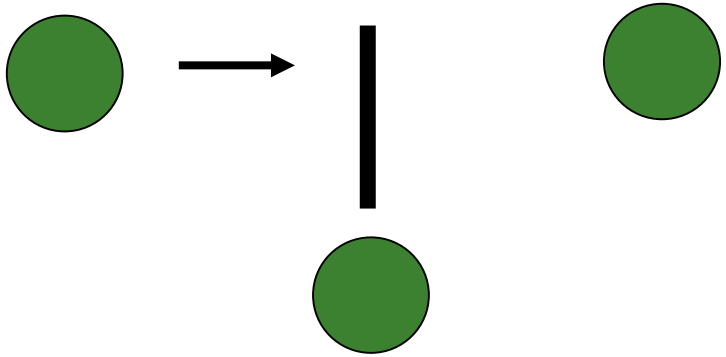
Confidentiality
Authentication

Security Threats. Cont.



Non-Repudiation

Source Authentication



Interruption

Network QOS

Model for Network Security

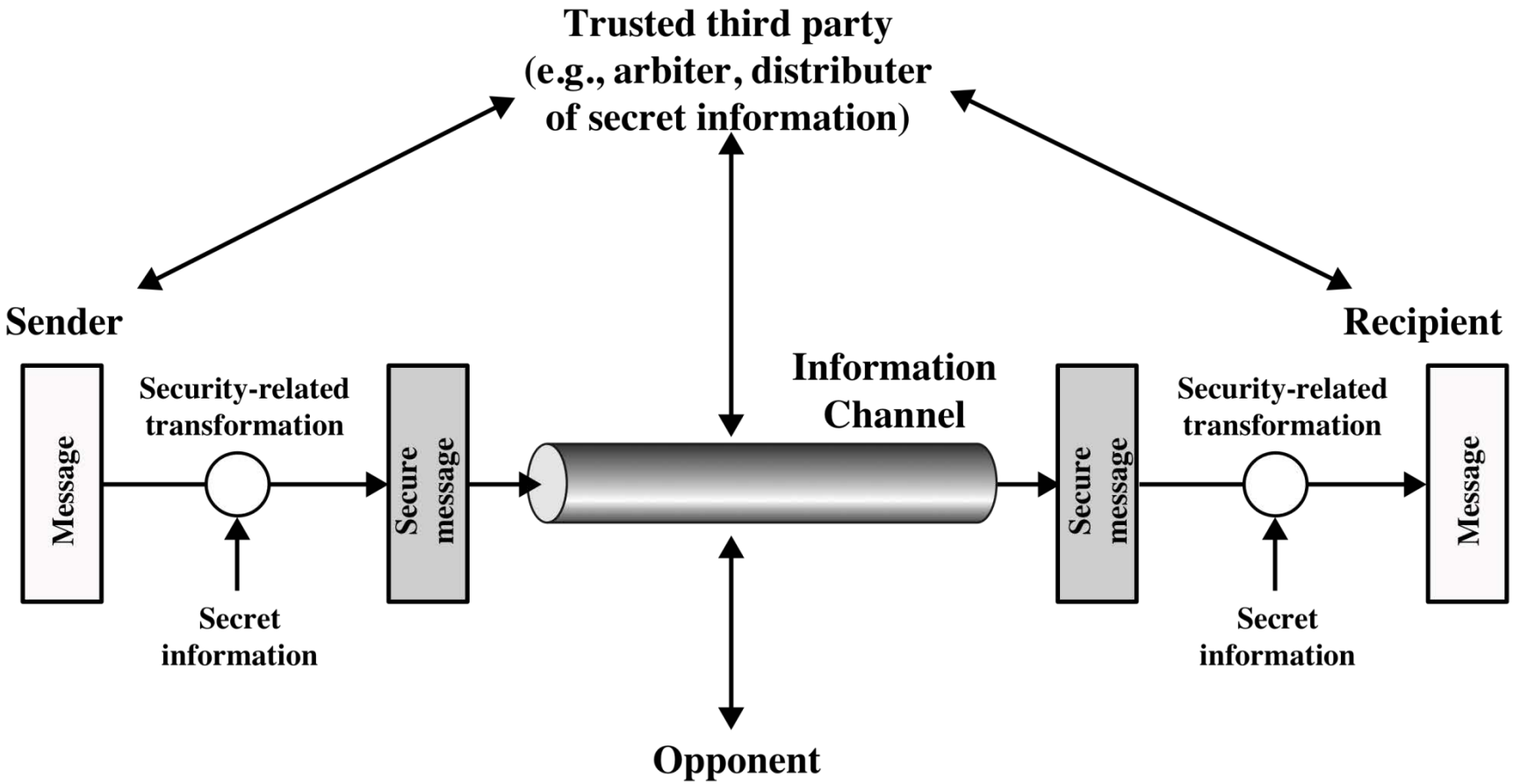


Figure 1.2 Model for Network Security

Network Access Security Model

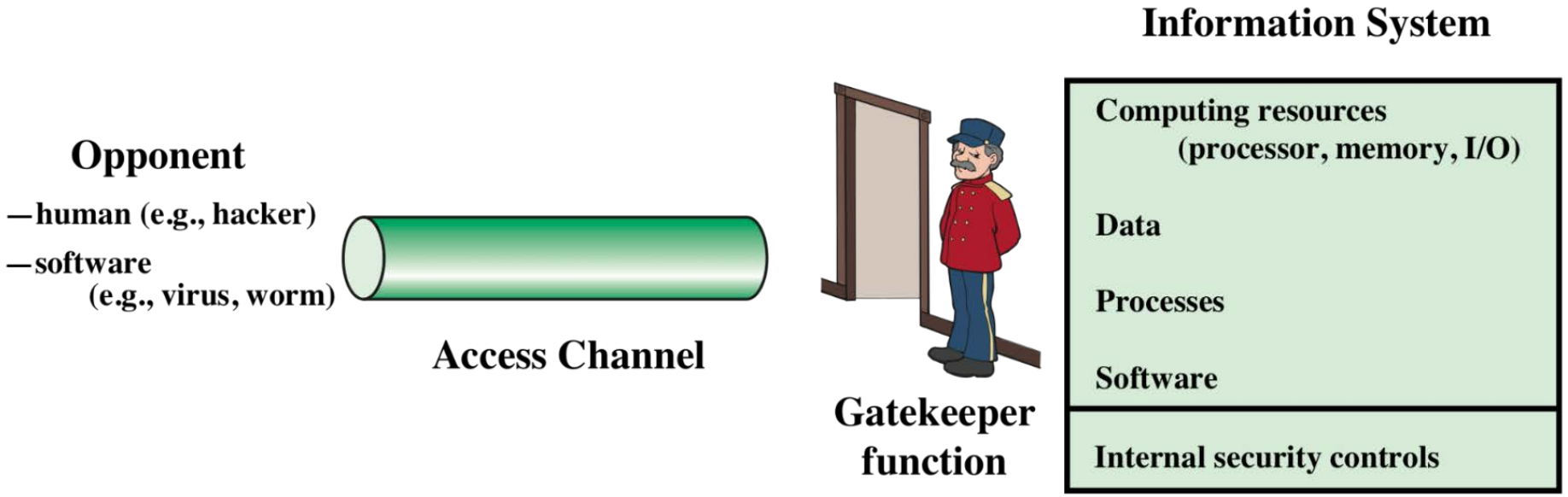


Figure 1.3 Network Access Security Model