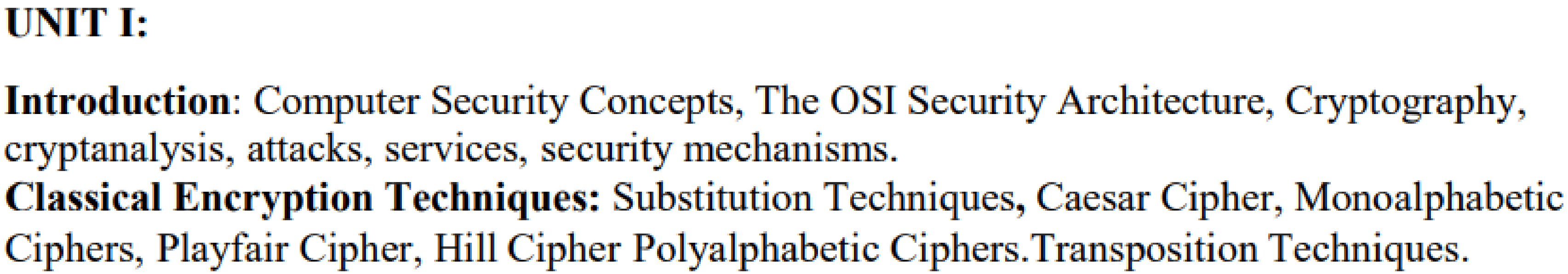
CRYPTOGRAPHY AND NETWORK SECURITY

Cryptography and Network Security ECS401



UNIT I:

Introduction: Computer Security Concepts, The OSI Security Architecture, Cryptography, cryptanalysis, attacks, services, security mechanisms.
Classical Encryption Techniques: Substitution Techniques**,** Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Hill Cipher Polyalphabetic Ciphers.Transposition Techniques.

Arif Mohammad Abdul

GITAM

(Deemed to be University)

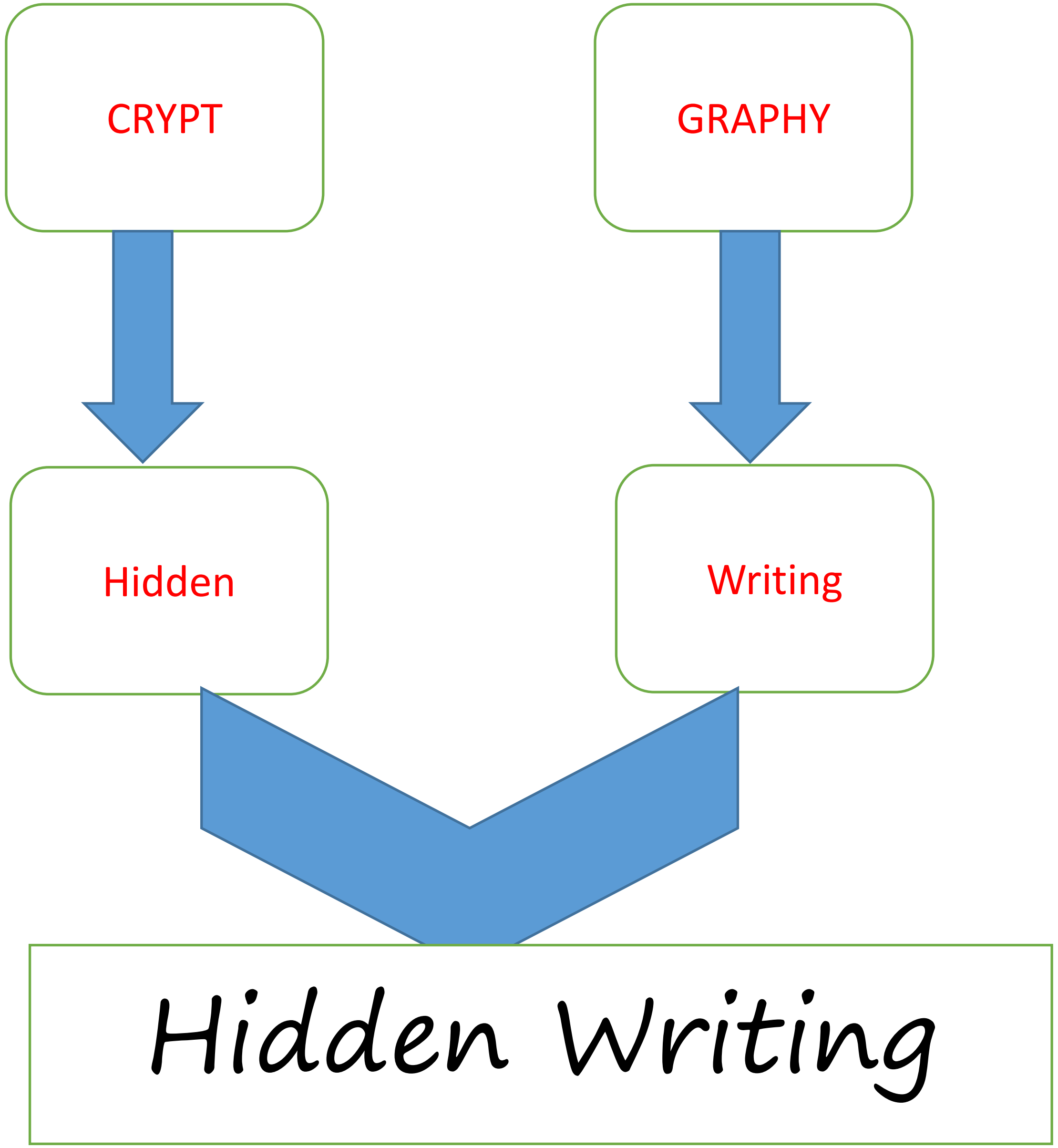
What is
Cryptography?

The art of secret writing

ajkw okf 34kfj 4ojf 4Akakk jruidjo nsjeoj njoe nof lkdieun menr nokr eojr koit roj toek.

Non Readable

CRYPTOGRAPHY



CRYPT

Hidden

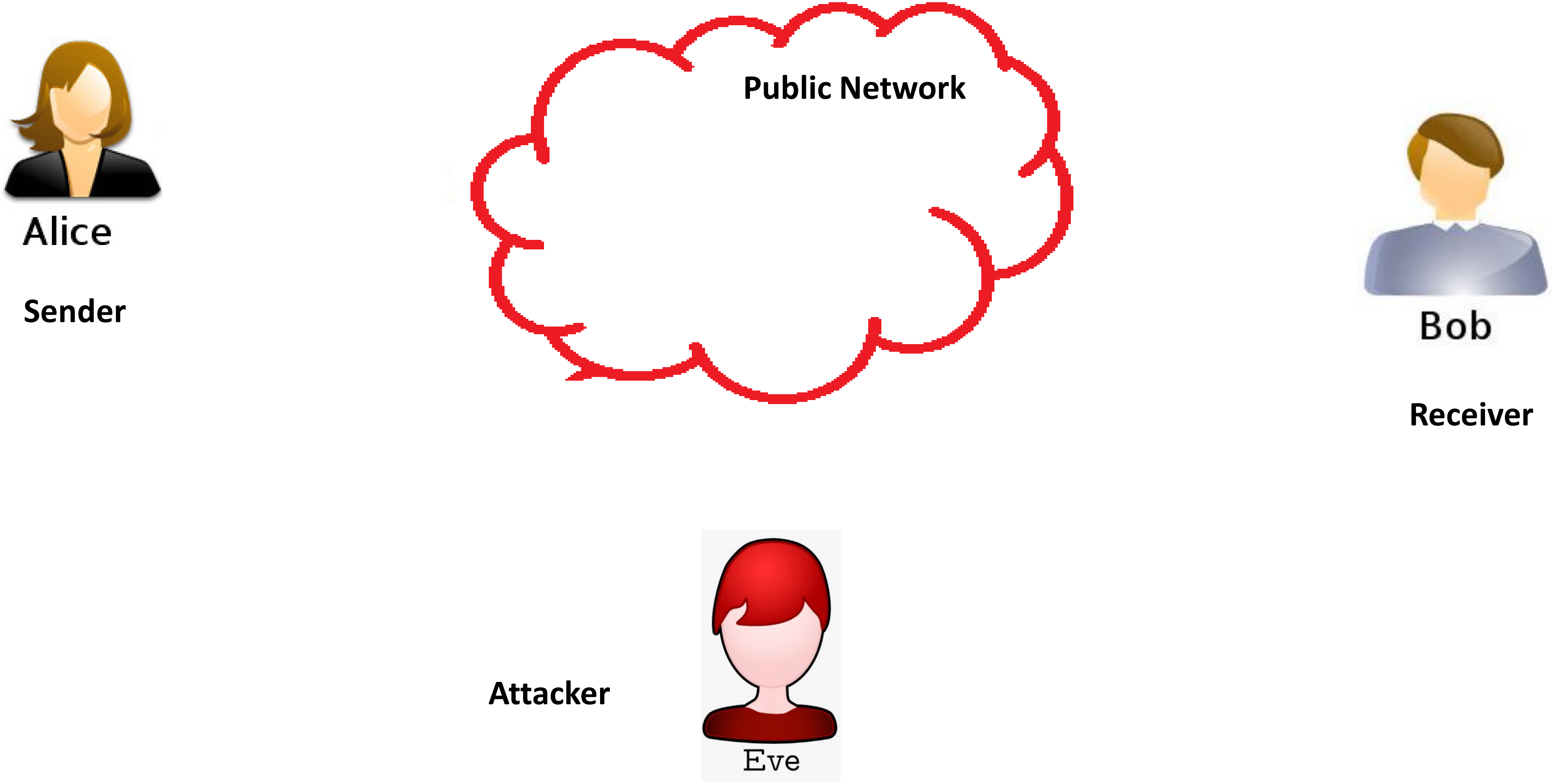
GRAPHY

Writing

Hidden Writing

Ancient Greek Language

Alice, Bob and Eve Framework



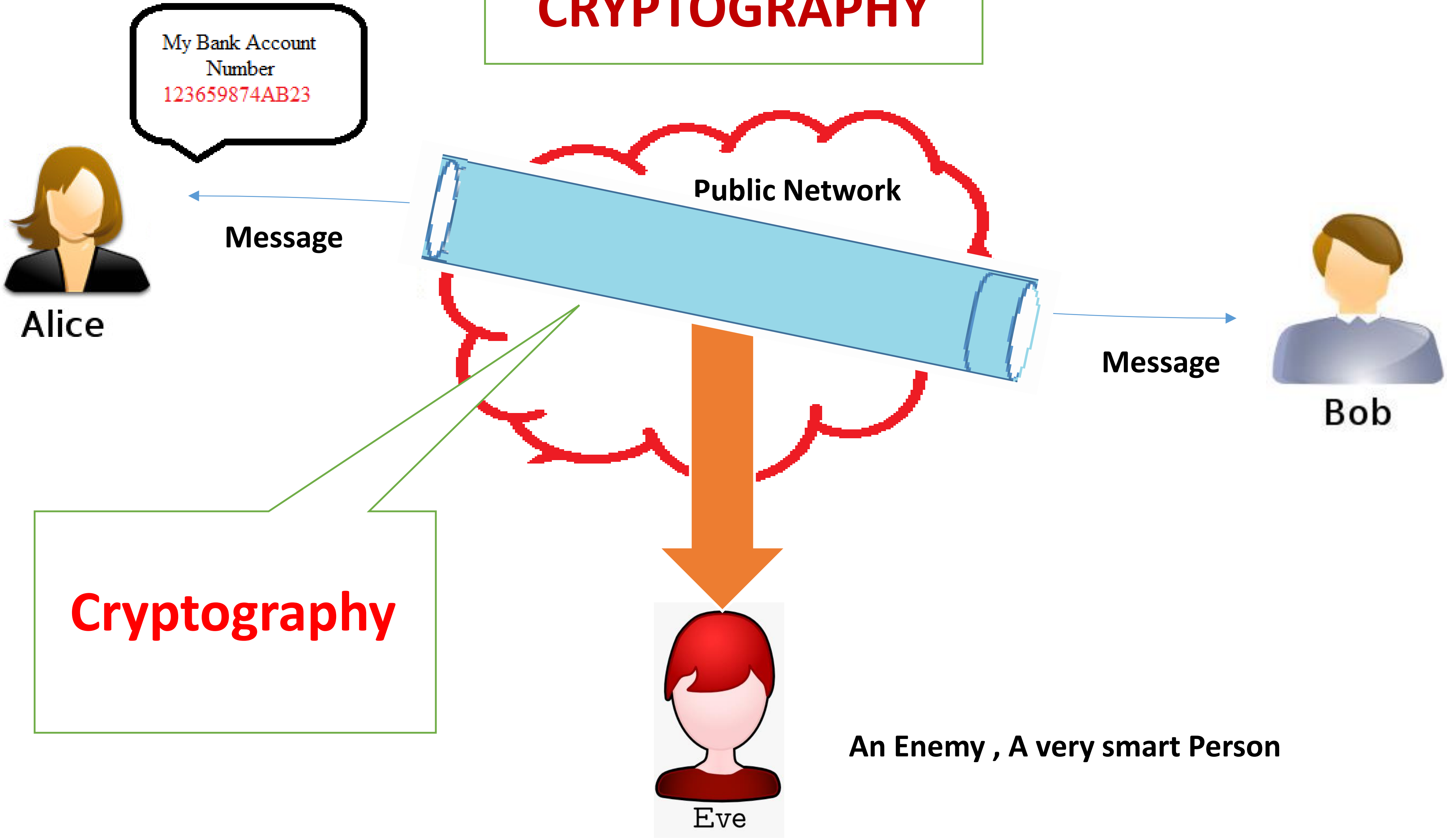
Public Network

Sender

Receiver

Attacker

CRYPTOGRAPHY



Cryptography

An Enemy , A very smart Person

CRYPTOGRAPHY

Definition

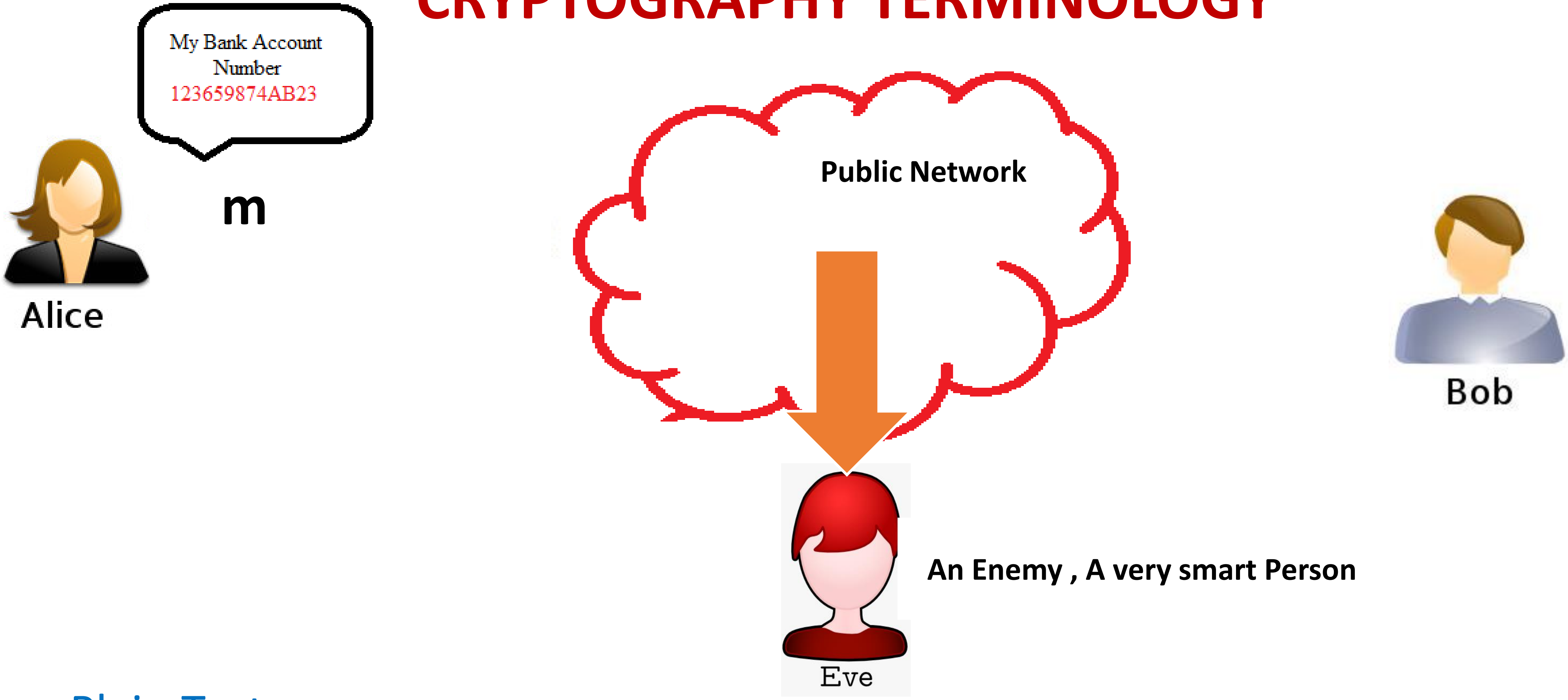
Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries

CRYPTOGRAPHY

Definition

Cryptography is the art of achieving security by encoding messages (plain text) to make them non-readable (cipher text).

CRYPTOGRAPHY TERMINOLOGY



My Bank Account Number 123659874AB23

m

Alice

Public Network

Bob

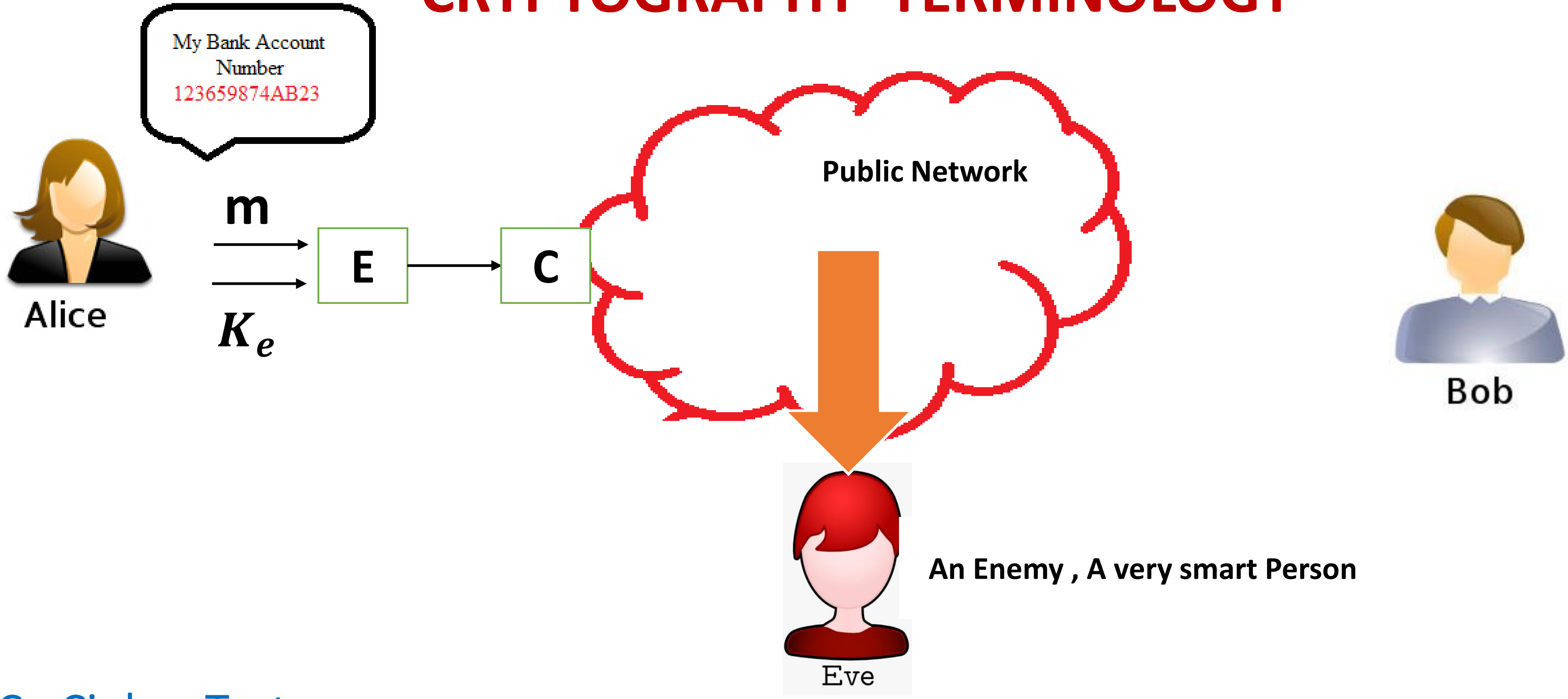
Eve

An Enemy , A very smart Person

m : Plain Text

Clear text or plain text signifies that can be understood by the sender, the receiver, and also anyone else who gets an access to that message

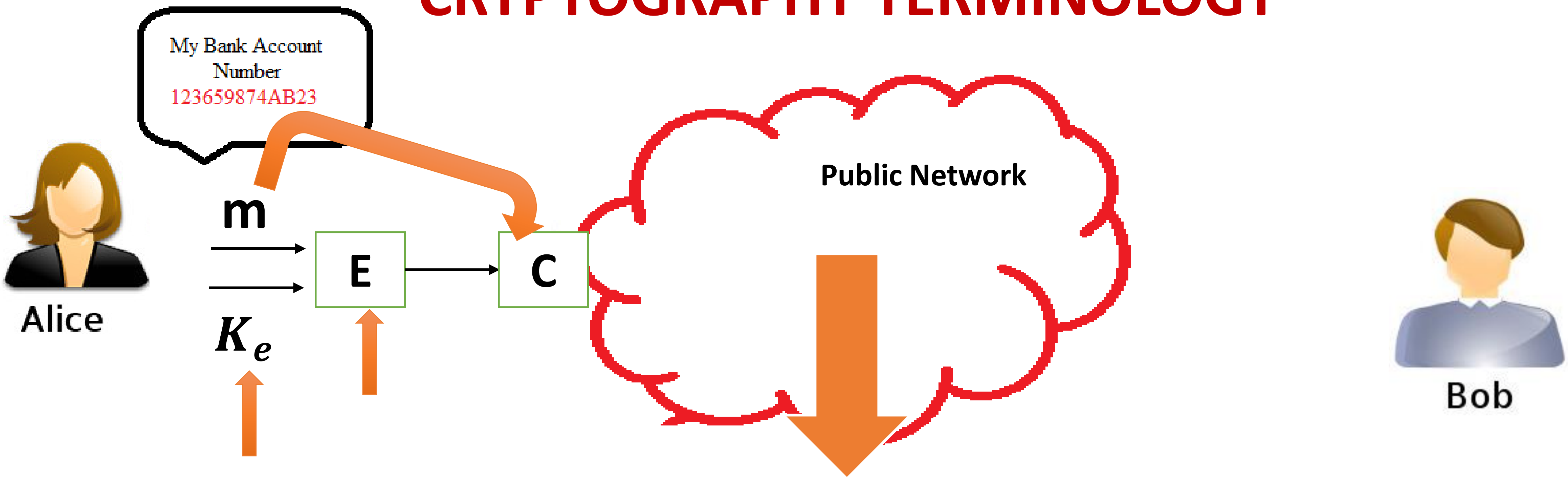
CRYPTOGRAPHY TERMINOLOGY



C : Cipher Text

When a plain text message is codifies using any suitable technique, the resulting message is called as cipher text.

CRYPTOGRAPHY TERMINOLOGY



An Enemy , A very smart Person

K_e: Encryption Key

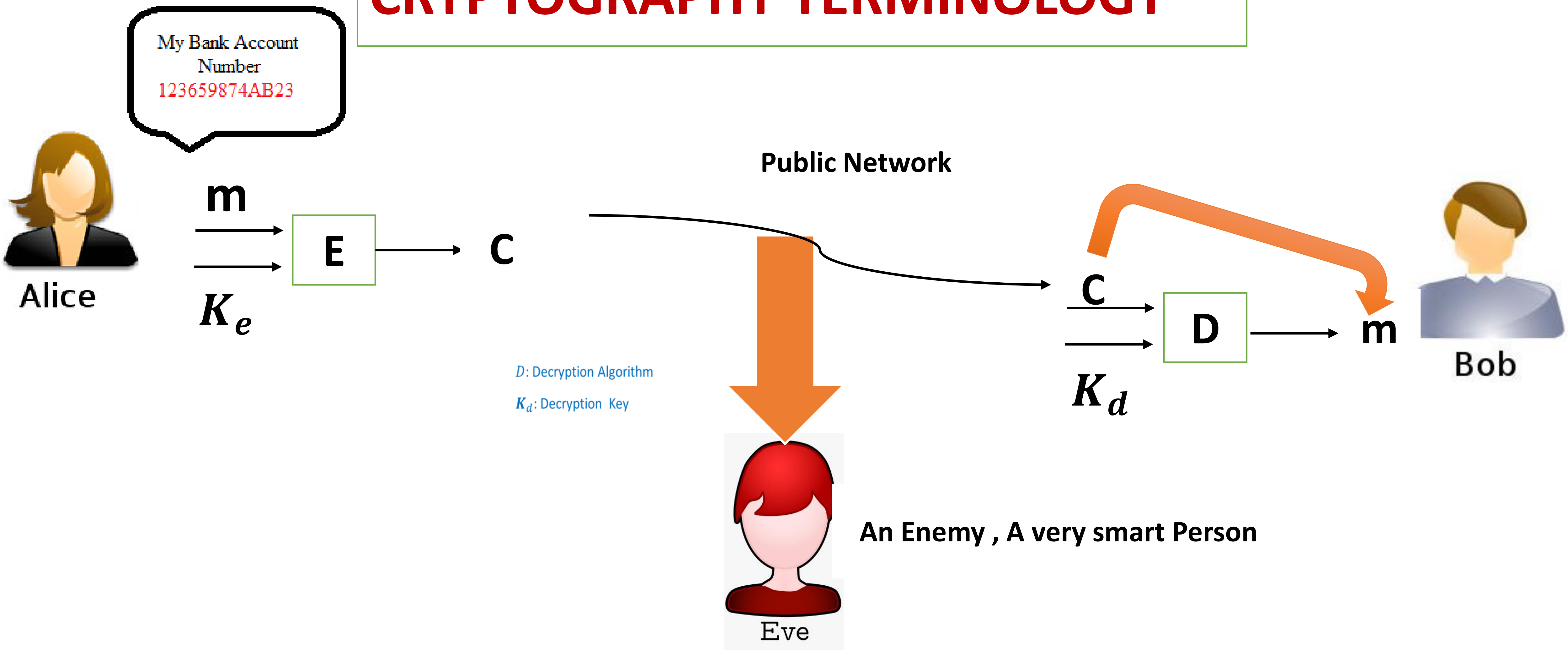
E: Encryption Algorithm

K_e: Encryption Key

Encryption

E: Encryption Algorithm

CRYPTOGRAPHY TERMINOLOGY

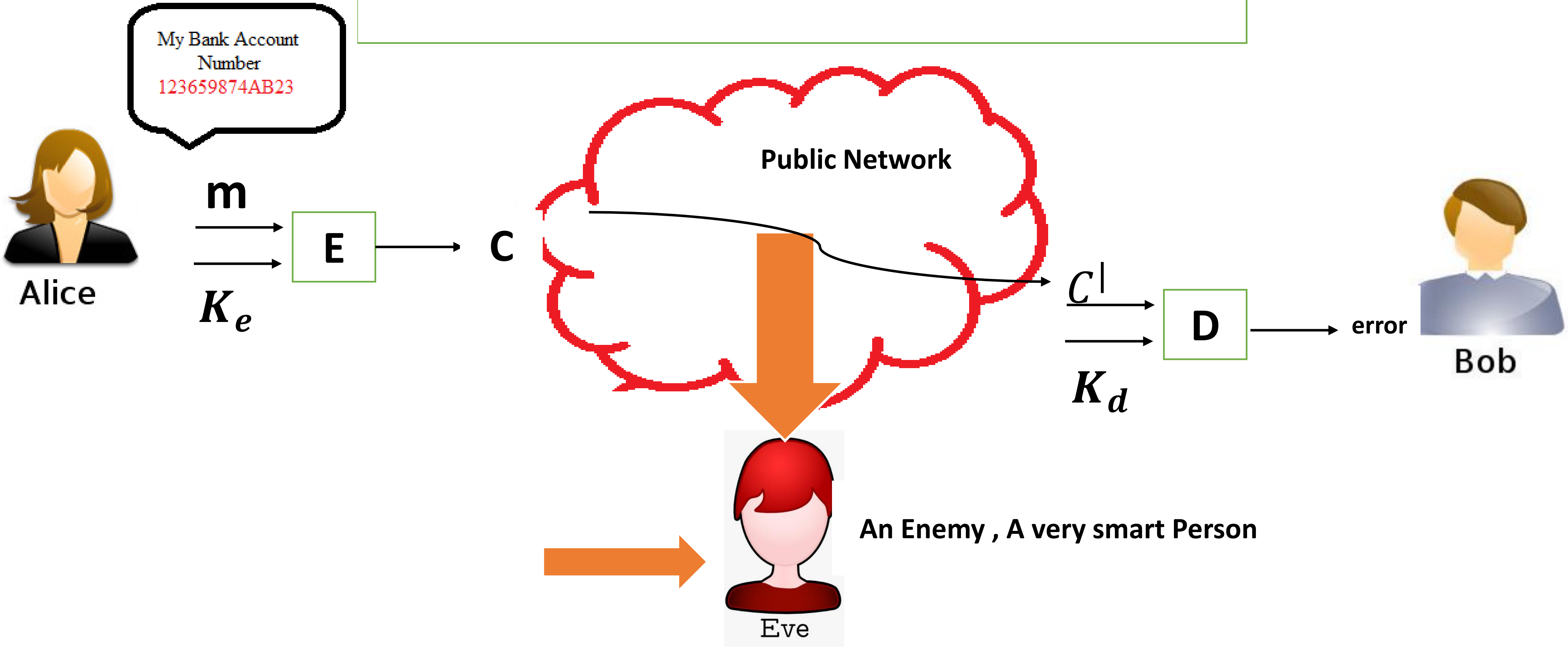


D: Decryption Algorithm

K_d: Decryption Key

Decryption

CRYPTOGRAPHY TERMINOLOGY



My Bank Account Number
123659874AB23

Alice

m

K_e

E

C

Public Network

$C^|$

D

K_d

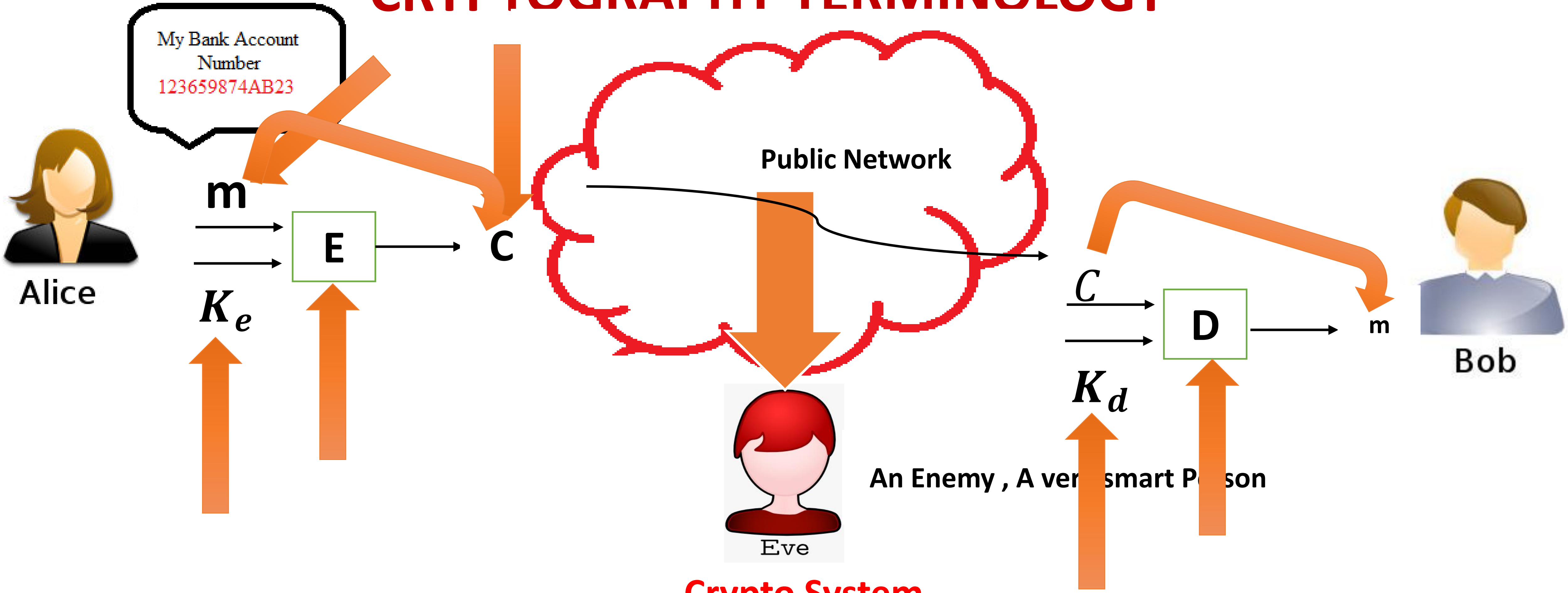
error

Bob

Eve

An Enemy , A very smart Person

CRYPTOGRAPHY TERMINOLOGY



Crypto System

m : Plain Text

C : Cipher Text

Encryption

E: Encryption Algorithm

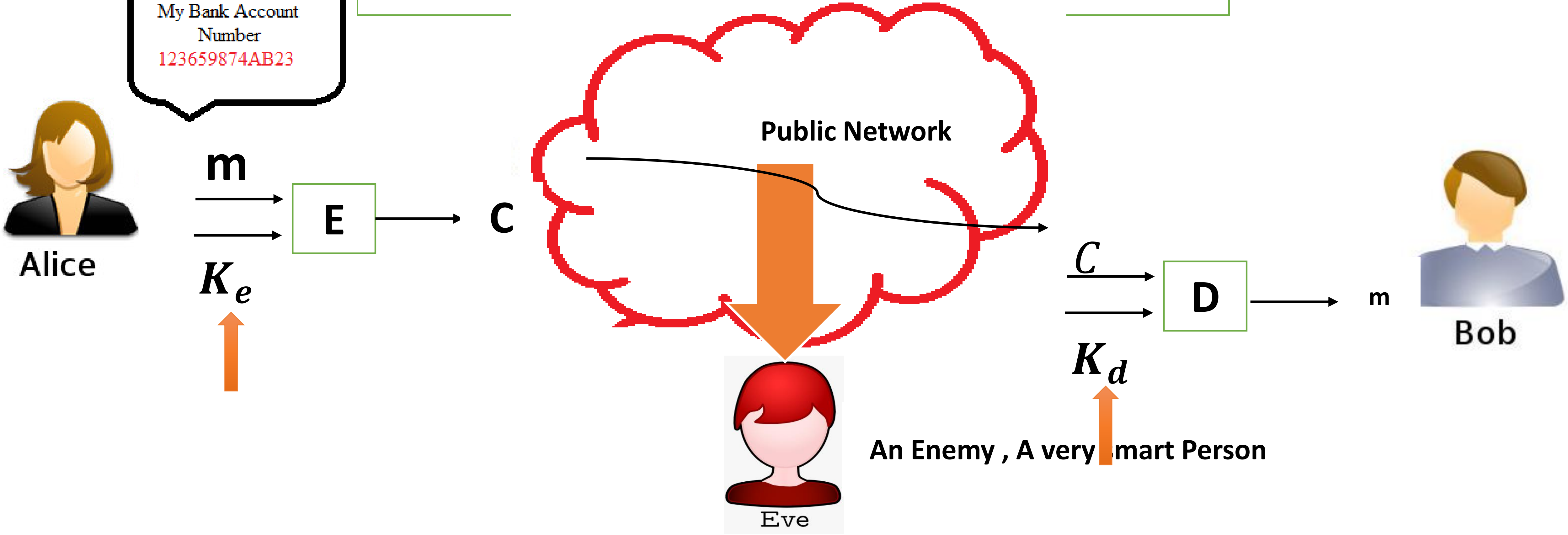
K_e: Encryption Key

Decryption

D: Decryption Algorithm

K_d: Decryption Key

SYMMETRIC KEY CRYPTOGRAPHY

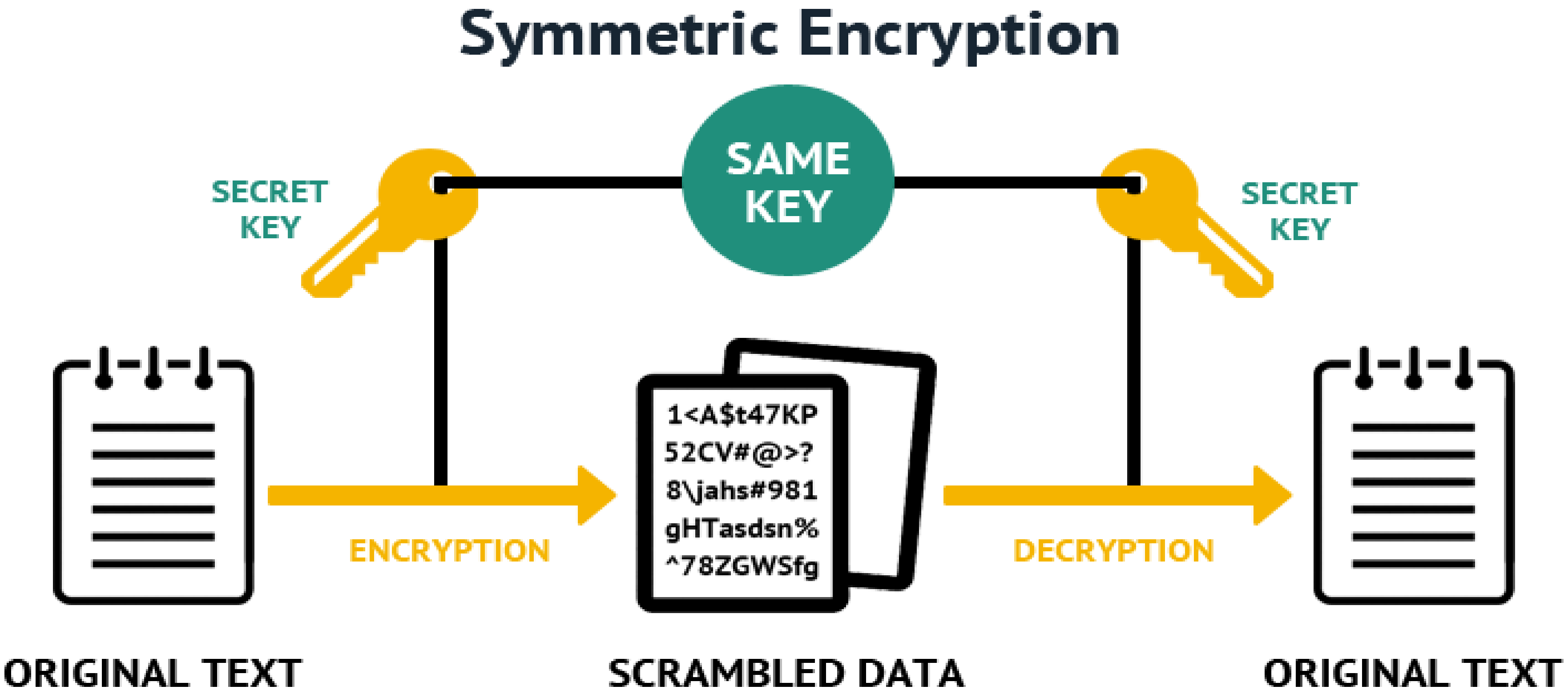


Symmetric Key Cryptography

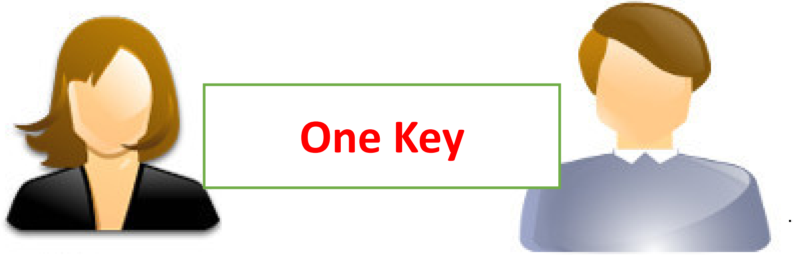
K_e: Encryption Ke = K_d: Decryption Key

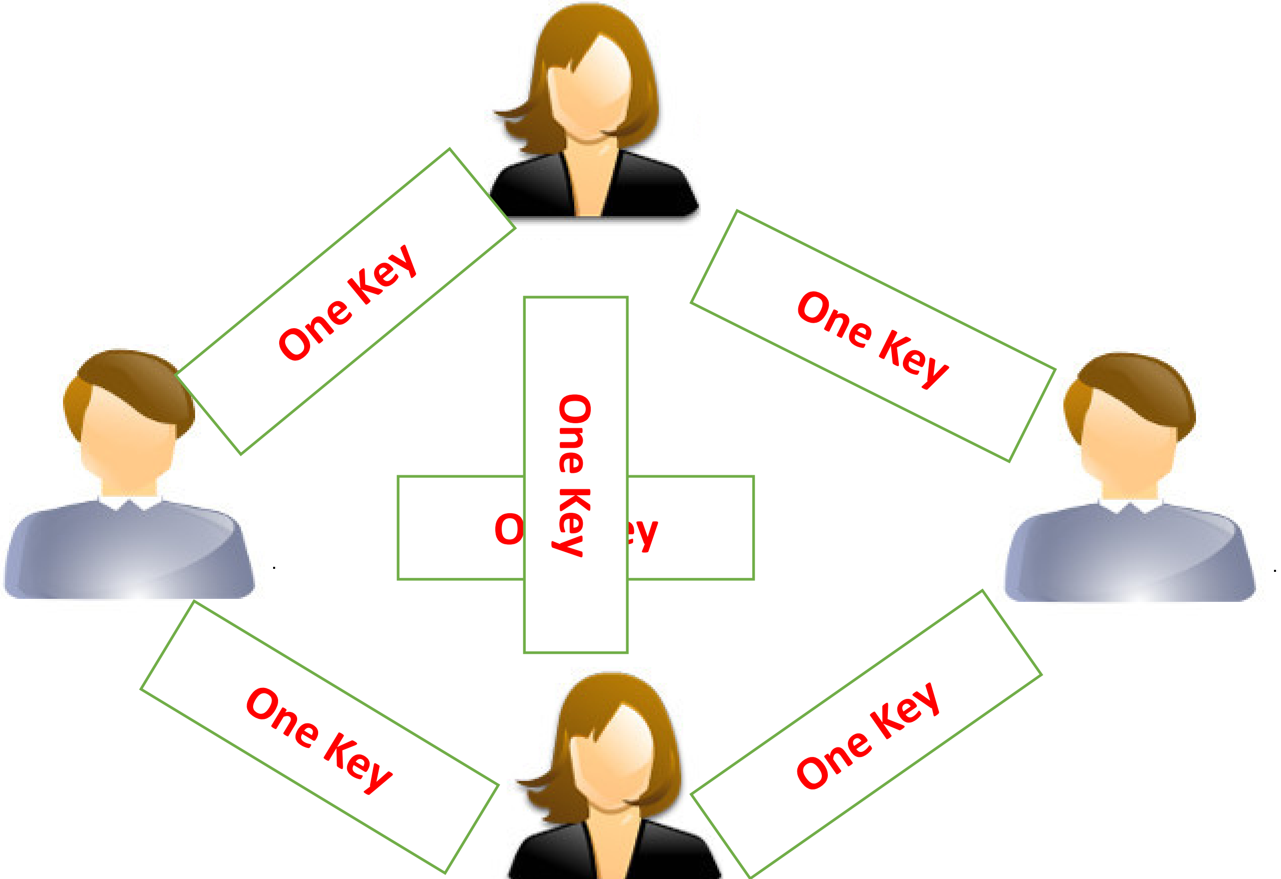
SYMMETRIC KEY CRYPTOGRAPHY

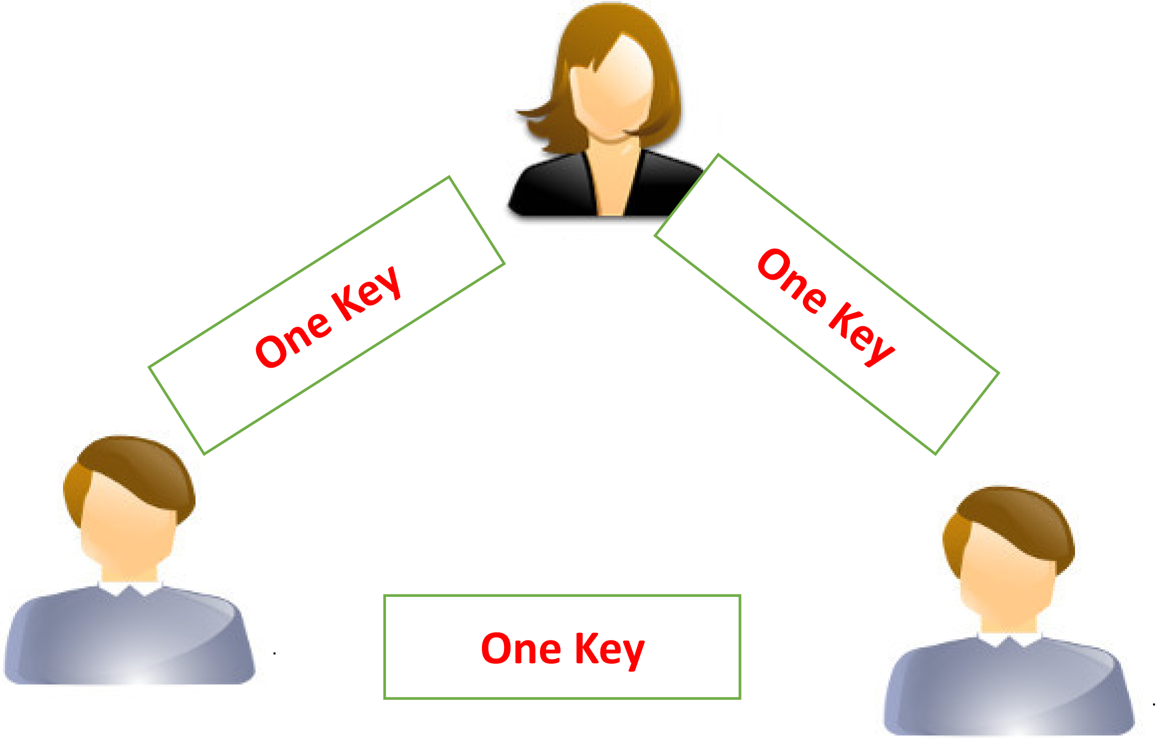
- Symmetric key also called Symmetric Encryption, which requires both the sender and the recipient to have the same key.



SYMMETRIC KEY CRYPTOGRAPHY

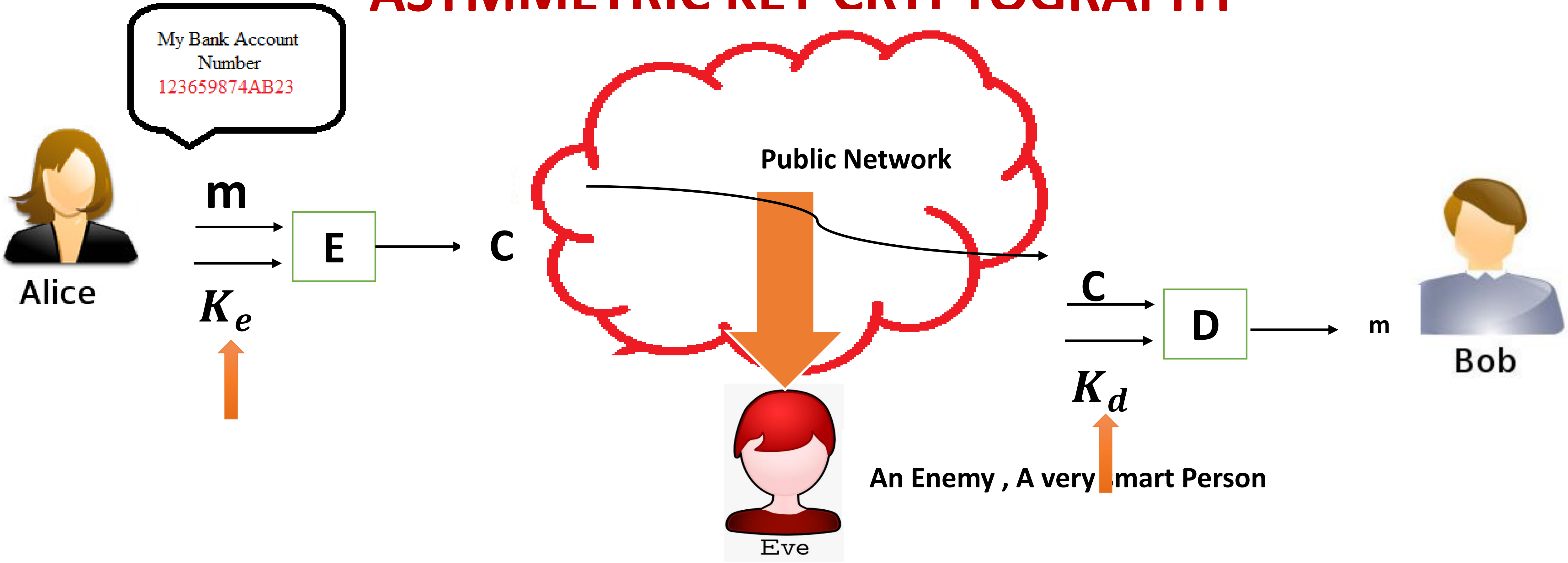






$$Number\ of\ keys = (N * (N - 1))/2$$

ASYMMETRIC KEY CRYPTOGRAPHY



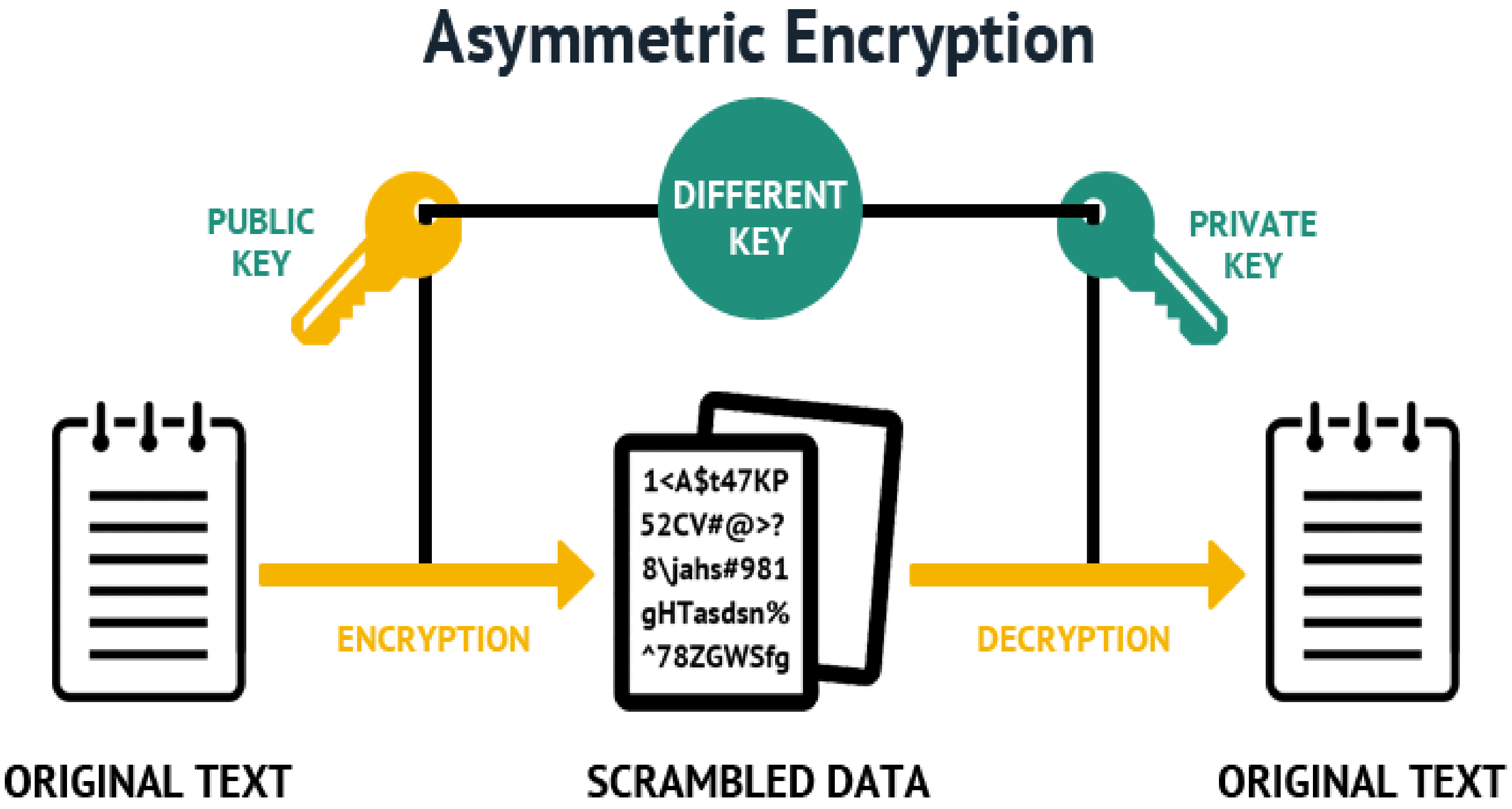
Asymmetric Key Cryptography

K_e: Encryption Ke $\neq$ K_d: Decryption Key

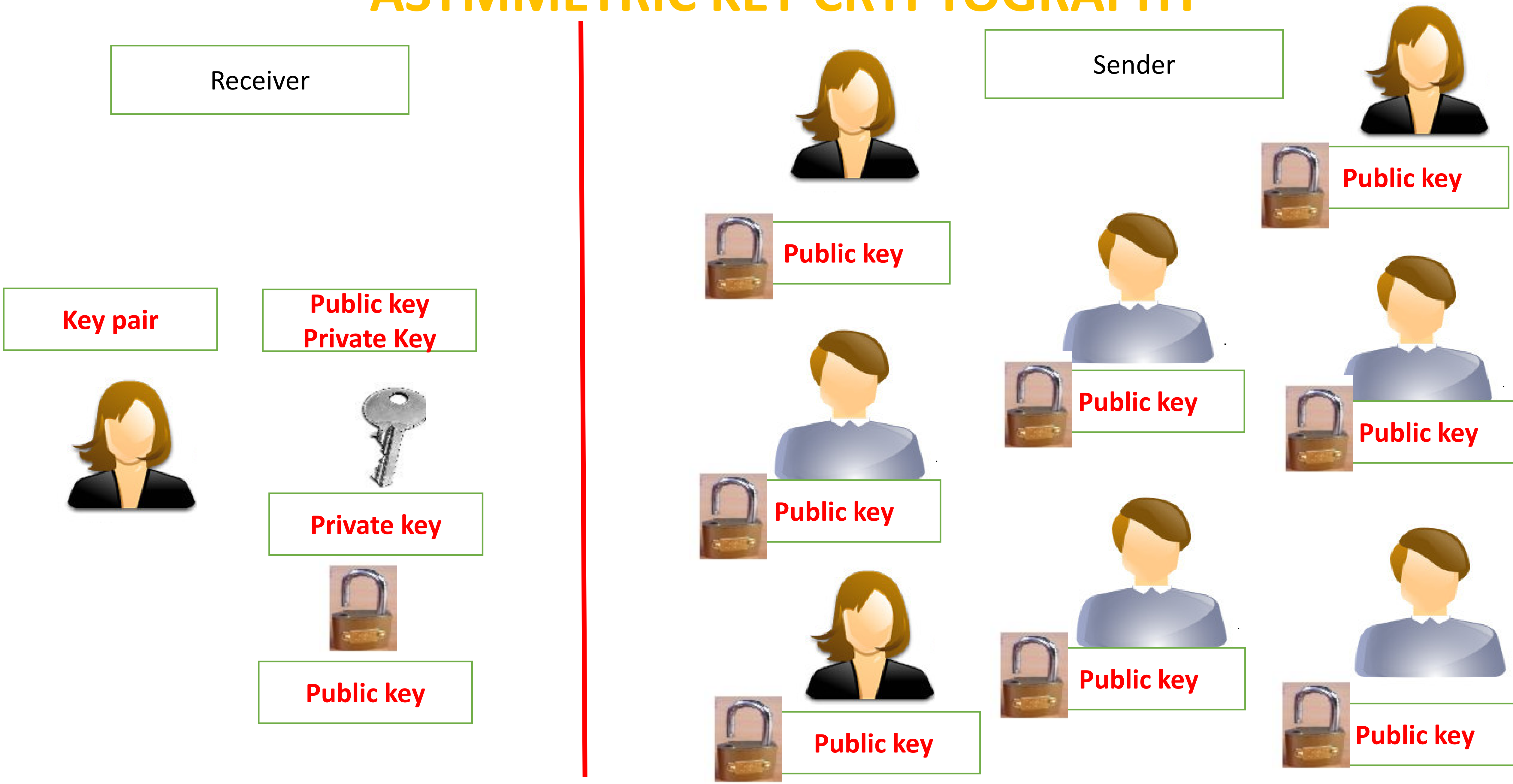
Public Key Cryptography

ASYMMETRIC KEY CRYPTOGRAPHY

- Asymmetric key also called Asymmetric Encryption, it uses two different keys – a public key used for encryption and a private key used for decryption.



ASYMMETRIC KEY CRYPTOGRAPHY



Receiver

Key pair

Public key
Private Key

Private key

Public key

Sender

Public key

Public key

Public key

Public key

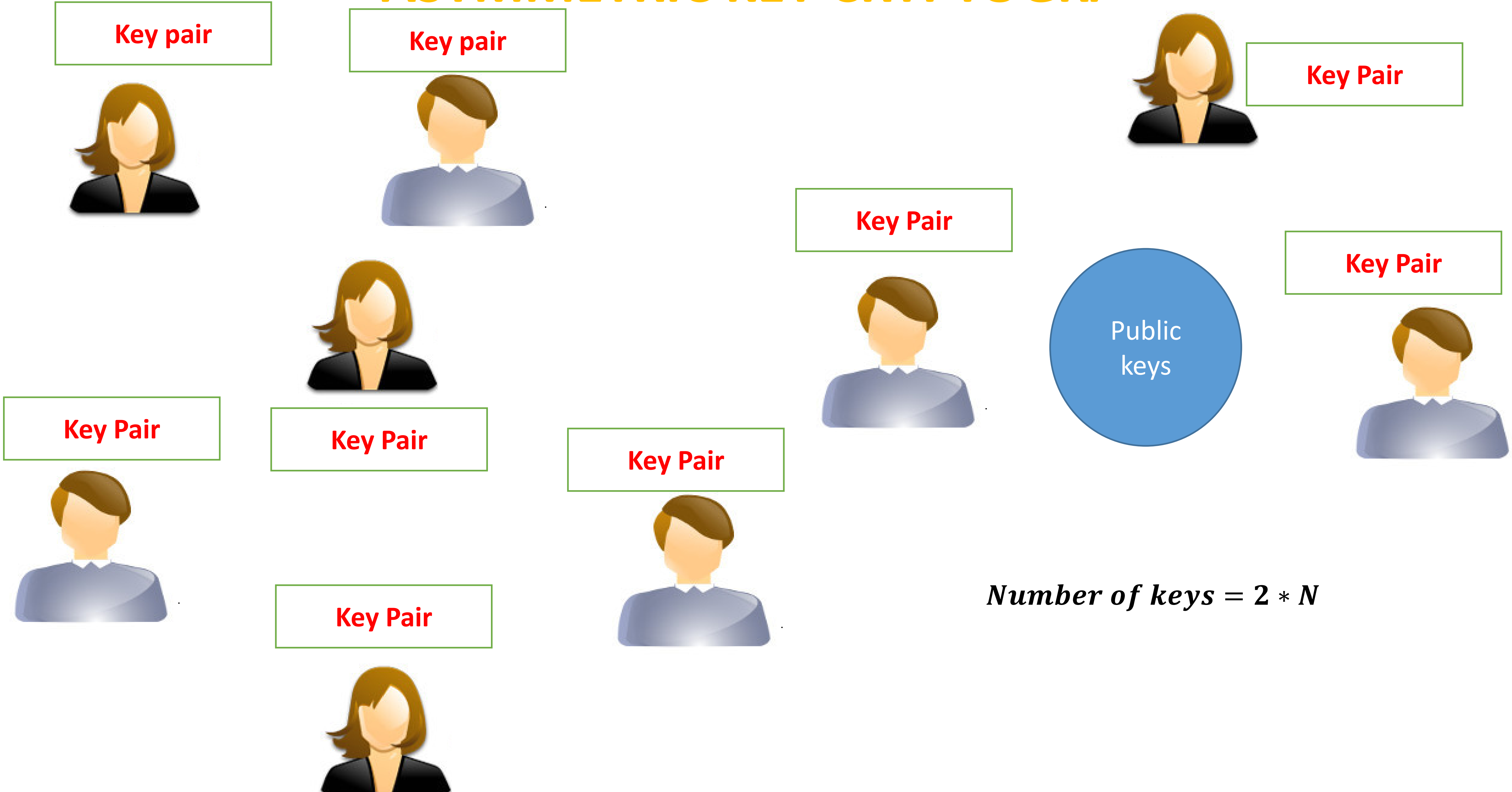
Public key

Public key

Public key

Public key

ASYMMETRIC KEY CRYPTOGRAPHY



Key pair

Key pair

Key Pair

Key Pair

Public keys

Key Pair

Key Pair

Key Pair

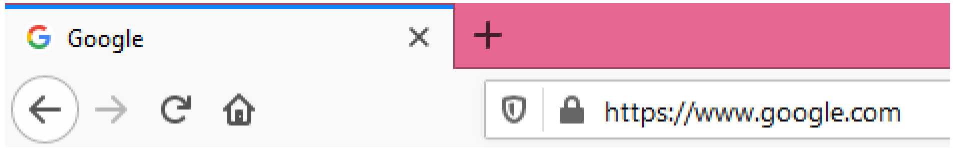
Key Pair

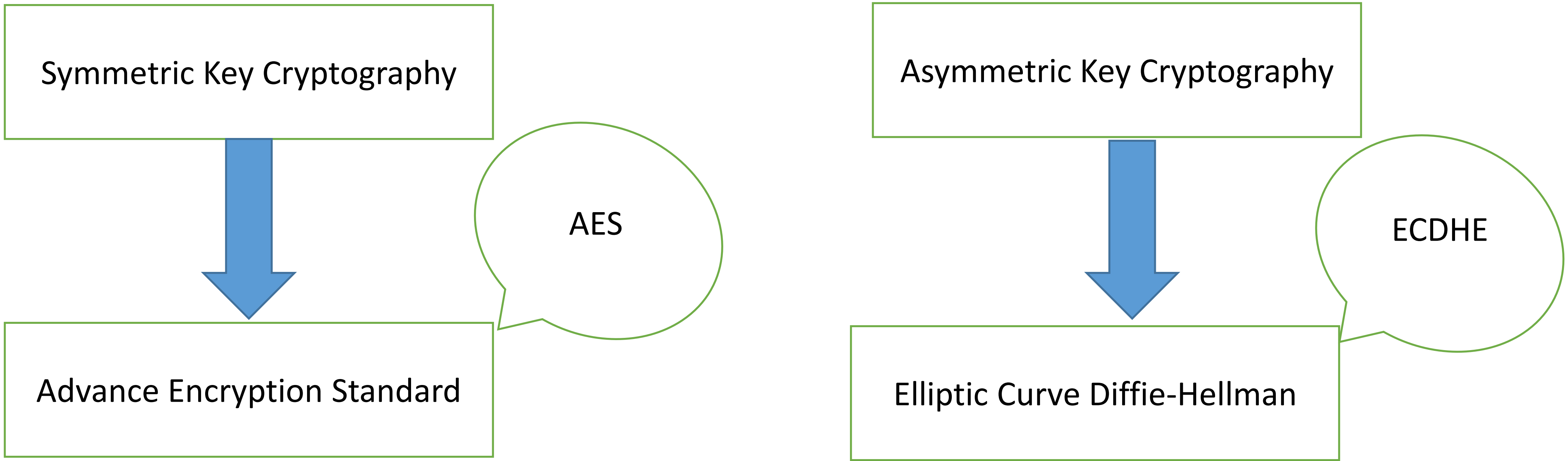
Key Pair

$$Number\ of\ keys = 2 * N$$

Real Time Scenario

HTTPS (Hyper Text Transfer Protocol)





Symmetric Key Cryptography

Advance Encryption Standard

AES

Asymmetric Key Cryptography

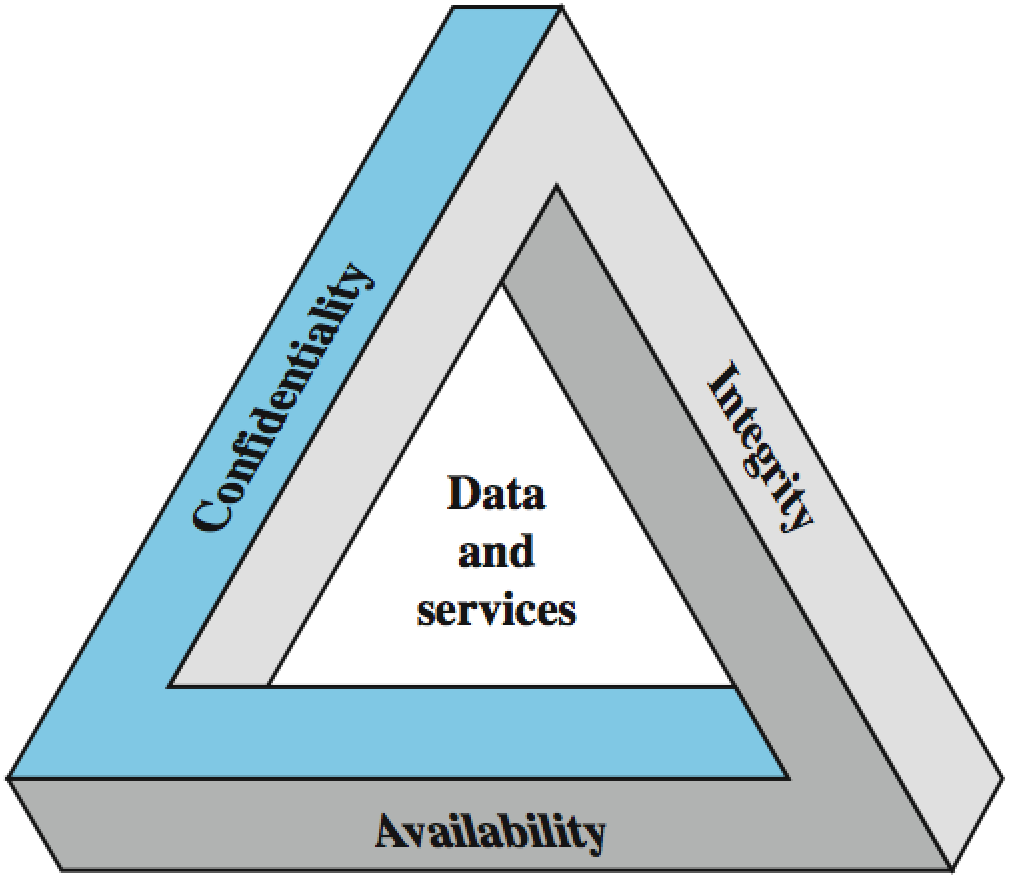
Elliptic Curve Diffie-Hellman

ECDHE

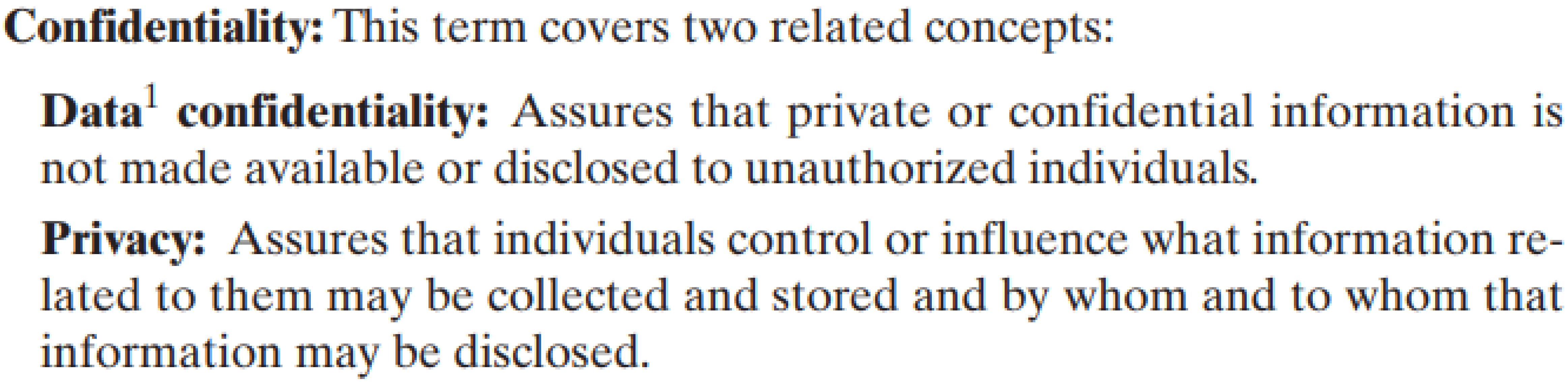
Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Heart of Computer Security



Confidentiality

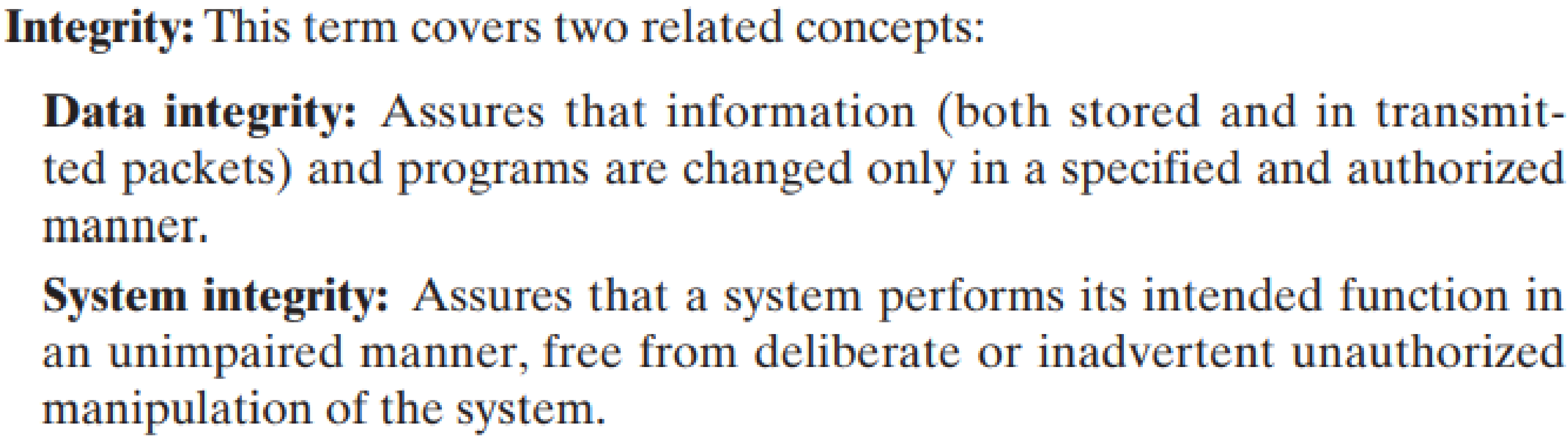


Confidentiality: This term covers two related concepts:

Data[1] confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity

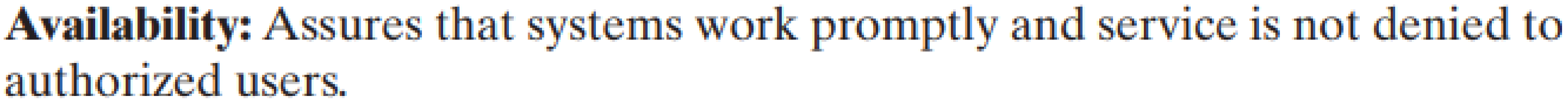


Integrity: This term covers two related concepts:

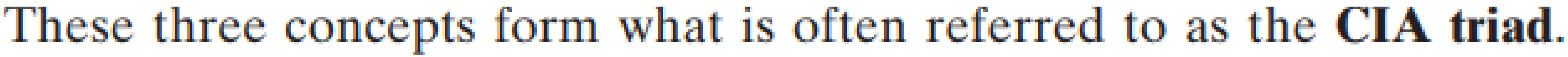
Data integrity: Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability



Availability: Assures that systems work promptly and service is not denied to authorized users.



These three concepts form what is often referred to as the **CIA triad**.

Along with the CIA additional concepts are Authenticity and Accountability

Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Low Impact

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
  - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  - (ii) result in minor damage to organizational assets;
  - (iii) result in minor financial loss; or
  - (iv) result in minor harm to individuals.

Moderate Impact

- The loss could be expected to have a serious adverse effect on organizational operations, assets, or individuals.
- A serious adverse effect means that, e.g., the loss might
  - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - (ii) result in significant damage to organizational assets;
  - (iii) result in significant financial loss; or
  - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High Impact

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss might
  - (i) cause severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  - (ii) result in major damage to organizational assets;
  - (iii) result in major financial loss; or
  - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

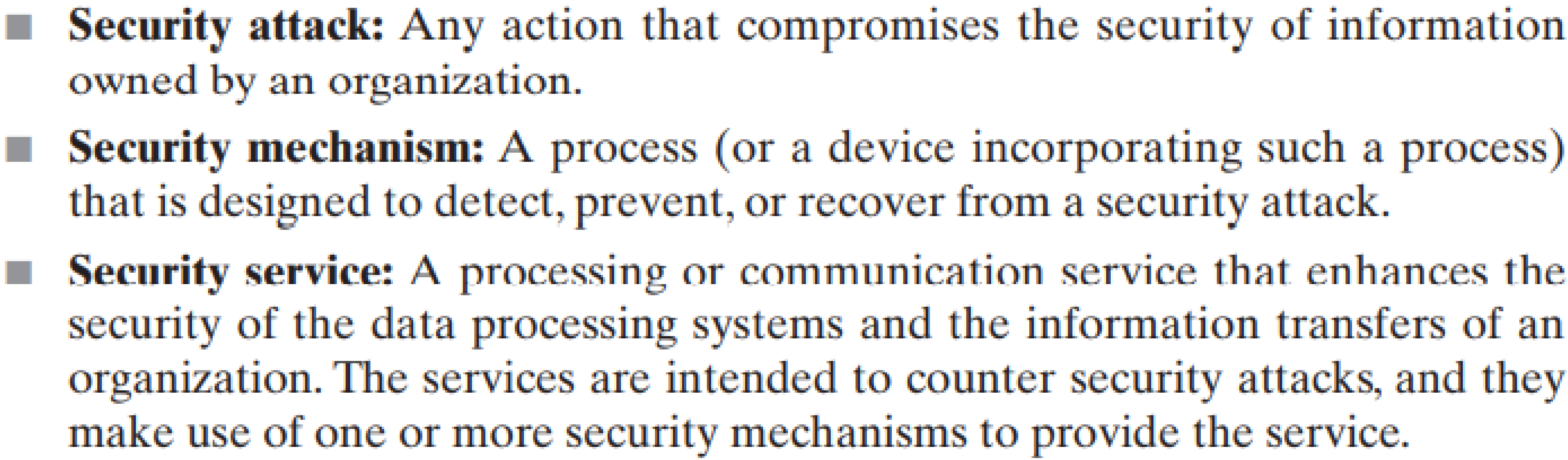
Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service
- authenticity – admission ticket
- non-repudiation – stock sell order

Computer Security Challenges

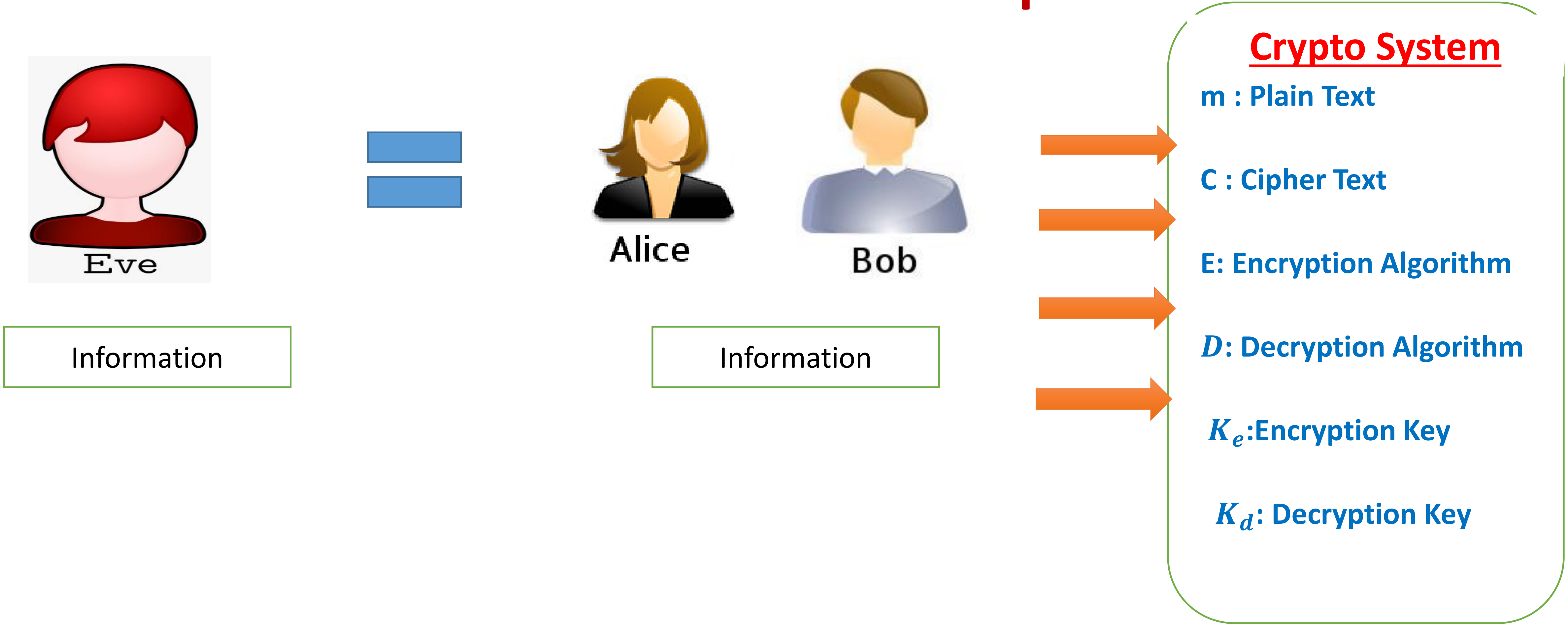
1. not simple – easy to get it wrong
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived to be of benefit until it fails
8. requires regular monitoring a process, not an event
9. too often an after-thought
10. regarded as impediment to using system
    “Unusable security is not secure”

OSI Security Architecture



- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Kerckhoff's Principle



Crypto System

m : Plain Text

C : Cipher Text

E: Encryption Algorithm

D: Decryption Algorithm

K_e:Encryption Key

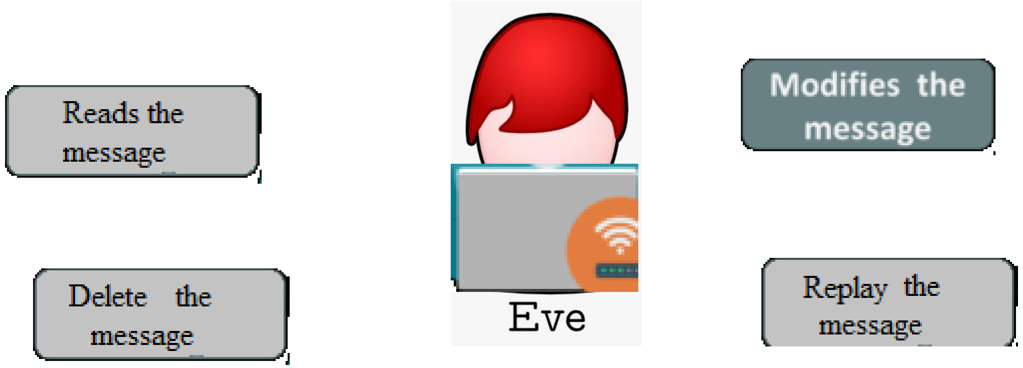
K_d: Decryption Key

- Kerckhoff's principle states that Eve knows the system that Alice and Bob use for information transfer including the coding scheme, the algorithm, the protocol, and so on. Only unknown to Eve is Key.

Security Attacks

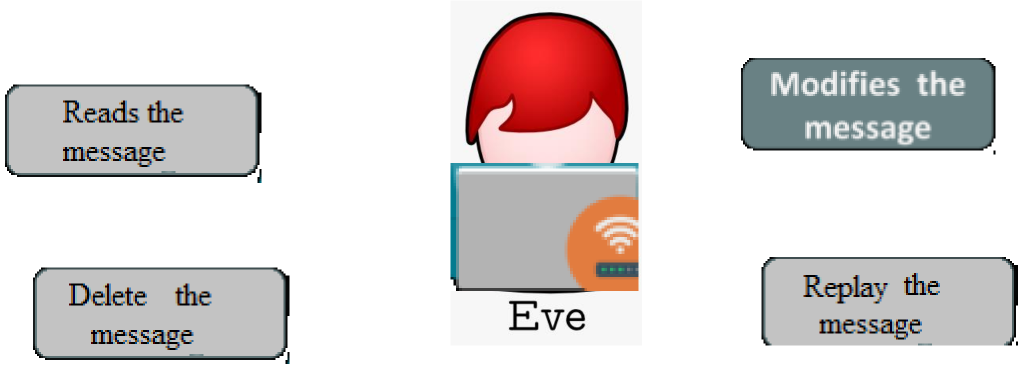
Security Attacks

- **Security attack**: Any action that compromises the security of information owned by an organization.



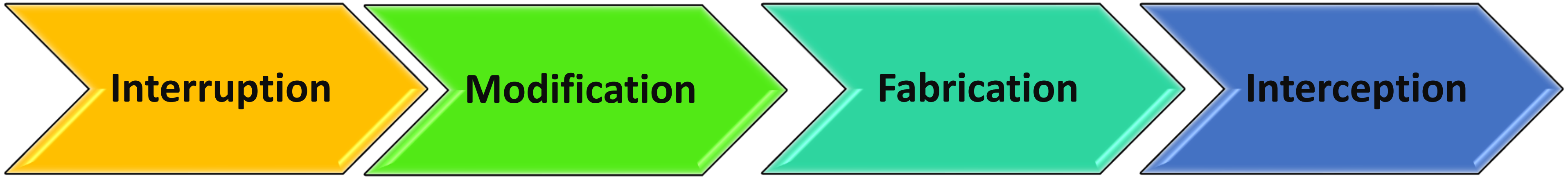
An Attacker , A very smart Person

Categories Security Attacks



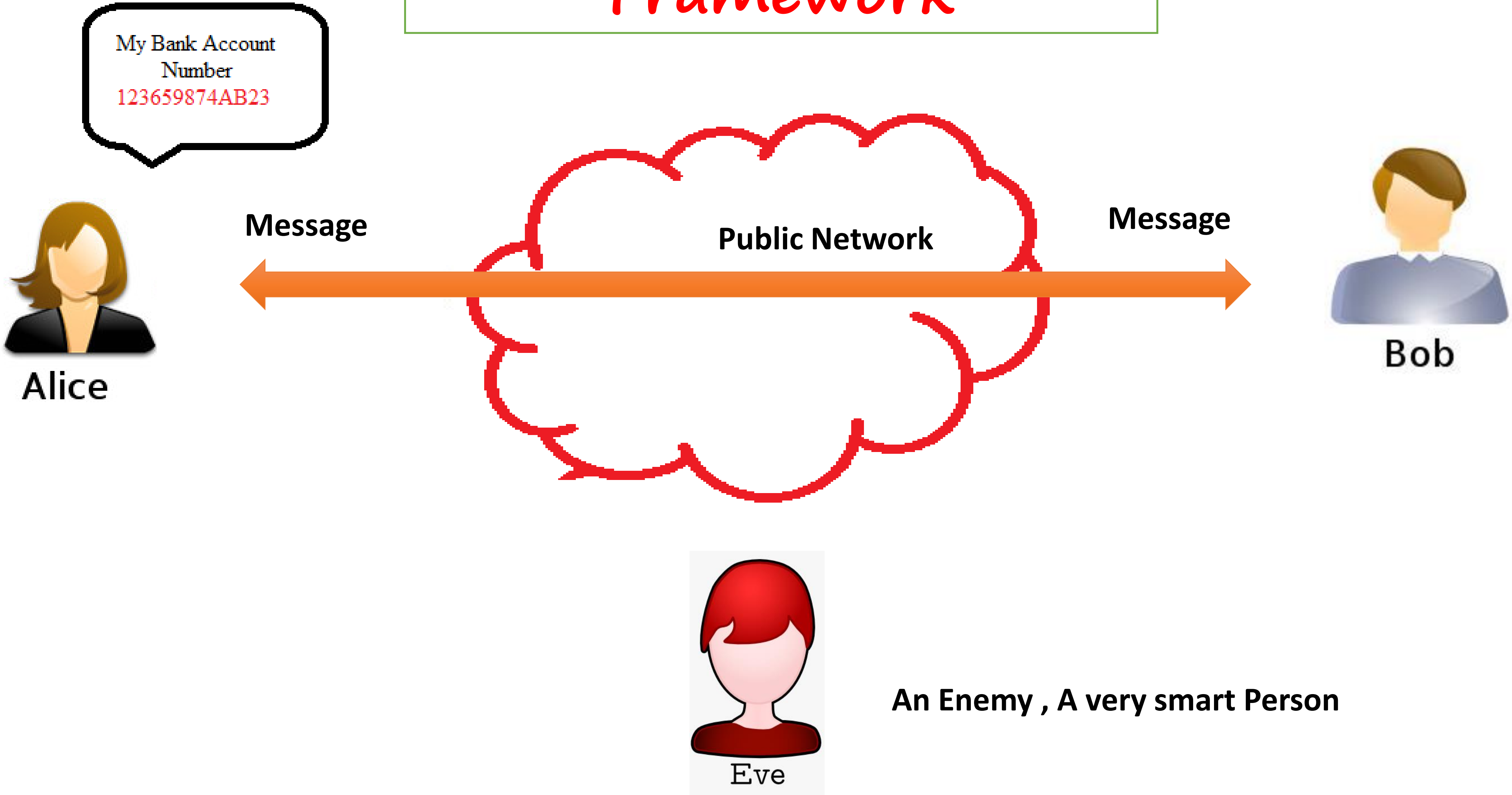
An Attacker , A very smart Person

The way in which attacker can launch the attack



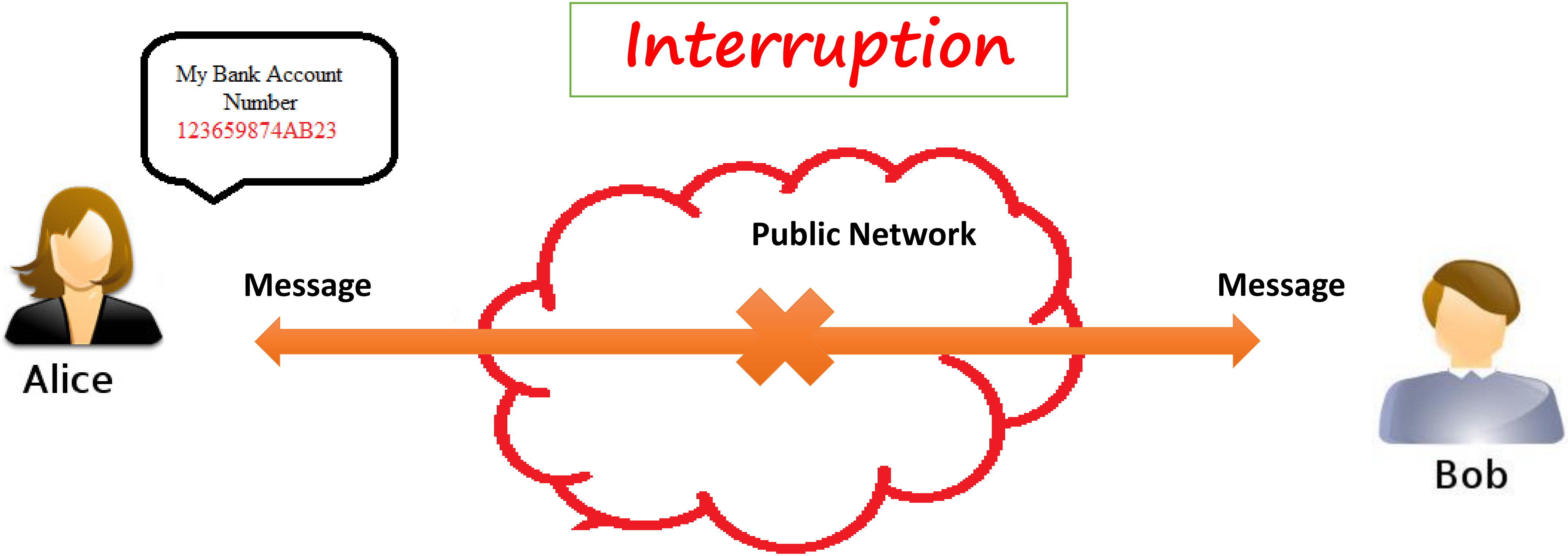
Interruption → Modification → Fabrication → Interception

Alice, Bob and Eve Framework

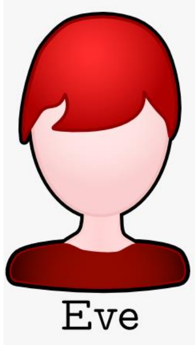


An Enemy , A very smart Person

Interruption



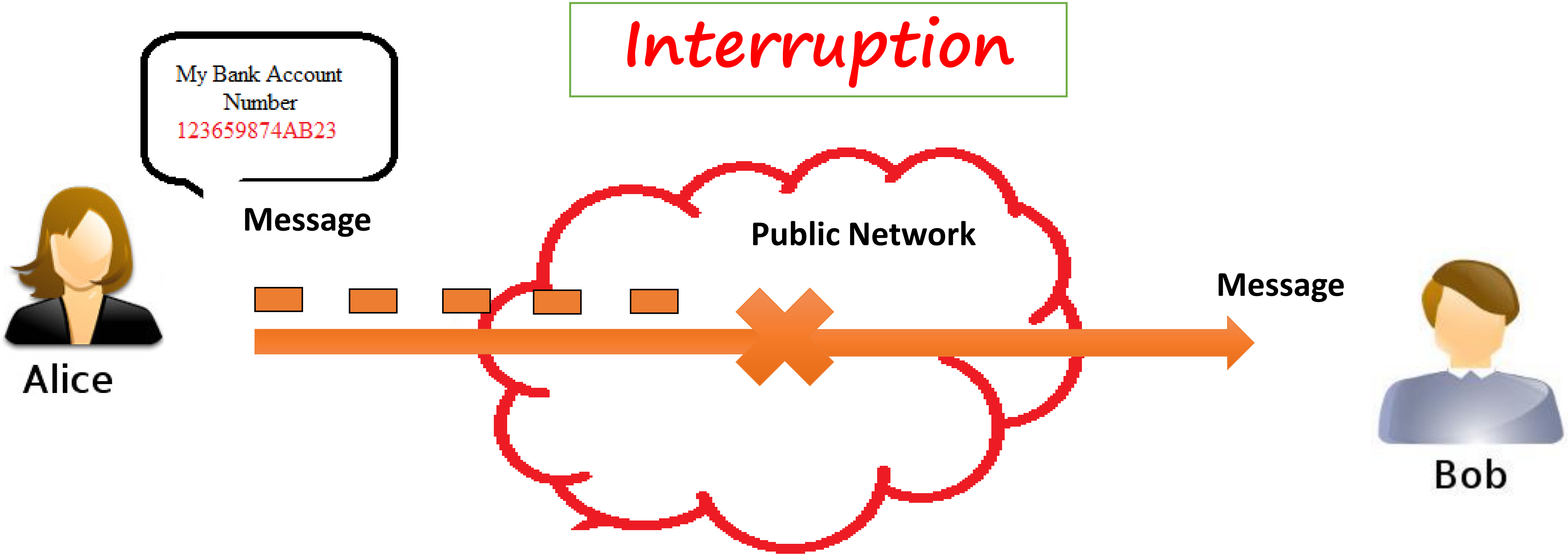
- **Attack on Availability – breaking the communication link**



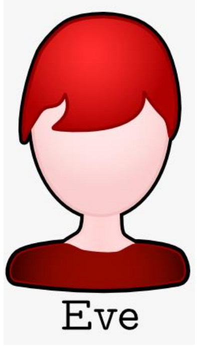
An Enemy , A very smart Person

Alice, Bob, Eve Framework

Interruption



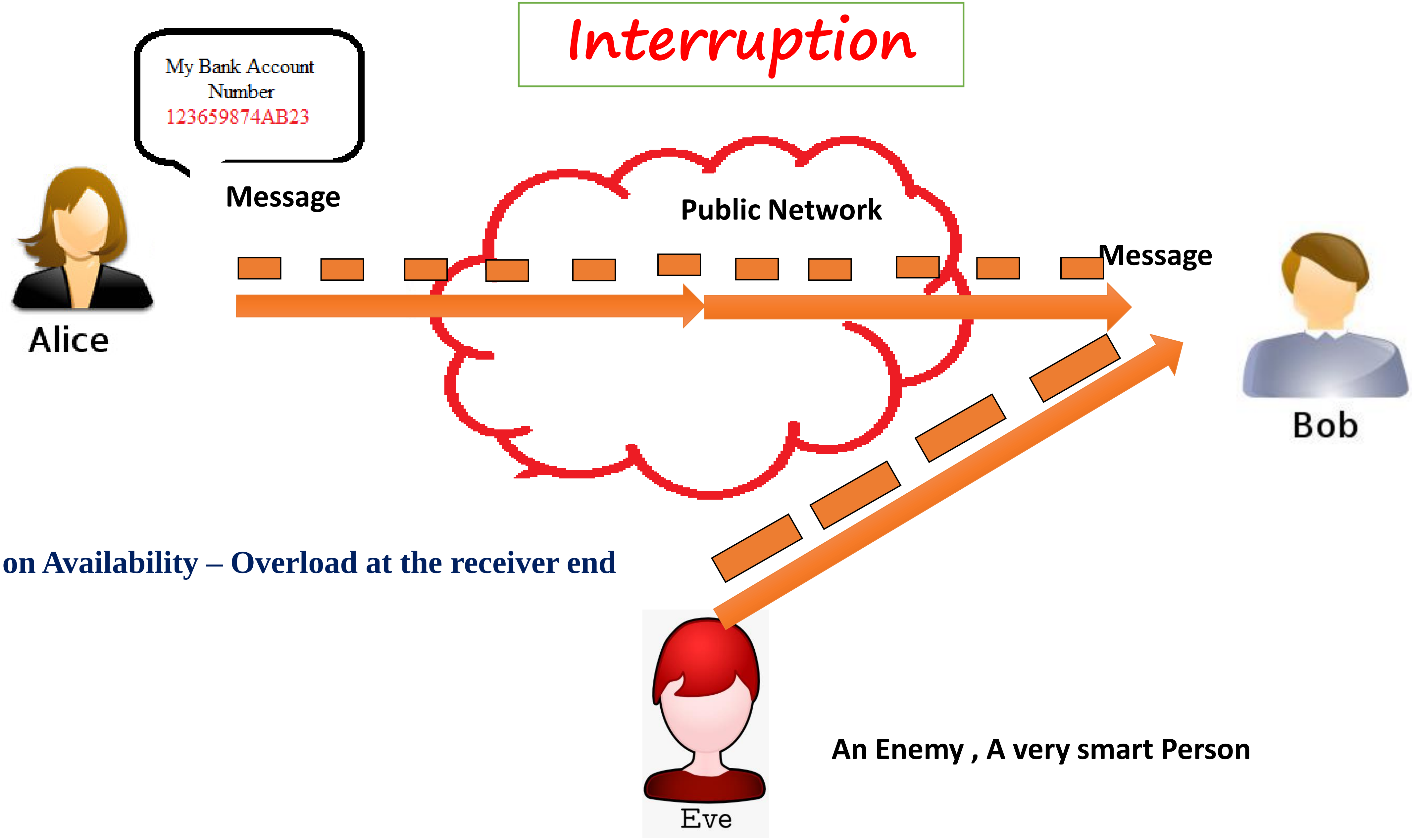
- **Attack on Availability – breaking the communication link**



An Enemy , A very smart Person

Alice, Bob, Eve Framework

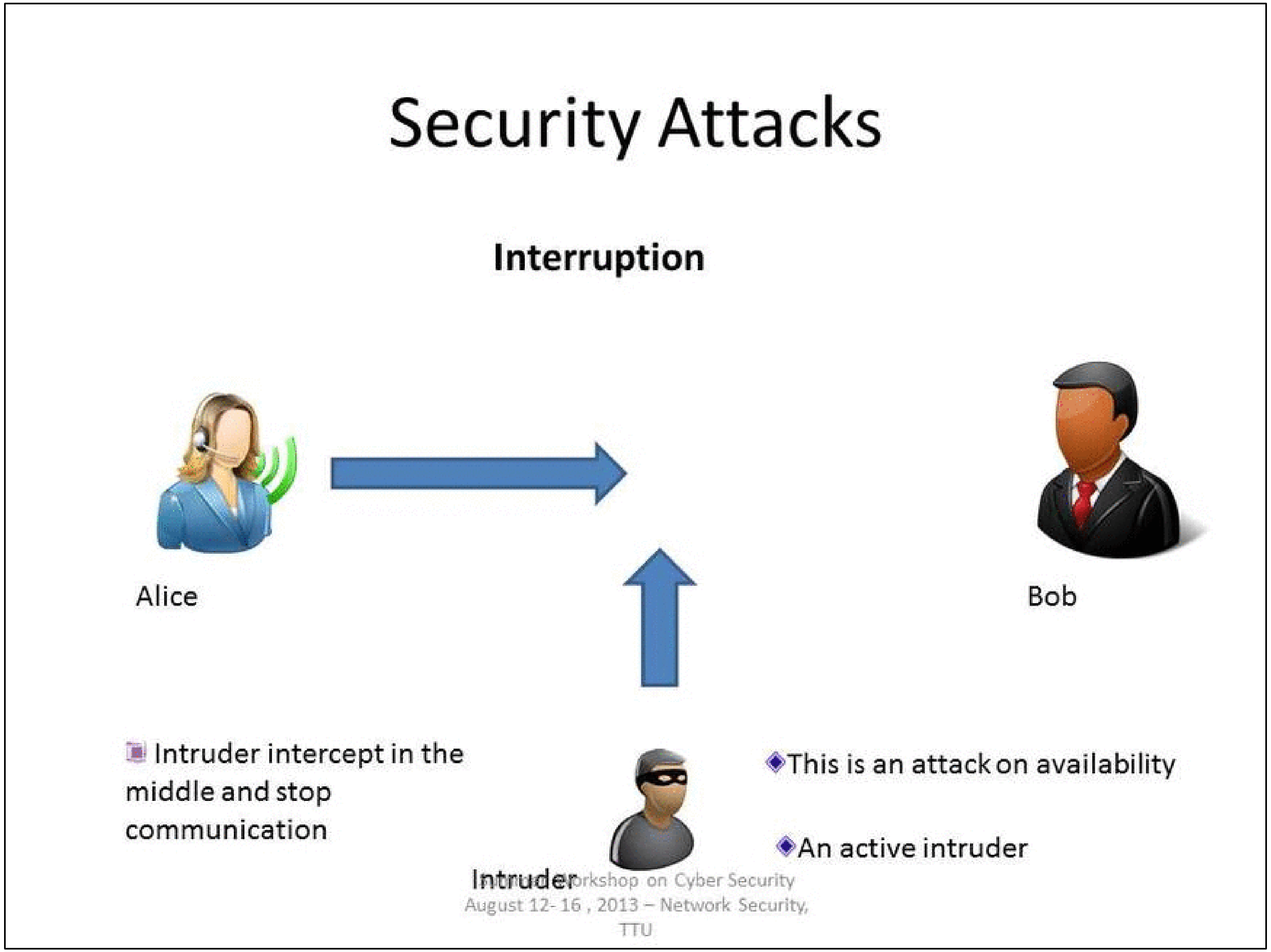
Interruption



- **Attack on Availability – Overload at the receiver end**

Alice, Bob, Eve Framework

Interruption



Security Attacks

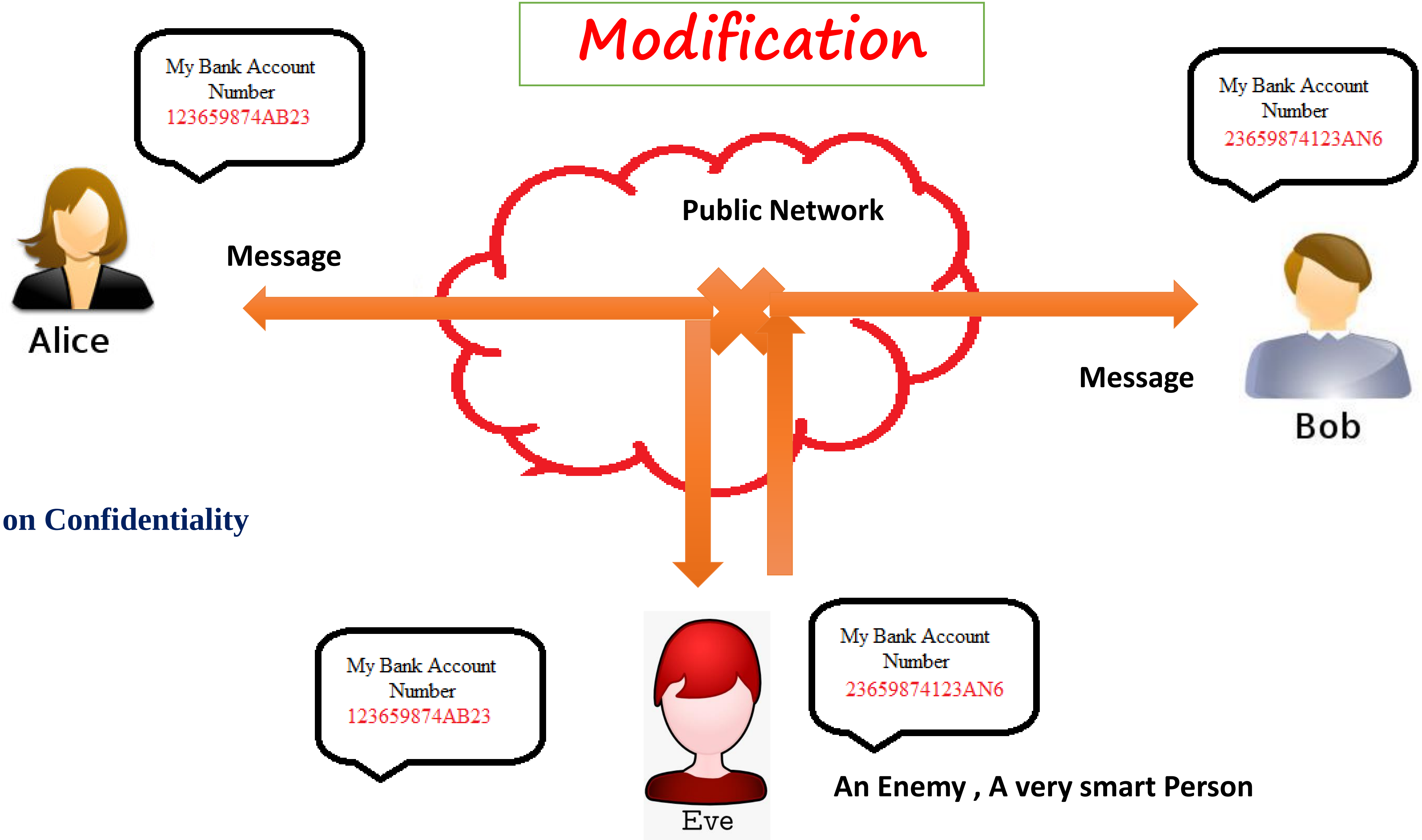
Interruption

- Intruder intercept in the middle and stop communication

- This is an attack on availability
- An active intruder

Workshop on Cyber Security
August 12- 16 , 2013 – Network Security,
TTU

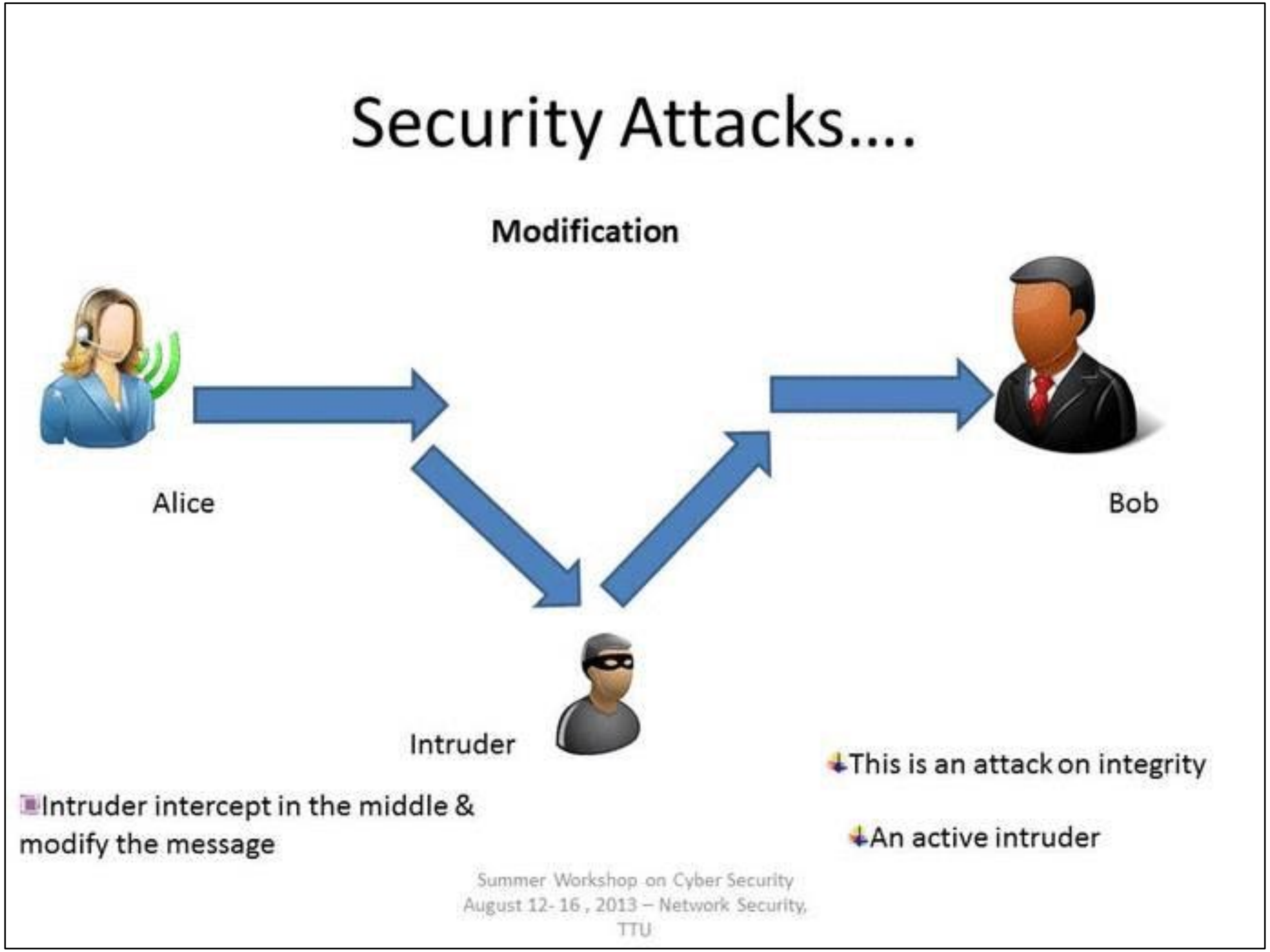
Modification


My Bank Account Number 123659874AB23
Public Network
Message
Alice
My Bank Account Number 23659874123AN6
Message
Bob
My Bank Account Number 123659874AB23
Eve
My Bank Account Number 23659874123AN6
An Enemy , A very smart Person

- **Attack on Confidentiality**

Alice, Bob, Eve Framework

Modification



Security Attacks….

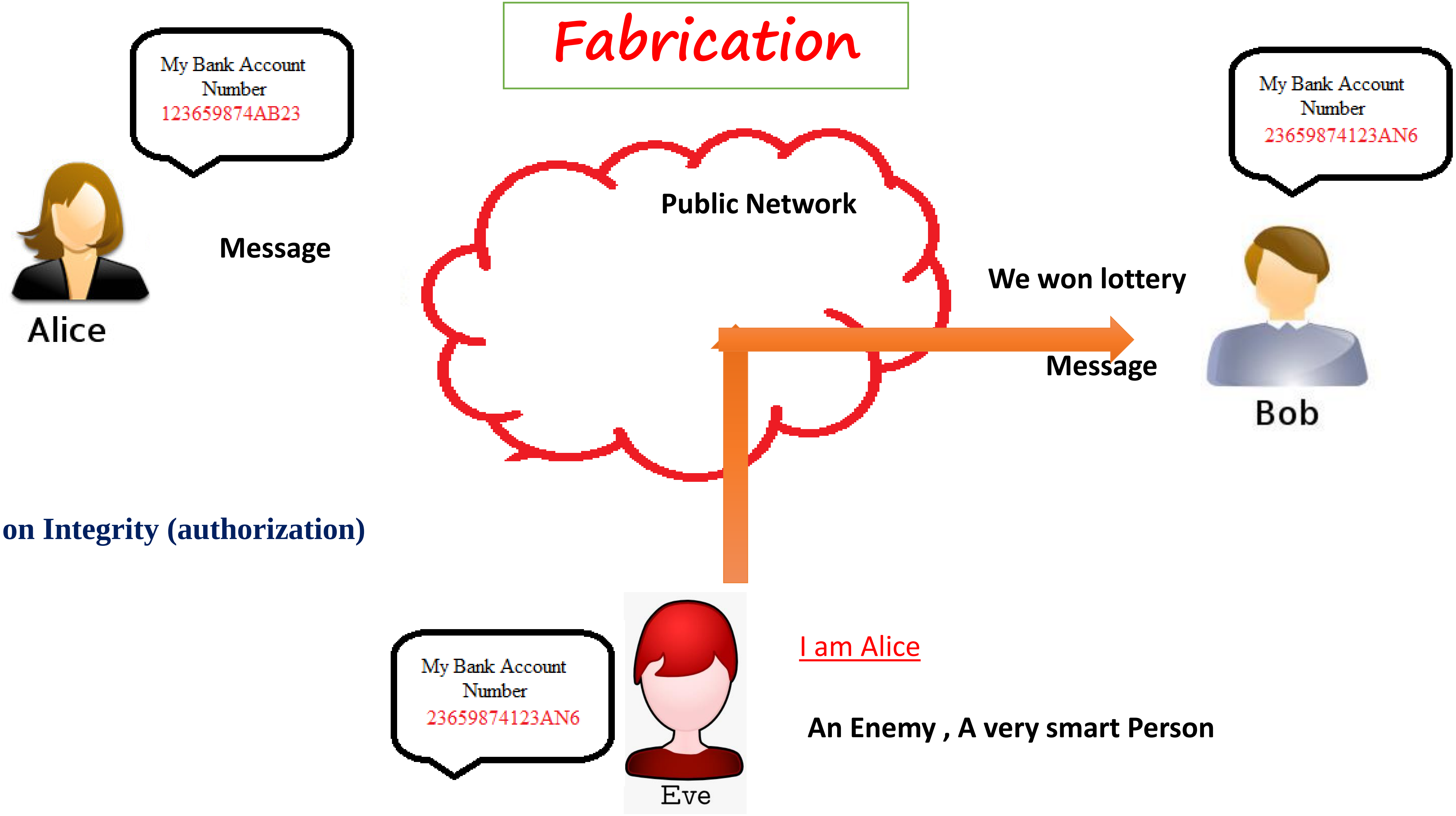
Modification

- Intruder intercept in the middle & modify the message

- This is an attack on integrity
- An active intruder

Summer Workshop on Cyber Security
August 12- 16 , 2013 – Network Security,
TTU

Fabrication



My Bank Account Number 123659874AB23

Alice

Message

Public Network

We won lottery

Message

My Bank Account Number 23659874123AN6

Bob

My Bank Account Number 23659874123AN6

Eve

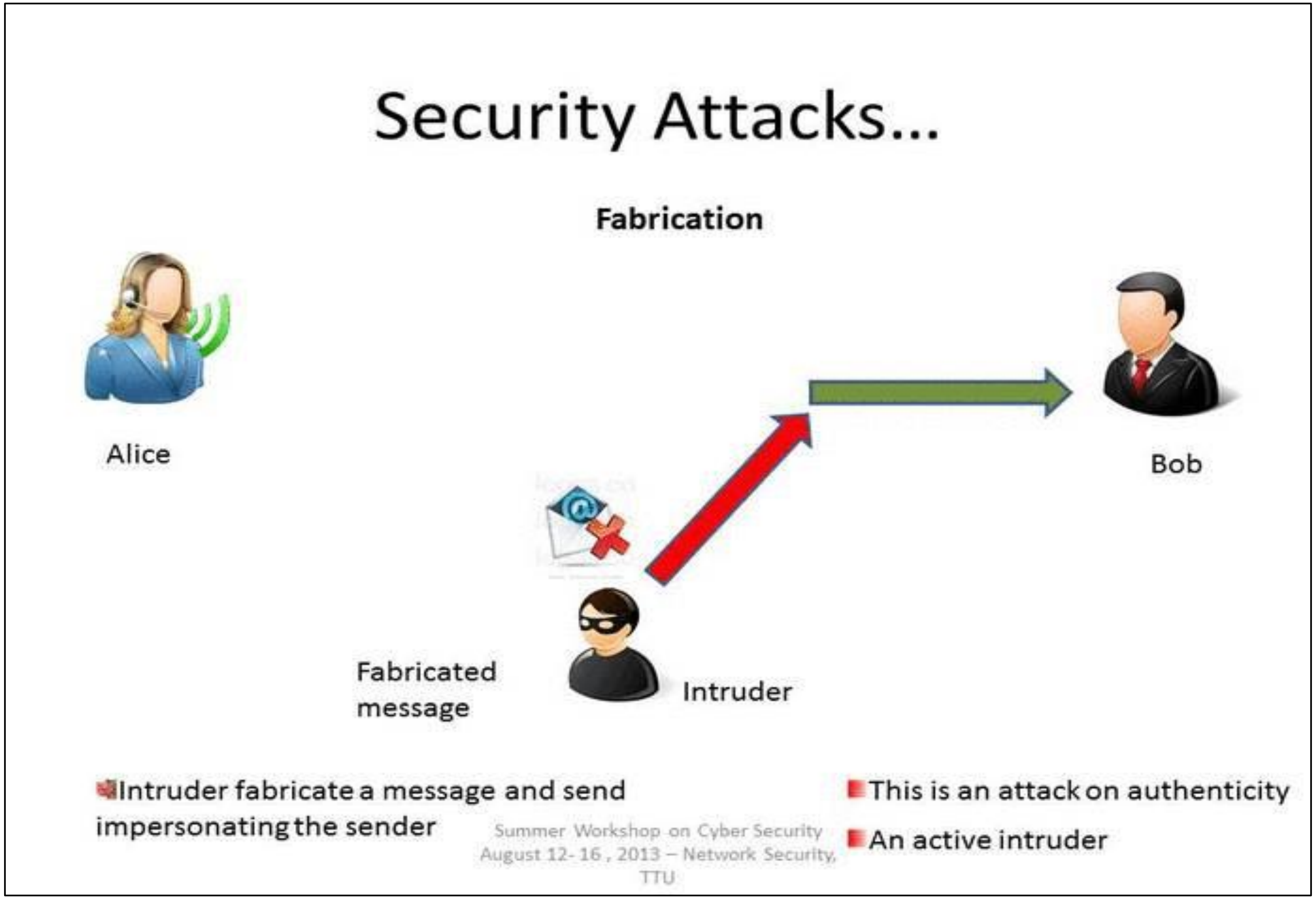
I am Alice

An Enemy , A very smart Person

- **Attack on Integrity (authorization)**

Alice, Bob, Eve Framework

Fabrication



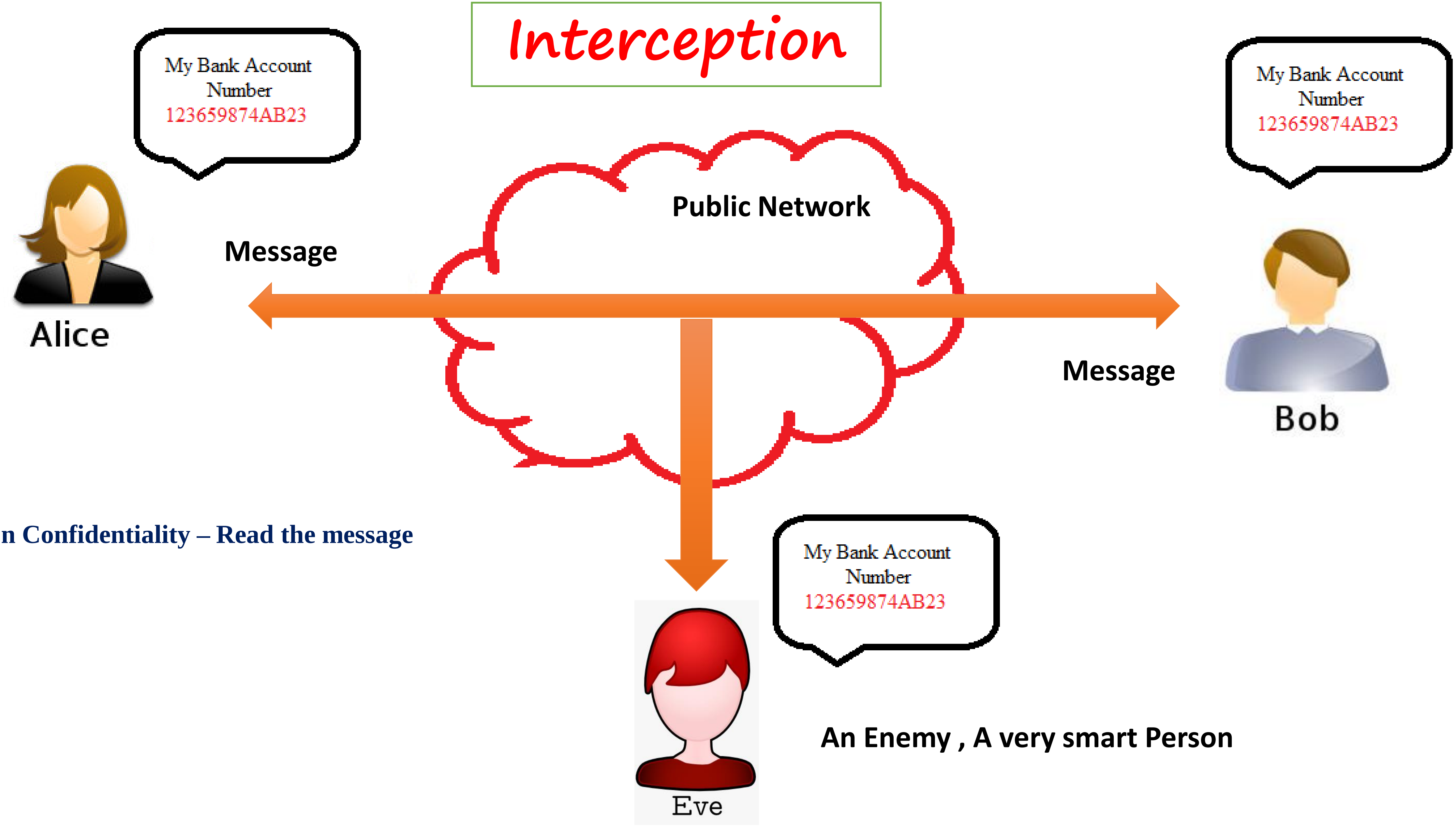
Security Attacks...

Fabrication

- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

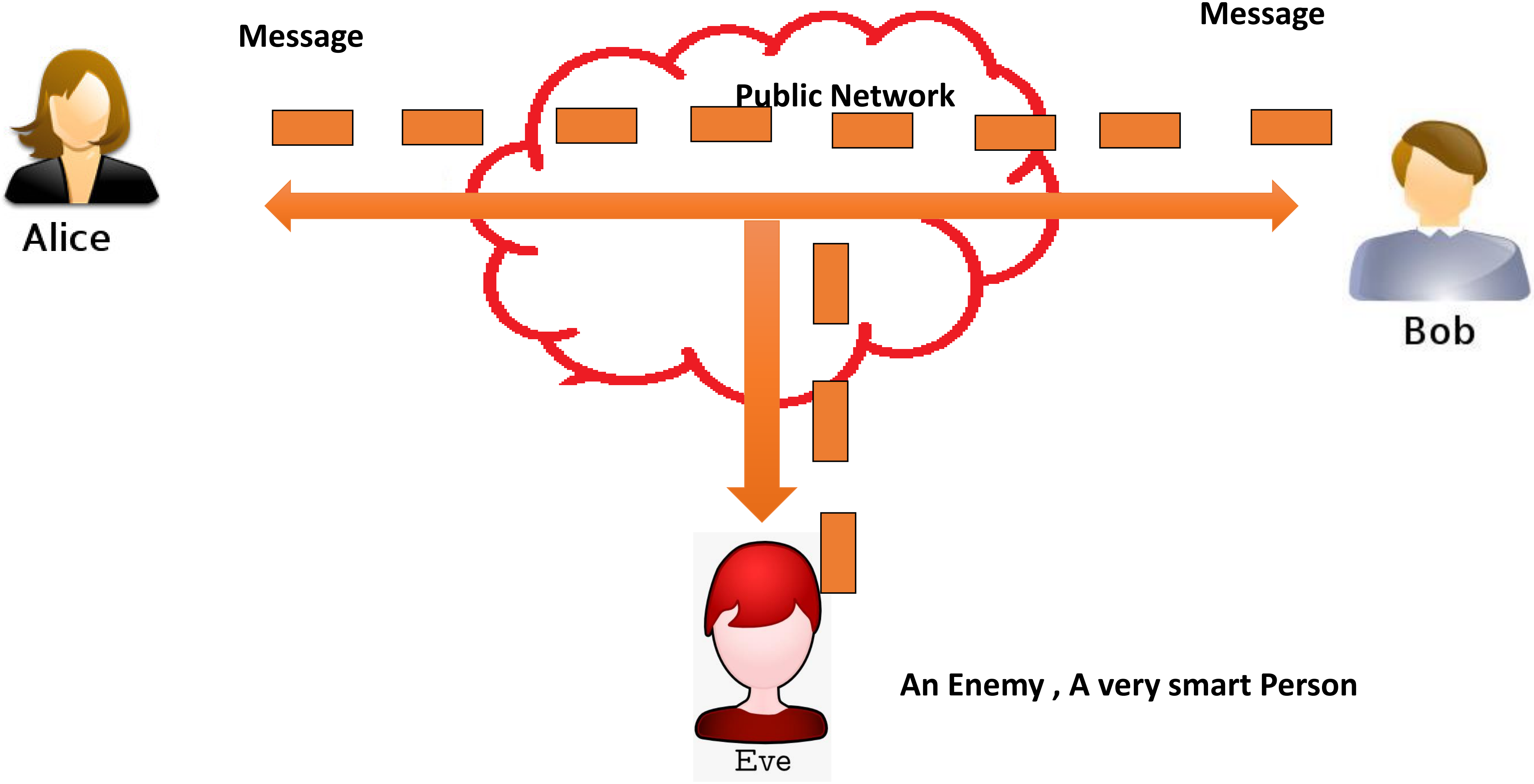
Interception


My Bank Account Number 123659874AB23
Alice
Message
Public Network
My Bank Account Number 123659874AB23
Message
Bob
My Bank Account Number 123659874AB23
Eve
An Enemy , A very smart Person

- **Attack on Confidentiality – Read the message**

Alice, Bob, Eve Framework

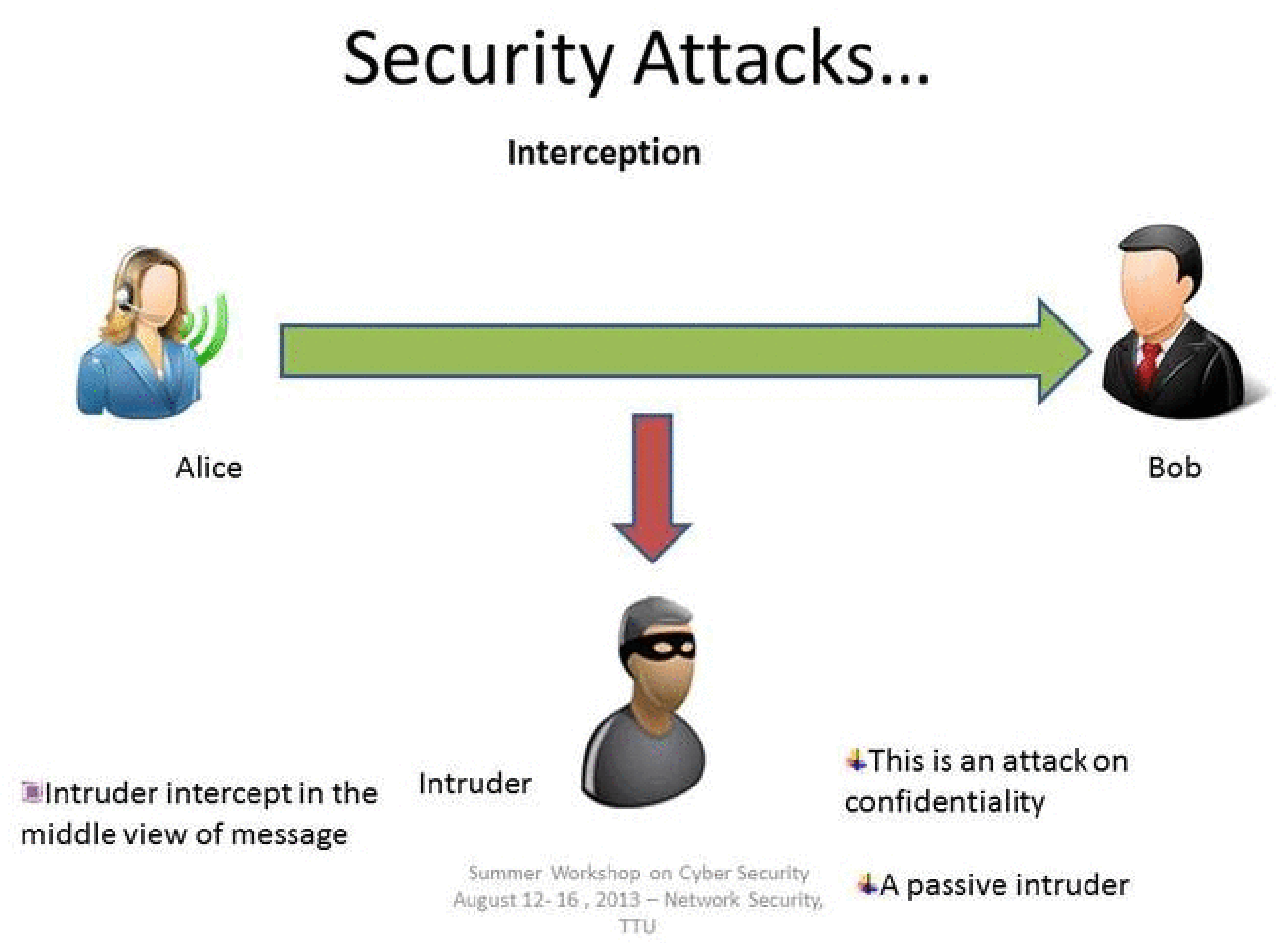
Interception



An Enemy , A very smart Person

Alice, Bob, Eve Framework

Interception



Security Attacks…

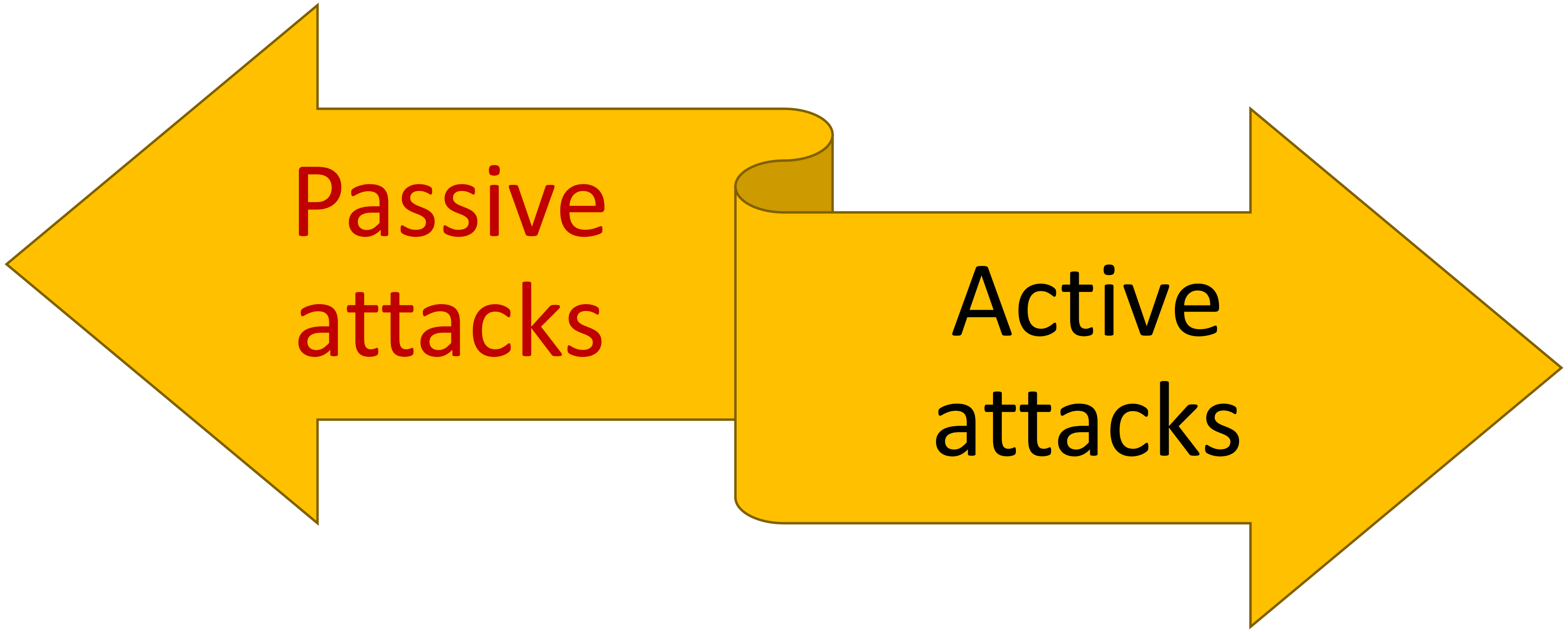
Interception

- Intruder intercept in the middle view of message

- This is an attack on confidentiality
- A passive intruder

Summer Workshop on Cyber Security
August 12- 16 , 2013 – Network Security,
TTU

Types of Attacks



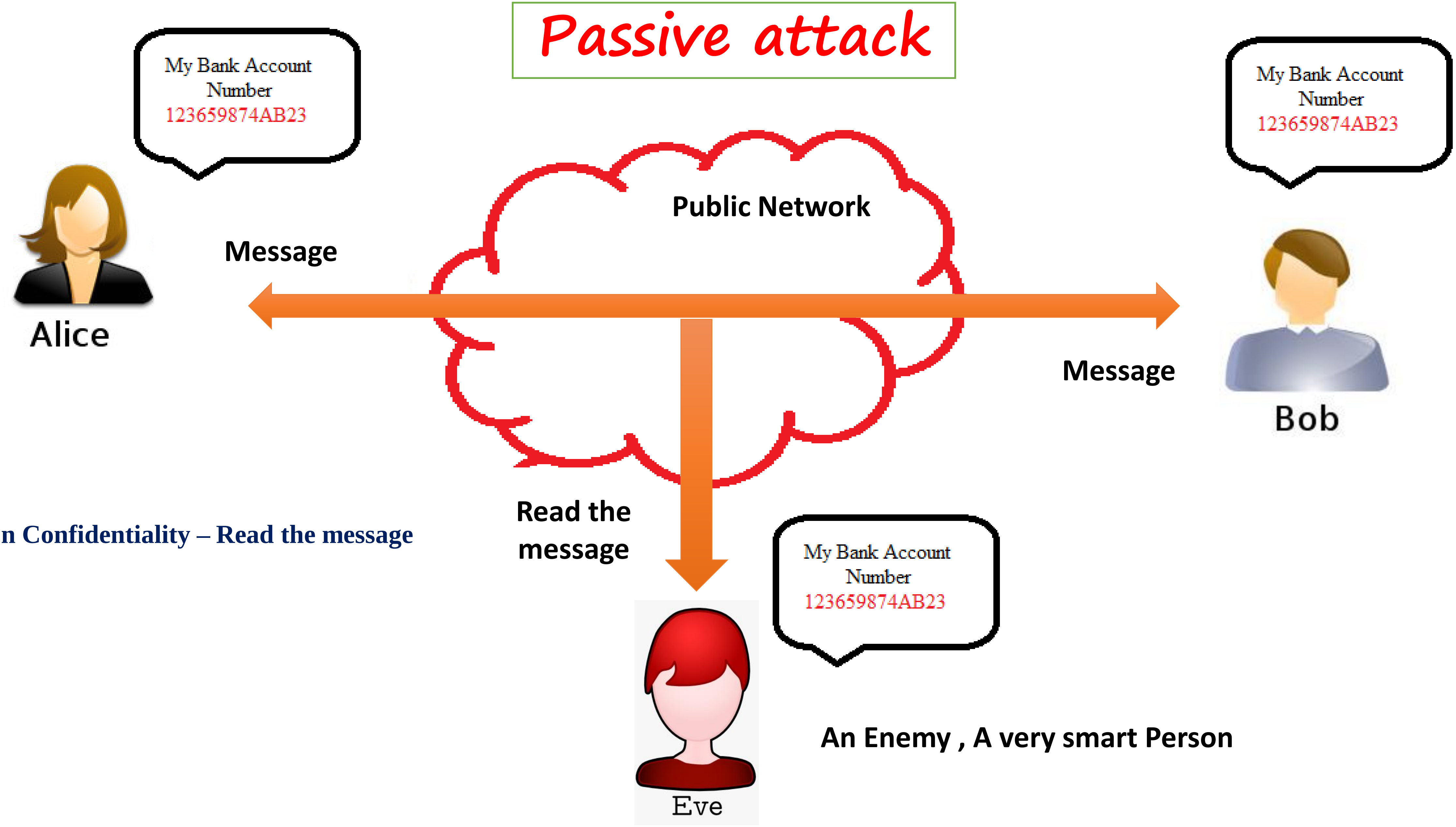
Passive attacks

Active attacks

Passive Attack

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.

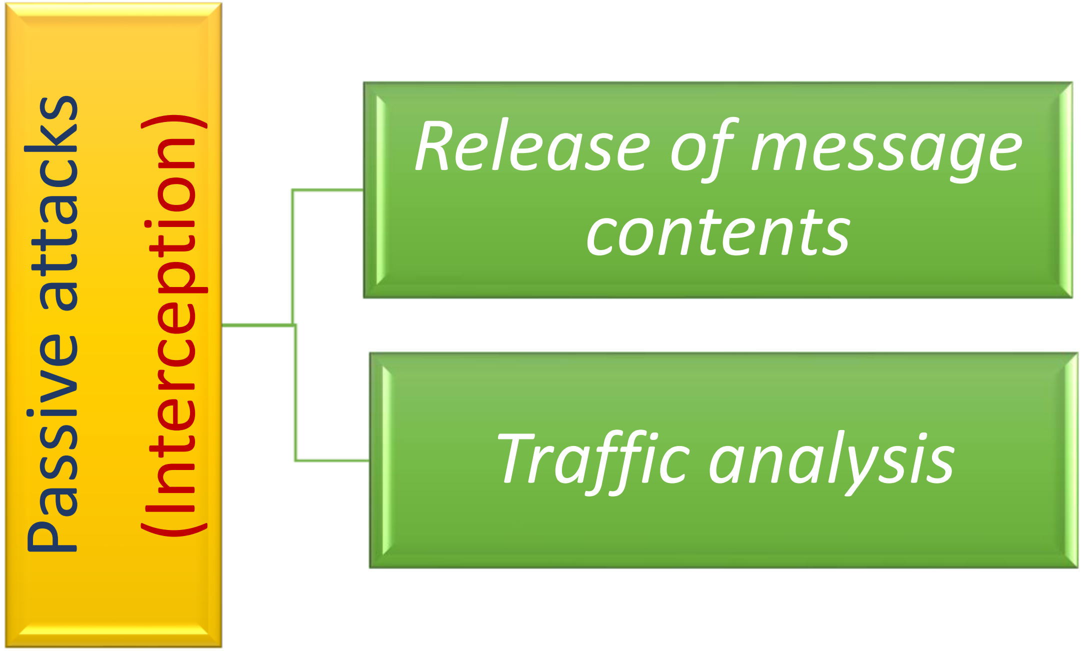
Passive attack


My Bank Account Number 123659874AB23
Alice
Message
Public Network
My Bank Account Number 123659874AB23
Message
Bob
Read the message
My Bank Account Number 123659874AB23
Eve
An Enemy , A very smart Person

- **Attack on Confidentiality – Read the message**

Alice, Bob, Eve Framework

Types of Passive Attack



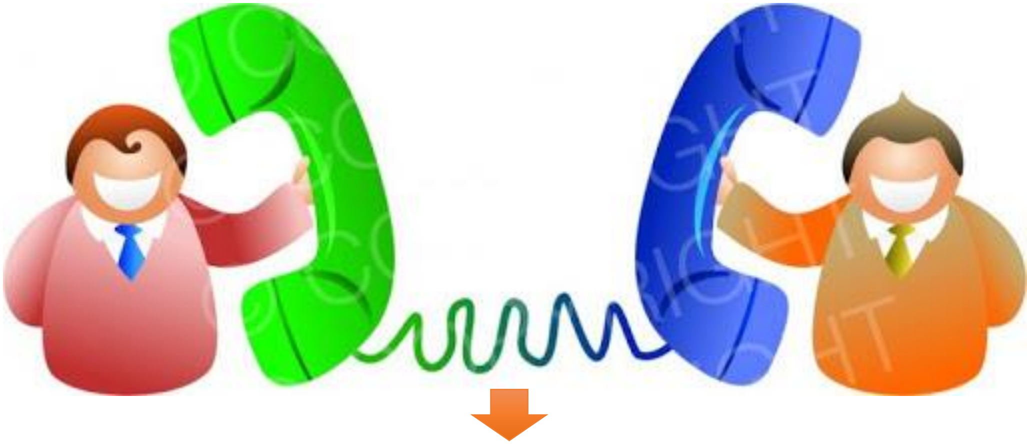
Passive attacks (Interception)

Release of message contents

Traffic analysis

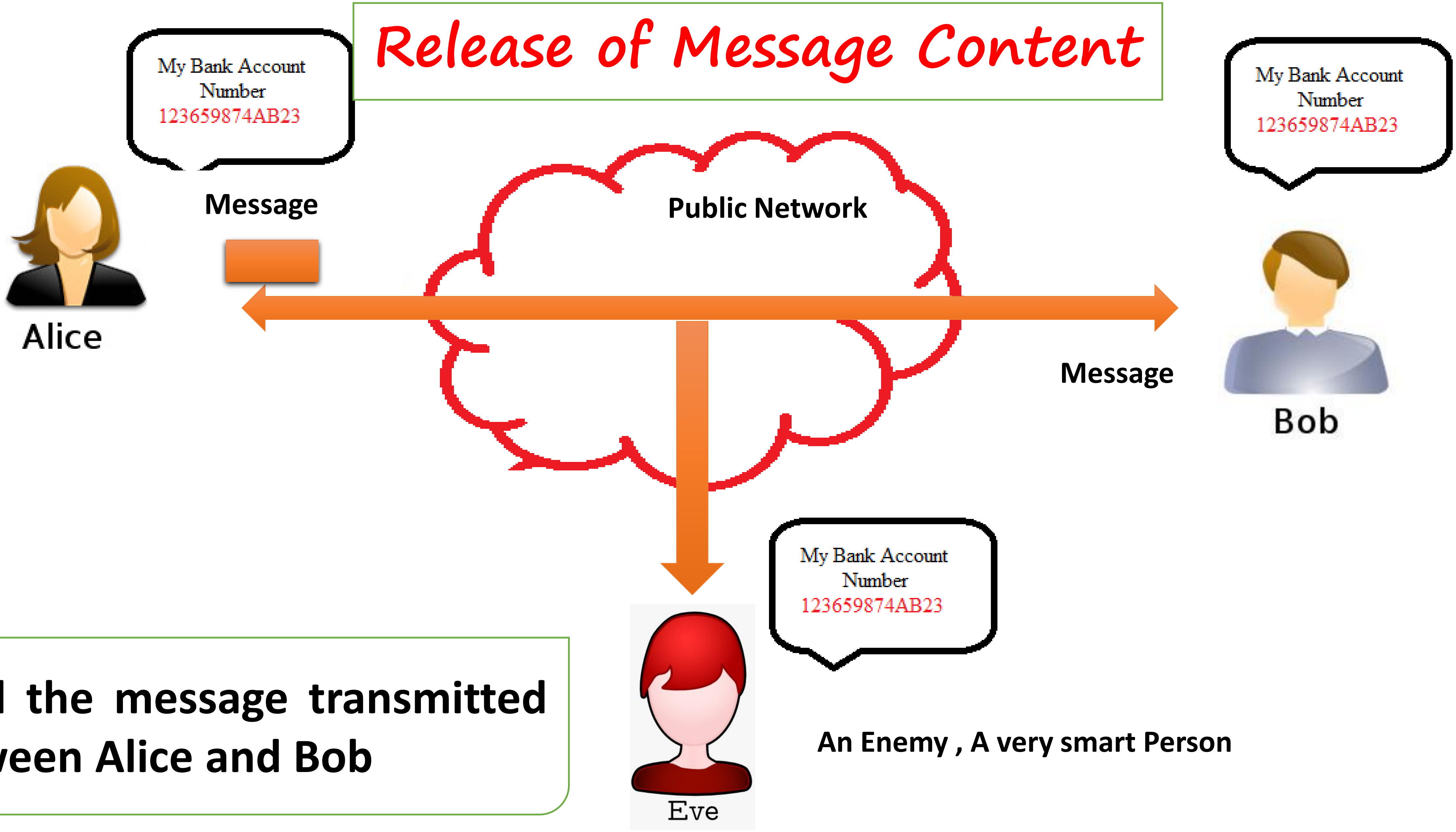
Release of message contents

Observe



Listen the
Communication

Release of Message Content


My Bank Account Number 123659874AB23
Message
Alice
Public Network
My Bank Account Number 123659874AB23
Message
Bob
My Bank Account Number 123659874AB23
Eve
An Enemy , A very smart Person

Read the message transmitted between Alice and Bob

Alice, Bob, Eve Framework

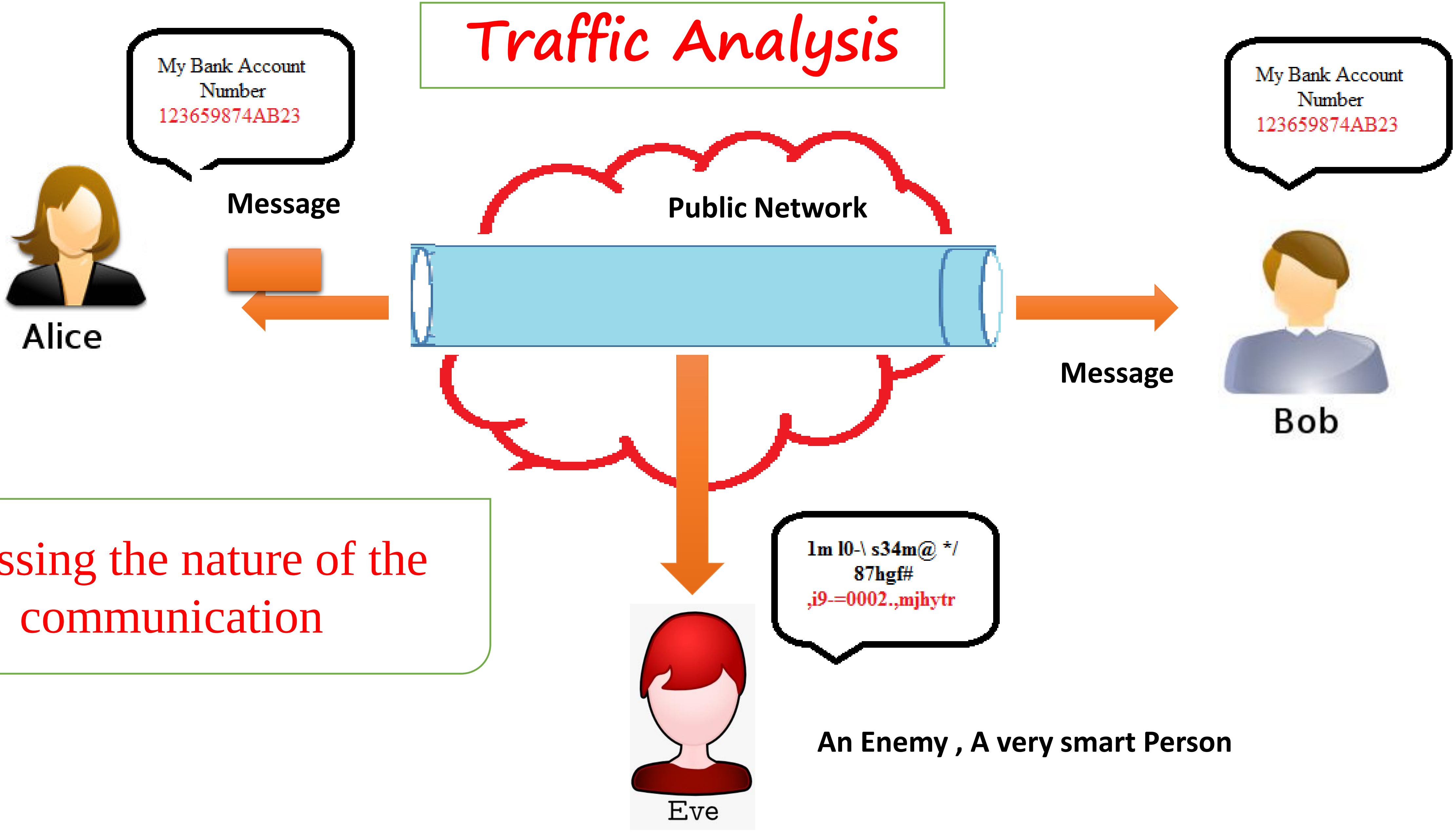
Traffic Analysis

- Traffic analysis – Attacker Monitor encrypted traffic flow to determine

1. location and identity of communicating hosts
2. Frequency and length of messages

This information might be useful in guessing the nature of the communication that was taking place

Traffic Analysis


My Bank Account Number 123659874AB23
Message
Alice
Public Network
My Bank Account Number 123659874AB23
Message
Bob
1m l0-\ s34m@ */ 87hgf# ,i9-=0002.,mjhytr
Eve
An Enemy , A very smart Person

Guessing the nature of the communication

Alice, Bob, Eve Framework

Passive Attacks

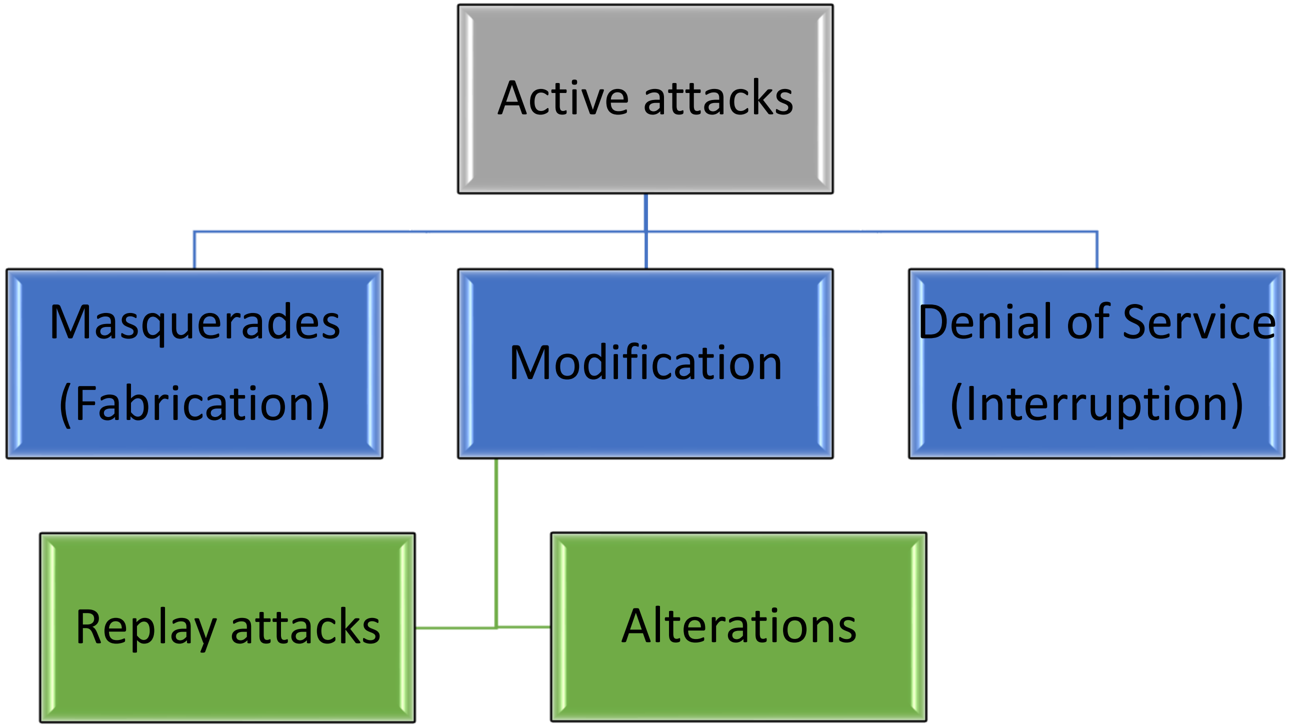
- **Passive attacks** are difficult to detect because they do not involve any alteration of the data.
- Neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern

Interception **Confidentiality**

- Passive attacks can be prevented by applying encryption

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream.



Active Attacks

- Active attacks
- The aim of attacker is to make some modification to the information that is being transmitted.

(or)

- creation of a false information and send it to destination by behaving as genuine sender

Modification	**Integrity**
Interruption	**Availability**
Fabrication	**Authentication**

Active Attacks

1. Masquerade of one entity as some other

2. Replay previous messages

3. Modify/alter (part of) messages in transit to produce an unauthorized effect

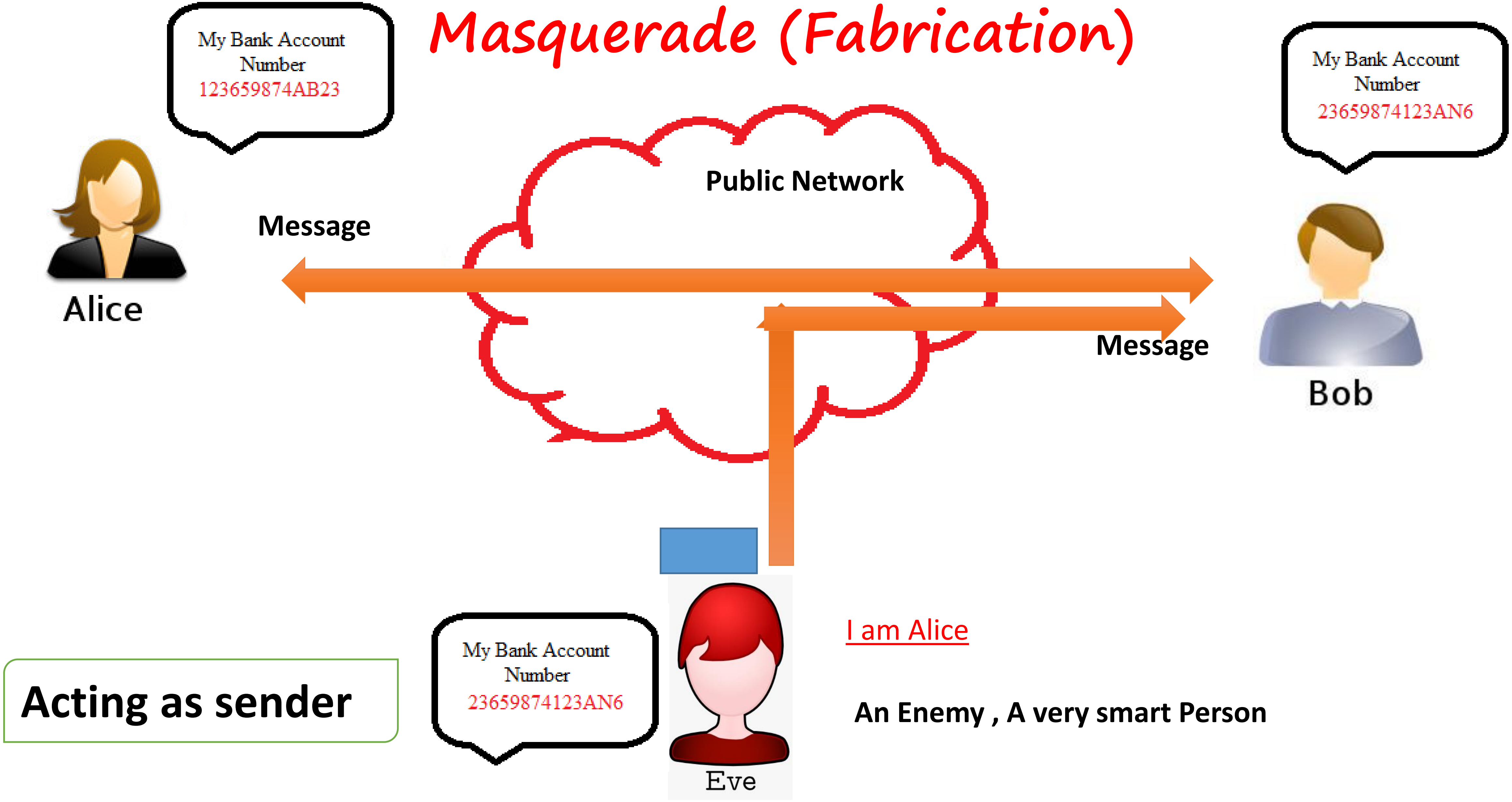
4. Denial of service - prevents or inhibits the normal use or management of communications facilities

.

Masquerade (Fabrication)

- Masquerade takes place when one entity pretends to be a different entity
- A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

Masquerade (Fabrication)



My Bank Account Number 123659874AB23

Alice

Message

Public Network

My Bank Account Number 23659874123AN6

Bob

Message

I am Alice

An Enemy , A very smart Person

Acting as sender

My Bank Account Number 23659874123AN6

Eve

Alice, Bob, Eve Framework

Masquerade (Fabrication)

Masquerade takes place when one entity pretends to be a different entity

- Attacker sends the email to receiver and sign it as sender. Here just attacker changes the sender identity.
- In internet, an attacker changes the IP address of the sending messages. Example (IP SPOOFING)

Masquerade (Fabrication)

- Masquerade attacks can be performed using

1. stolen passwords and logons,

2. By locating gaps in programs,

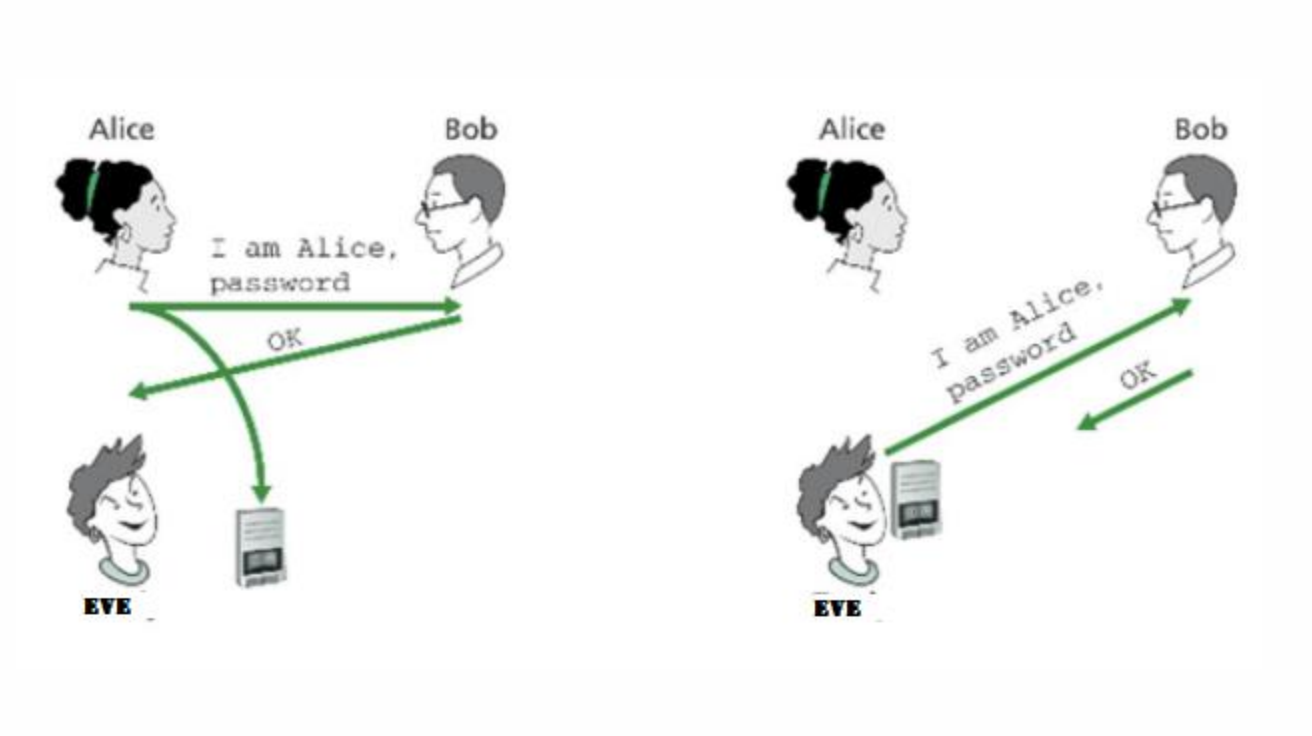
3. By finding a way around the authentication process..

Replay Attack (Modification)

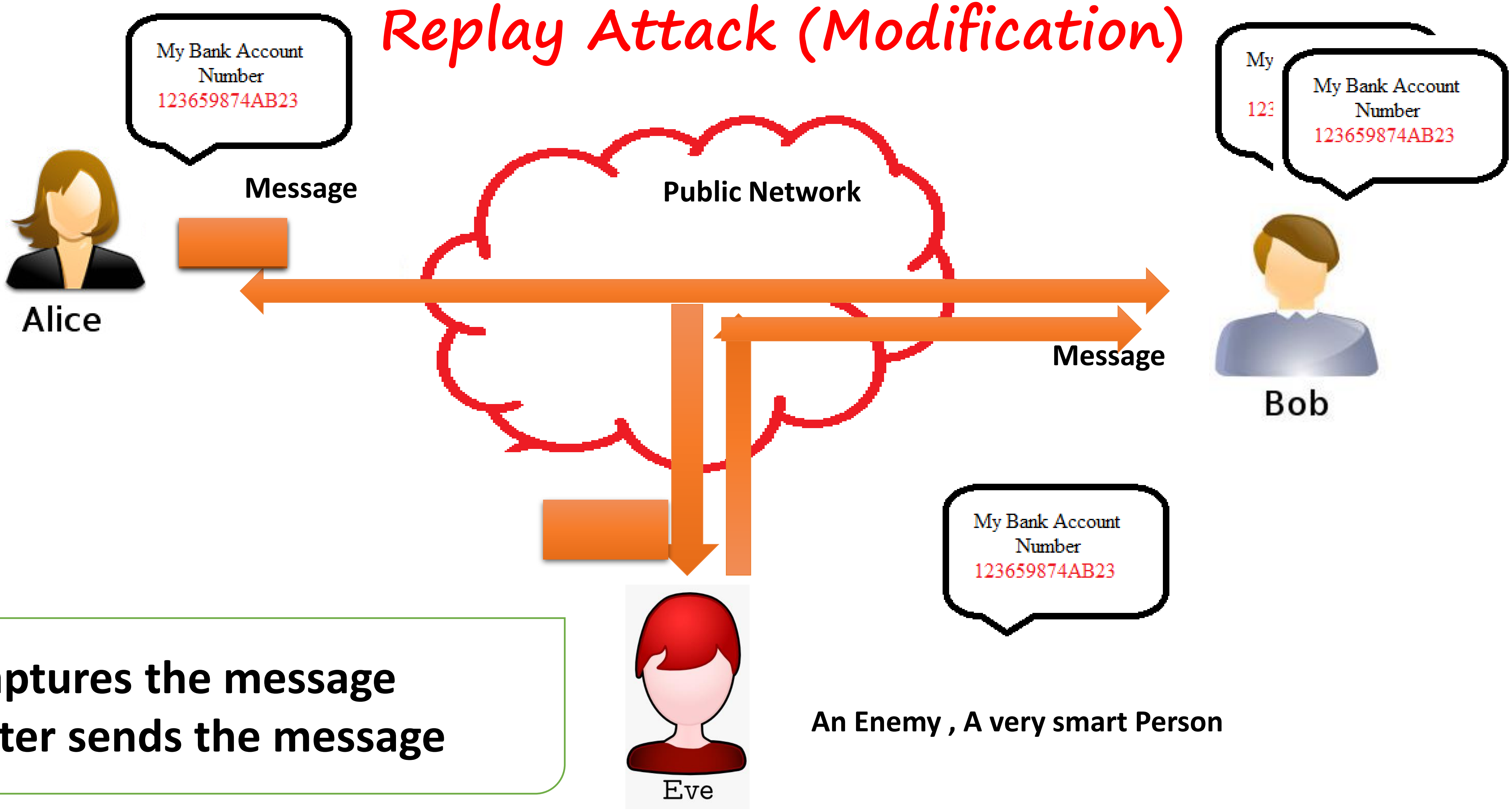
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- An attacker detects a data transmission and fraudulently has it delayed or repeated.
- An attacker captures the network traffic and then sends the communication to its original destination, acting as an original sender.
- It is the combination of two attacks i.e., interception and masquerade.

Replay Attack (Modification)



Replay Attack (Modification)

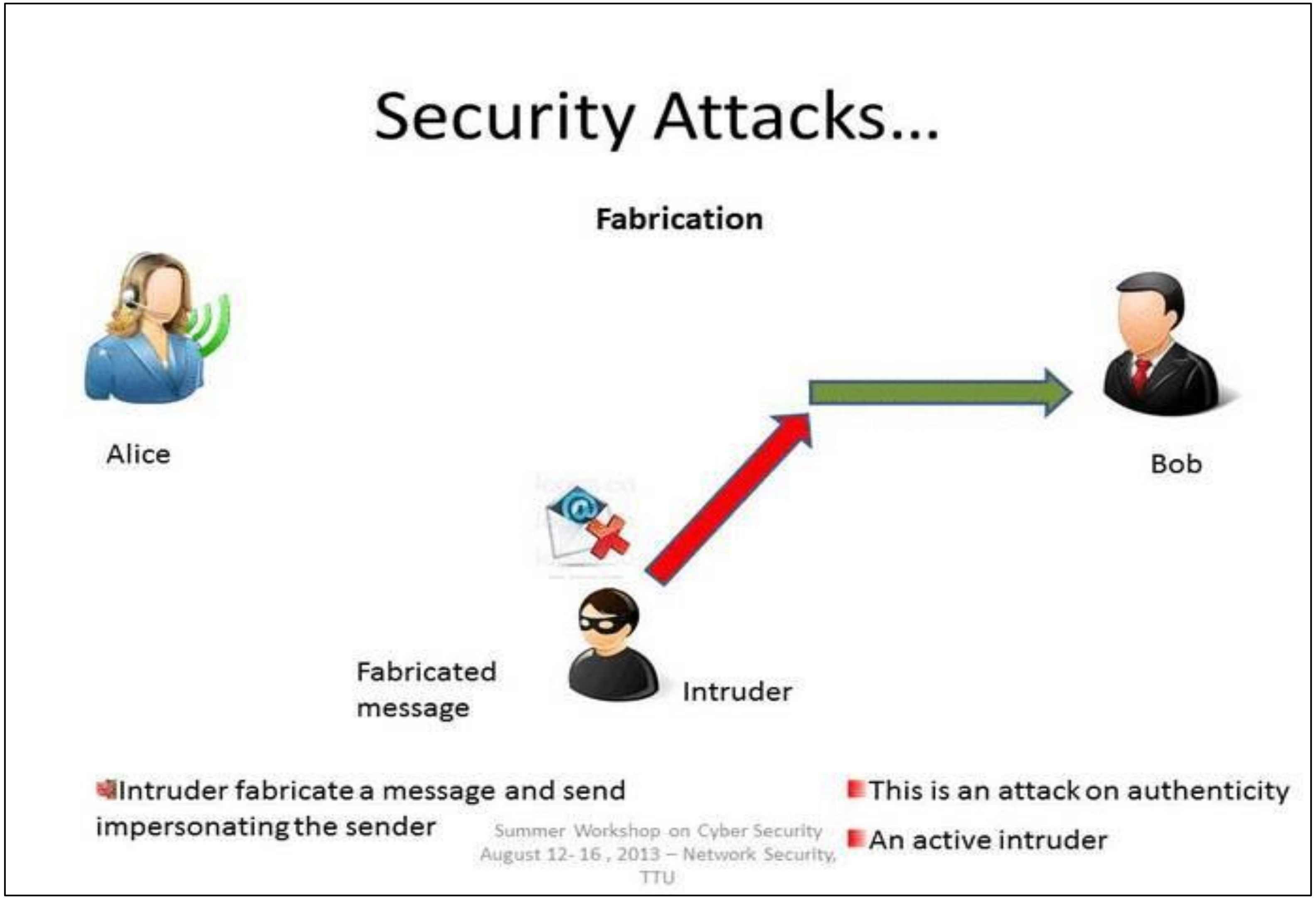

My Bank Account Number 123659874AB23
Message
Alice
Public Network
My
123
My Bank Account Number 123659874AB23
Bob
Message
My Bank Account Number 123659874AB23
Eve

1. Captures the message
2. Later sends the message

An Enemy , A very smart Person

Alice, Bob, Eve Framework

Masquerade (Fabrication)



Security Attacks...

Fabrication

- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

Replay Attack (Modification)

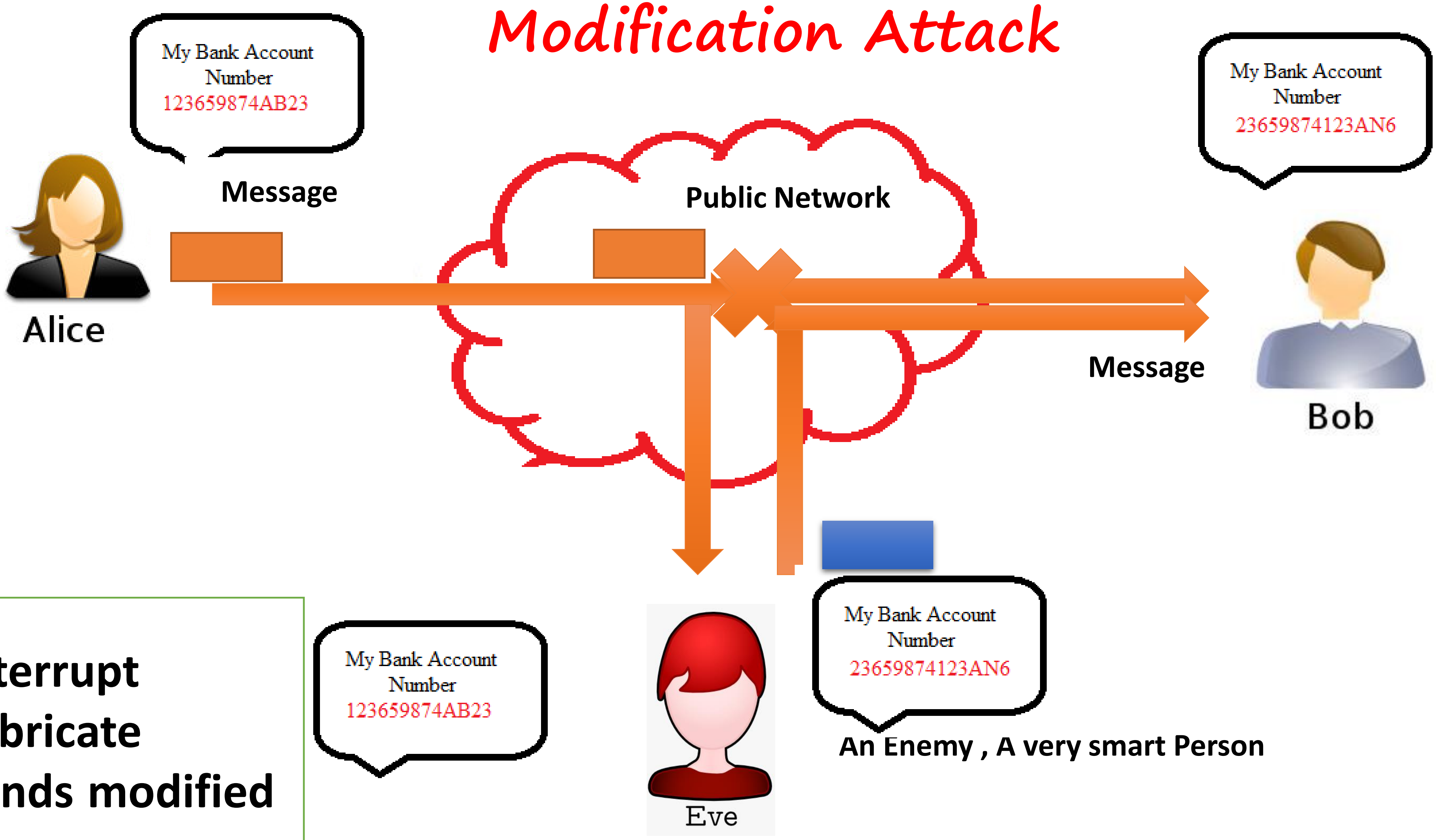
- Example: - Sender asks the destination to pay Rs. 1000, the information is captured by the attacker and he also send the same message to receiver that the pay Rs. 1000. Now receiver receive the two messages and he believe that Rs. 2000 should be paid to sender.
- How to overcome: - Time stamp and sequence number.

Modification Attack

- An attacker intercepts the messages and changes the contents of the messages and send it to receiver.

- Attacker changes the some portion of a message or that message is delayed or reordered to produce an unauthorized effect.

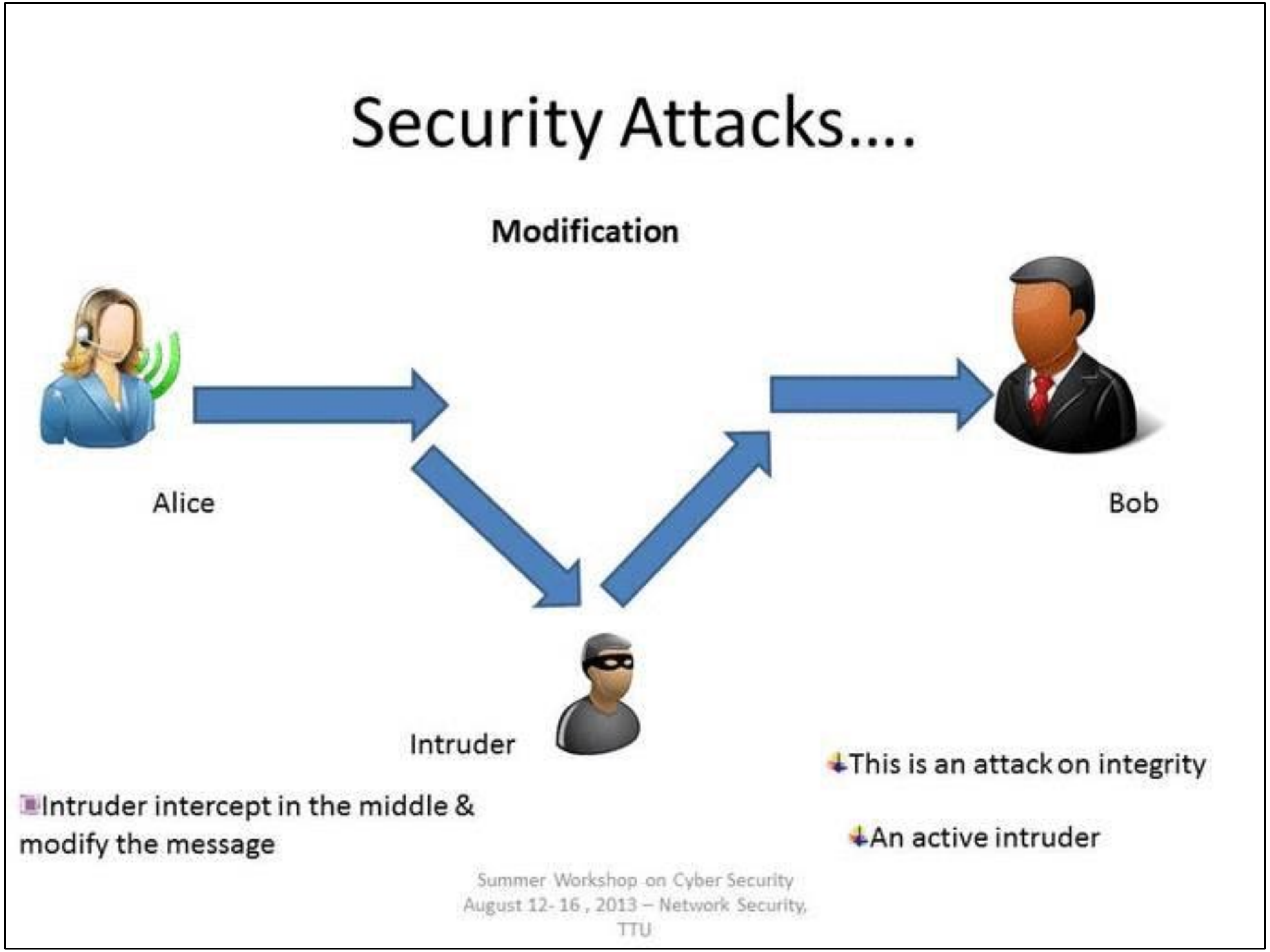
Modification Attack


My Bank Account Number 123659874AB23
Message
Alice
Public Network
My Bank Account Number 23659874123AN6
Message
Bob
My Bank Account Number 123659874AB23
Eve
My Bank Account Number 23659874123AN6
An Enemy , A very smart Person

1. **Interrupt**
2. **Fabricate**
3. **Sends modified message**

Alice, Bob, Eve Framework

Modification Attack



Security Attacks….

Modification

- Intruder intercept in the middle & modify the message

- This is an attack on integrity

- An active intruder

Summer Workshop on Cyber Security
August 12- 16 , 2013 – Network Security,
TTU

Modification Attack

- For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.
- An attacker needs to block the direct communication (DNS hijacking) and then act as a masquerade

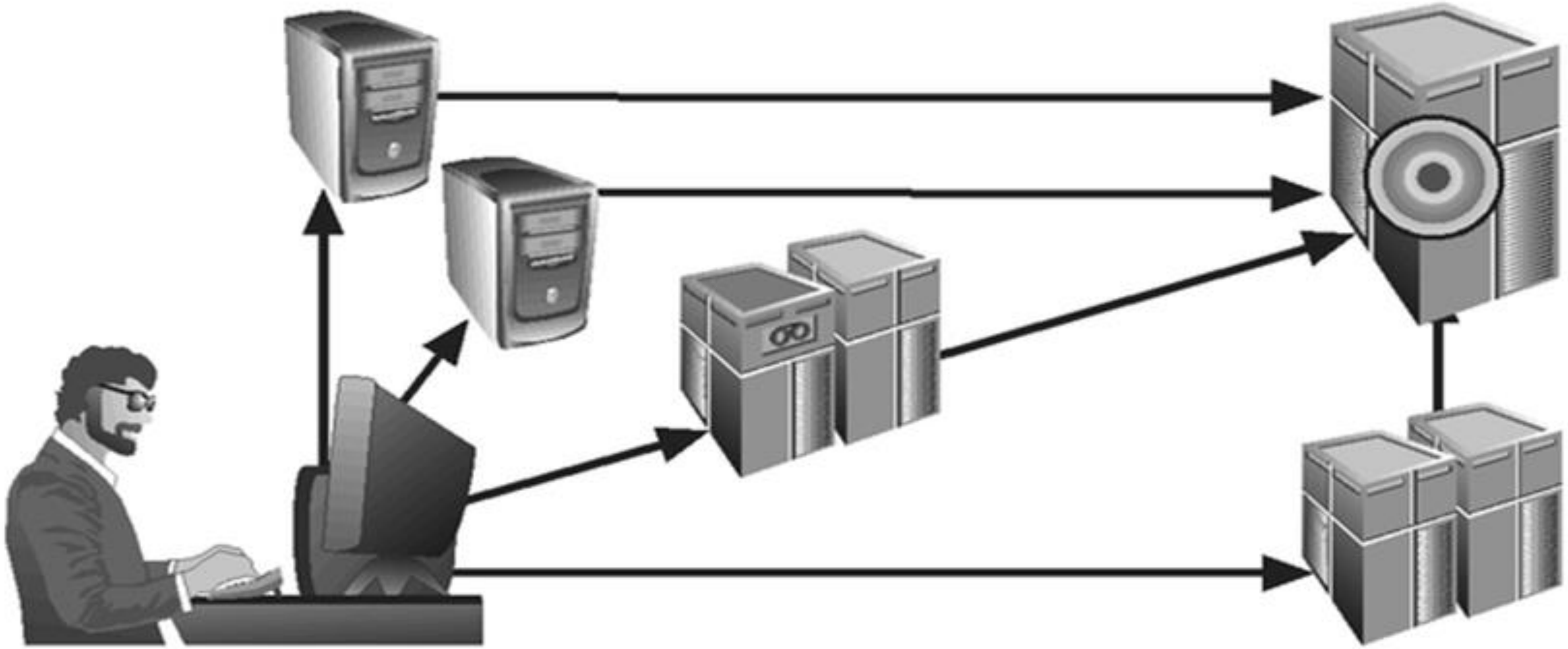
Denial of Service Attack

- The aim of the attacker to block the usage of network resources. Such resources can be computers or end users or laptops or servers or network links.

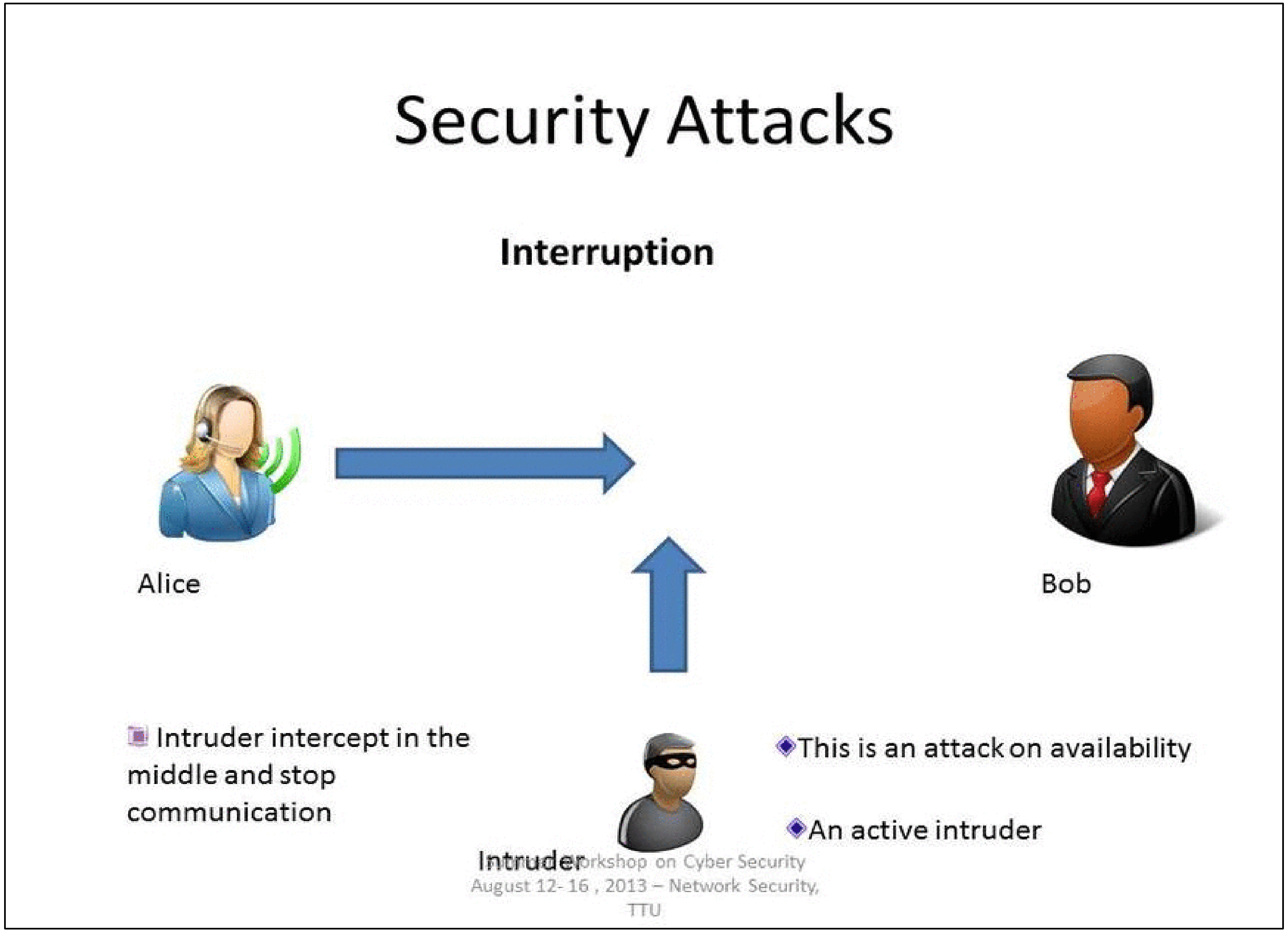
DOS (Denial of Service)

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.



DOS (Denial of Service)



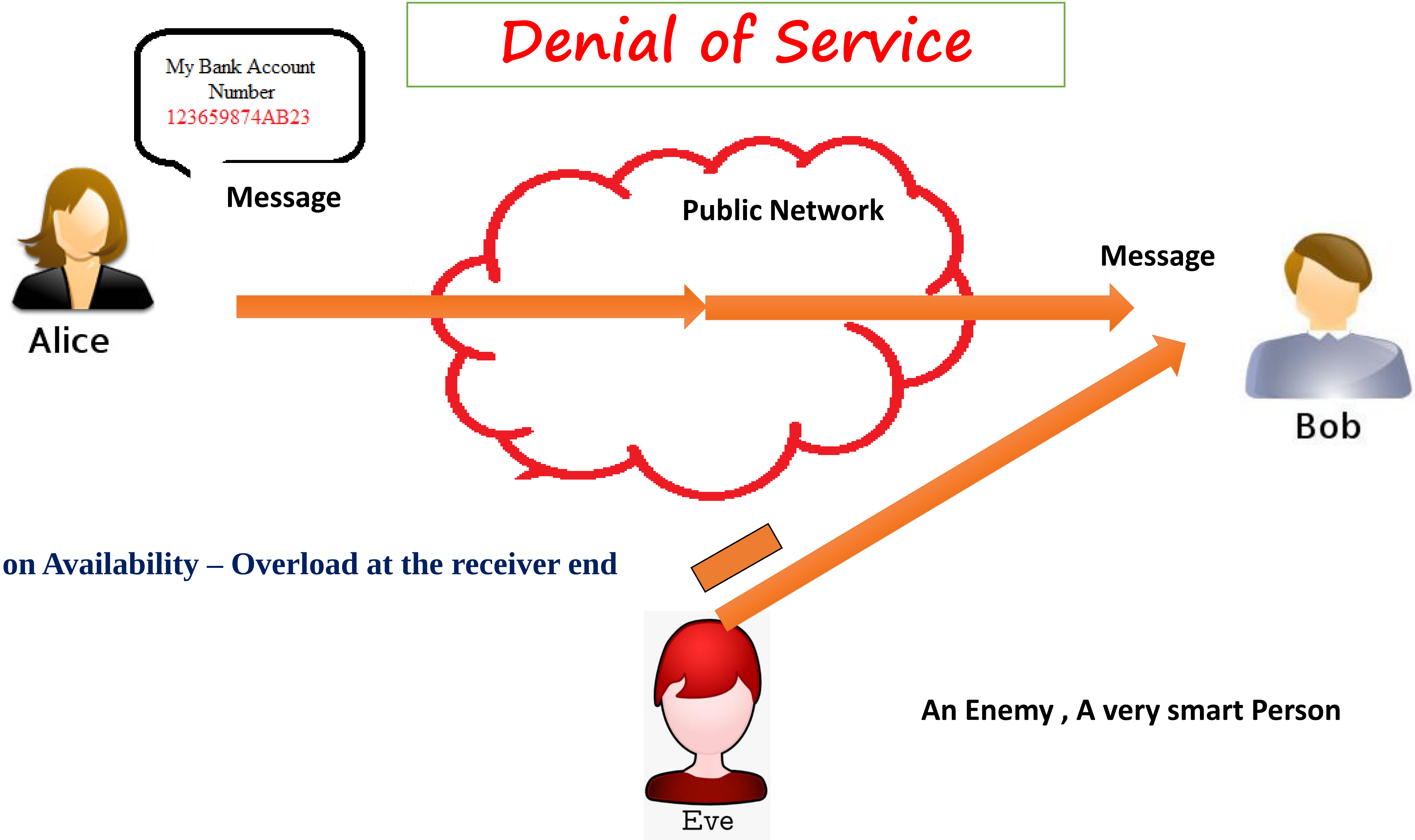
Security Attacks

Interruption

- Intruder intercept in the middle and stop communication

- This is an attack on availability
- An active intruder

Denial of Service



- **Attack on Availability – Overload at the receiver end**

Alice, Bob, Eve Framework

Denial of Service

- **Example**: - An attacker want to overload any computer. He sends the repeated messages to the computer so as to create heavy load on the computer. Attacker uses intermediate system as the amplifier to generate the one packet to 50 are more packets, and also it hides the IP address of the attacker. If attacker uses the multiple amplifier then the attack called as distributed denial of service attack.
- Denial of service (DoS). It may slow down or totally interrupt the service of a system

Need of Security

Protects personal identification information

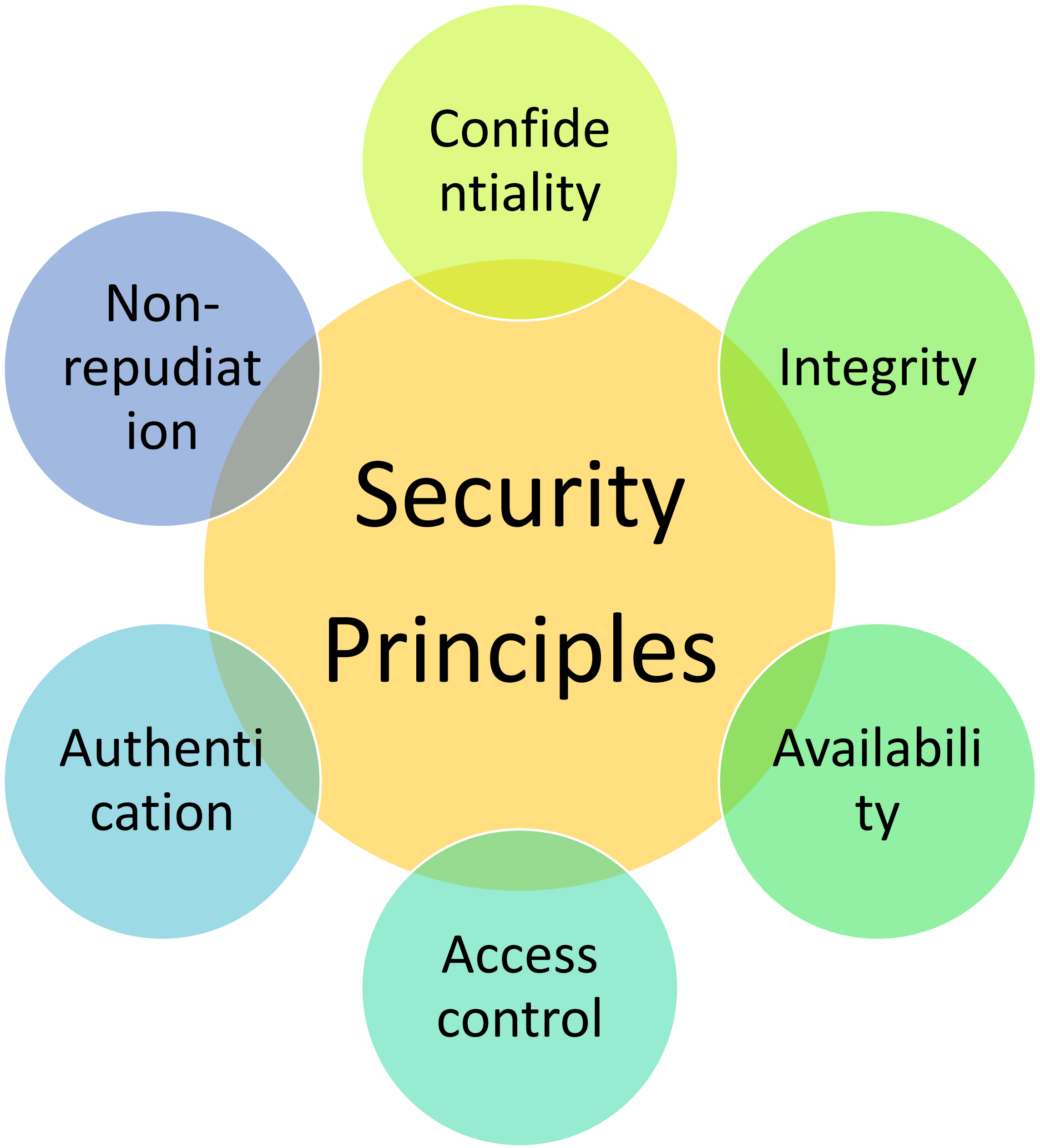
Protects sensitive data

Safeguarding technology assests in organizations

Enables the safe operation of applications

Surveillance

Security Services



Related to a message

- ***Confidentiality:*** It specifies that only the sender and the intended recipient(s) should be able to access a message.
  Attack- Interception
- ***Integrity:*** It ensures that the contents of the message remains unaltered when it reaches the recipient.
  Attack- Modification
- ***Authentication:*** It helps to establish proof of identities.
  Attack- Fabrication
- ***Non-repudiation:*** It does not allow the sender of a message to refute the claim of not sending that message.

Related to the overall system

- ***Access control:*** It specifies and controls who can access what.
- ***Availability:*** It states that resources (i.e. information) should be available to authorized parties at all times.
  Attack- Interruption

Authentication

- Assures recipient that the message is from the source that it claims to be from.
- Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Two types of Authentication:

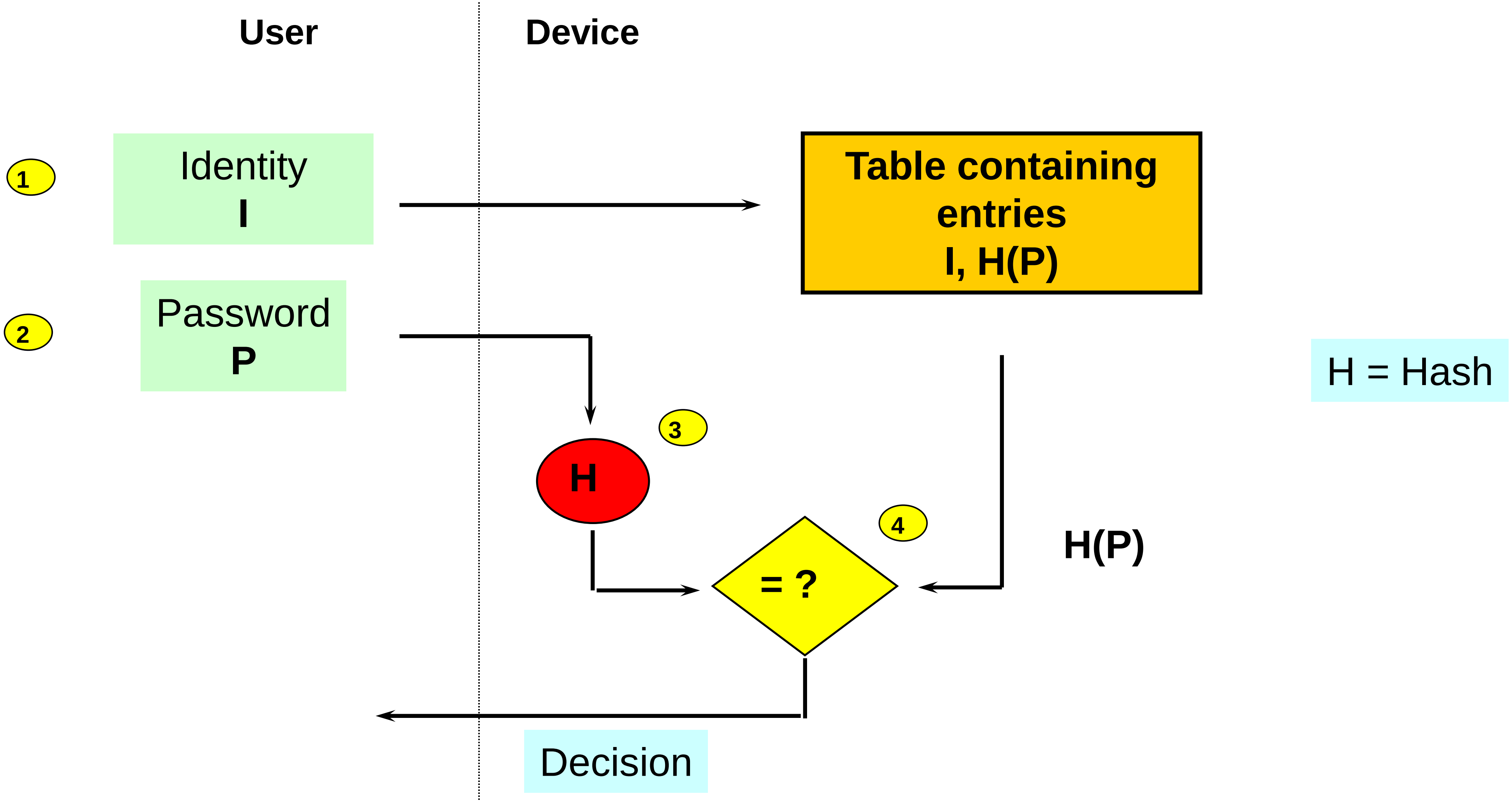
1. **Peer entity authentication**

   It provides mutual confidence in the identities of the parties involved in a connection. Both communicating entities provide each other with assurance of their identity.

2. **Data origin authentication**

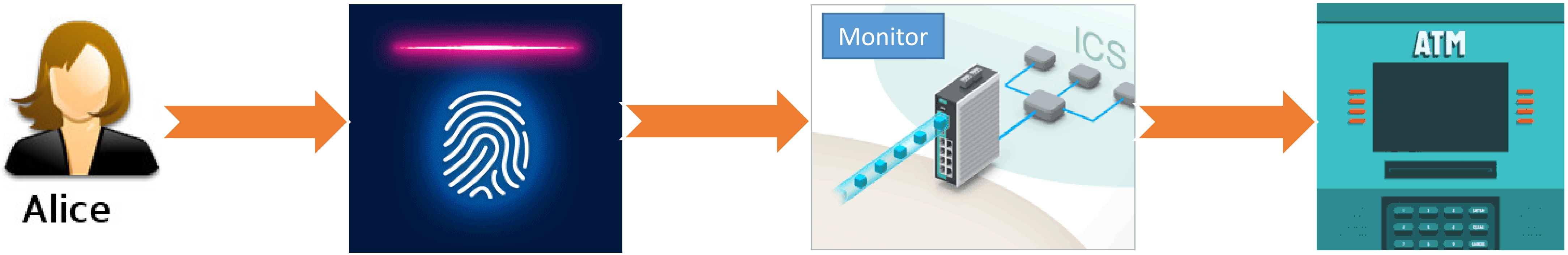
   It insures the assurance about the source of the received data.

Authentication



Access Control

The prevention of unauthorized use of a resource (i.e. this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).



Alice

Access Request

Guard

Resources

Confidentiality

It is the protection of information from unauthorized disclosure (against eavesdropping).

Four types of Confidentiality:

1. **Connection Confidentiality**

   The protection of all user data on a connection.

2. **Connectionless Confidentiality**

   The protection of all user data in a single data block.

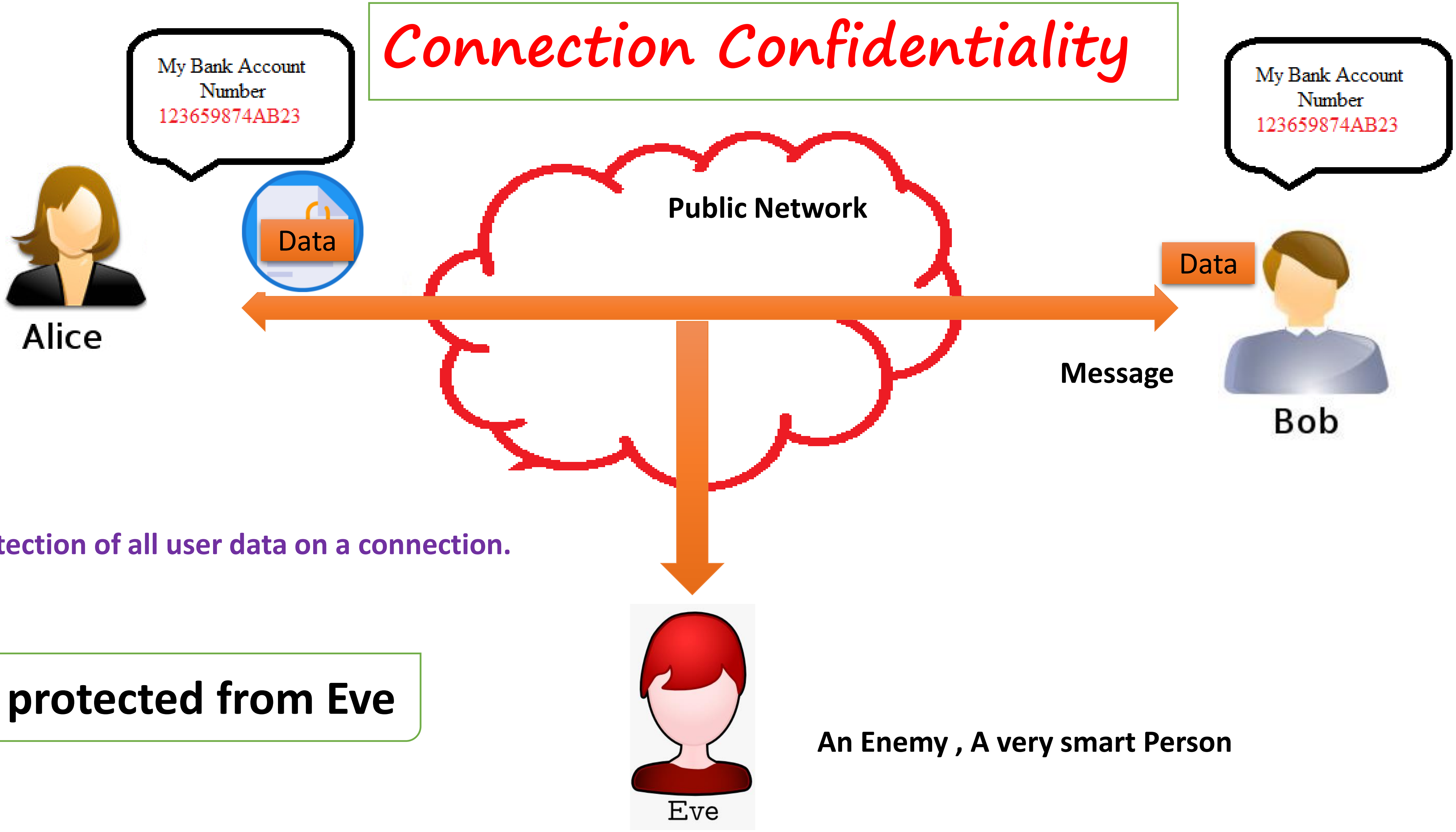
3. **Selective-Field Confidentiality**

   The confidentiality of selected fields within the user data on a connection or in a single data block.

4. **Traffic-flow Confidentiality**

   The protection of the information that might be derived from observation of traffic flows

Connection Confidentiality

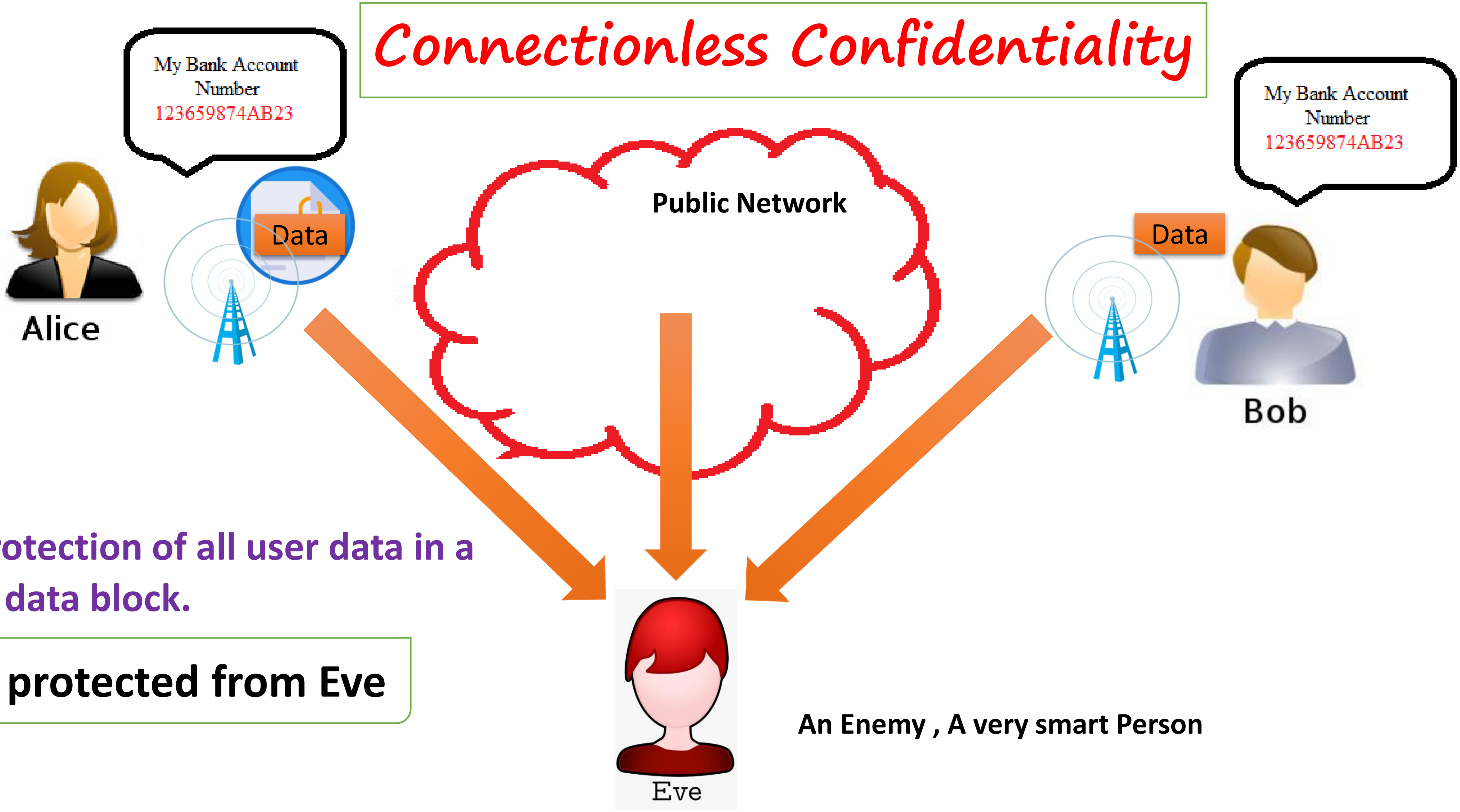


The protection of all user data on a connection.

Data protected from Eve

Alice, Bob, Eve Framework

Connectionless Confidentiality



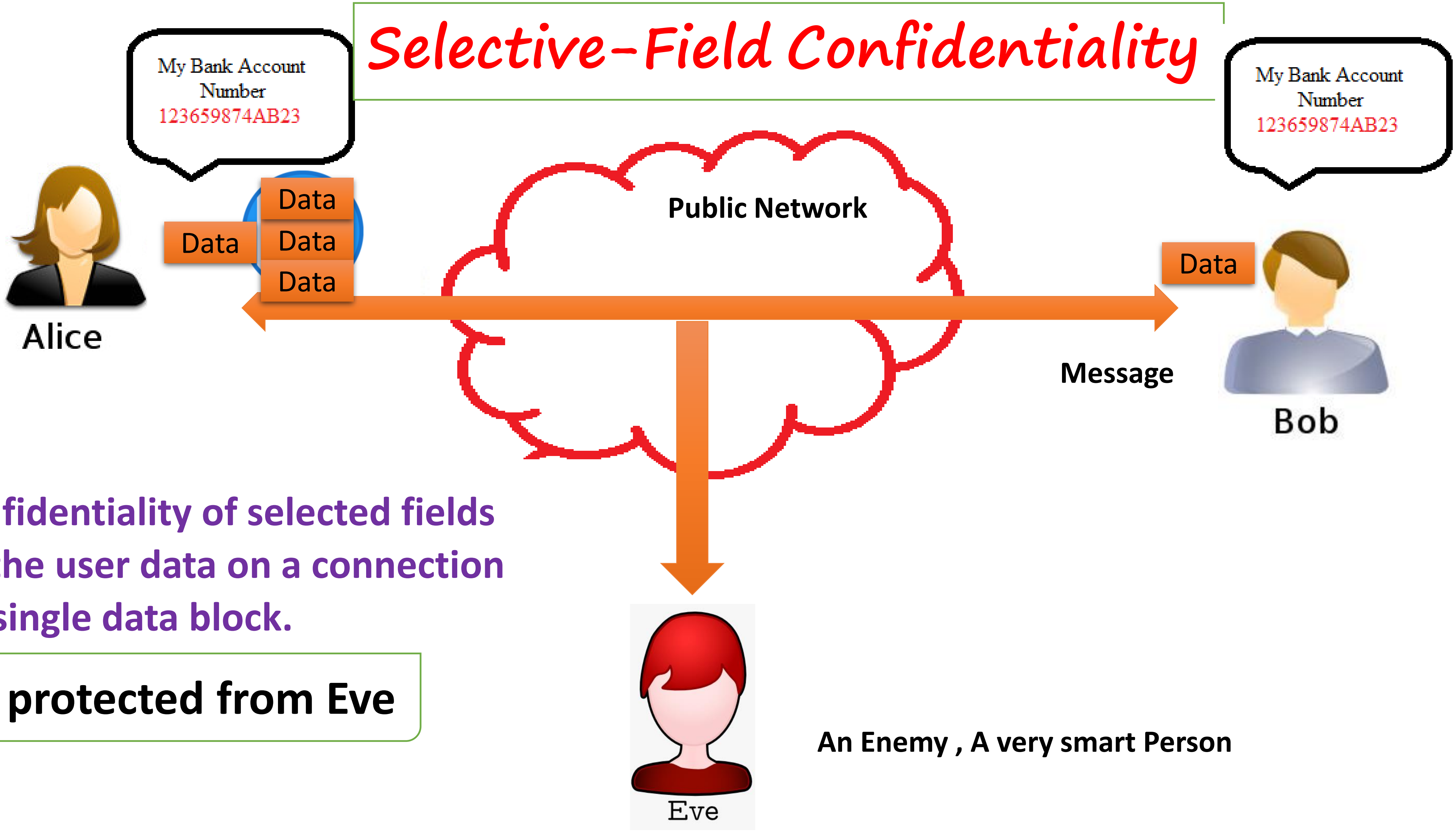
An Enemy , A very smart Person

The protection of all user data in a single data block.

Data protected from Eve

Alice, Bob, Eve Framework

Selective-Field Confidentiality

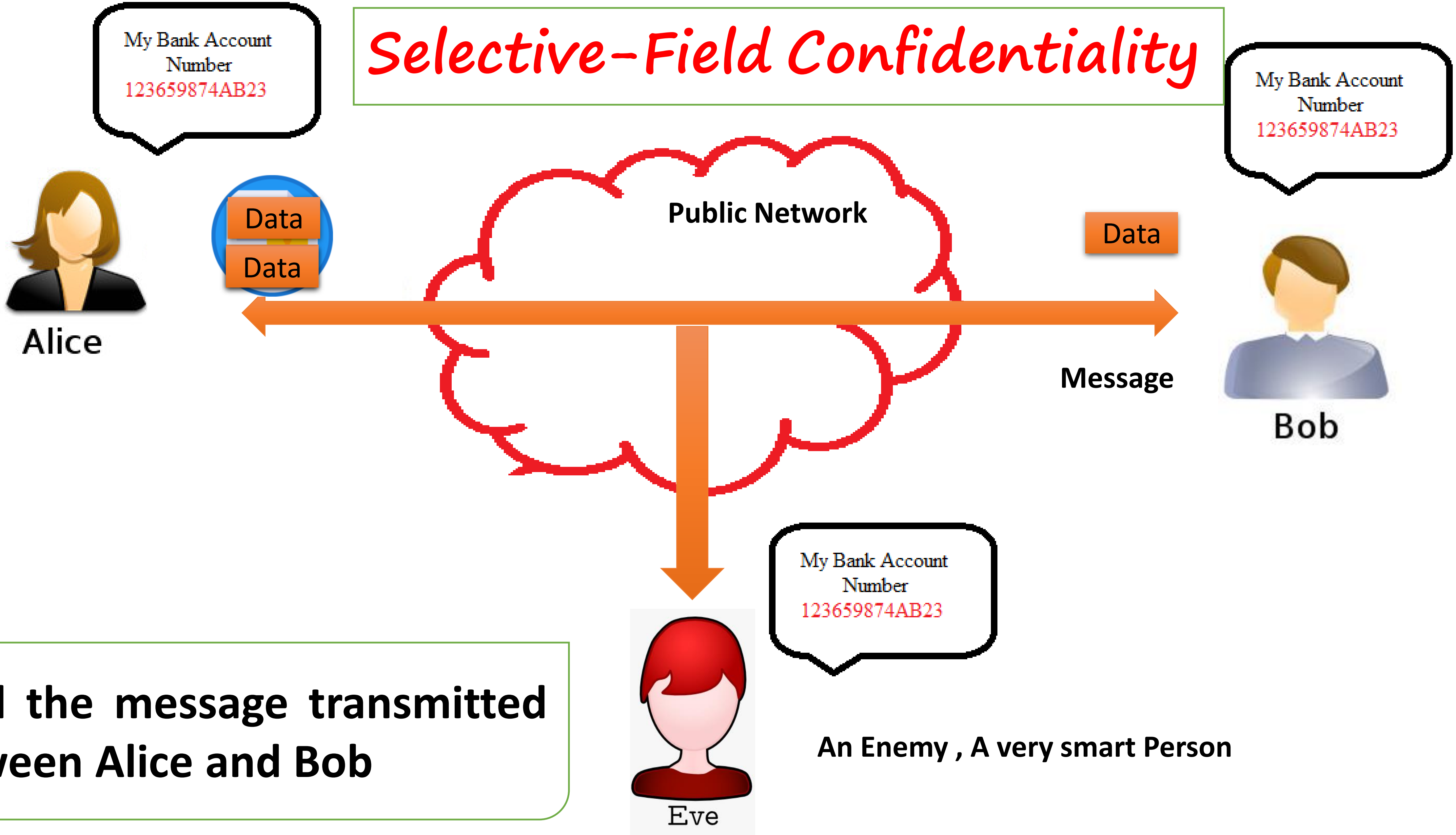

My Bank Account Number 123659874AB23
Data
Data
Data
Data
Alice
Public Network
Data
Message
My Bank Account Number 123659874AB23
Bob
Eve
An Enemy , A very smart Person

The confidentiality of selected fields within the user data on a connection Or in a single data block.

Data protected from Eve

Alice, Bob, Eve Framework

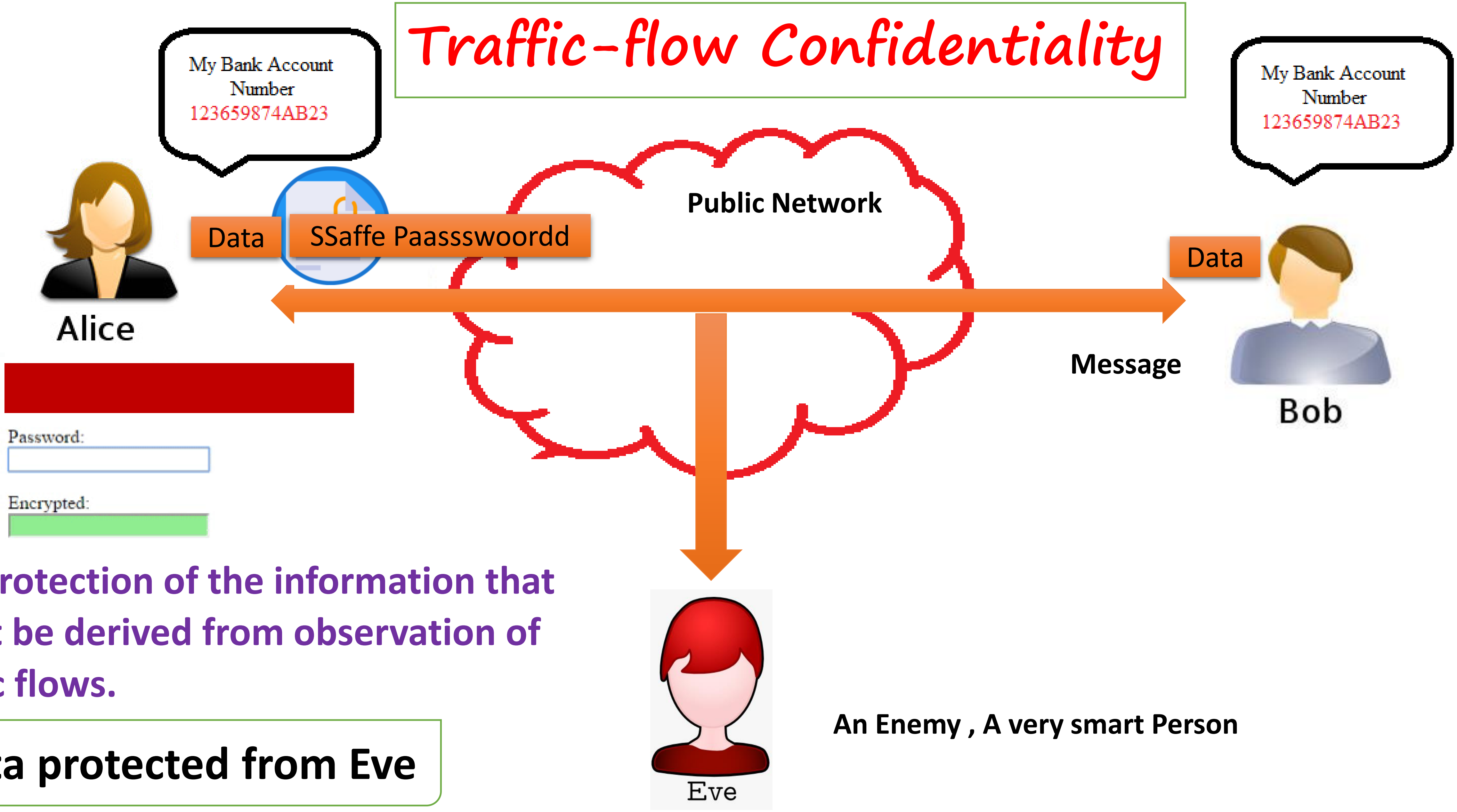
Selective-Field Confidentiality


My Bank Account Number 123659874AB23
Alice
Data
Data
Public Network
My Bank Account Number 123659874AB23
Data
Message
Bob
My Bank Account Number 123659874AB23
Eve
An Enemy , A very smart Person

Read the message transmitted between Alice and Bob

Alice, Bob, Eve Framework

Traffic-flow Confidentiality


My Bank Account Number 123659874AB23
Data
SSaffe Paassswoordd
Public Network
Alice
Password:
Encrypted:
My Bank Account Number 123659874AB23
Data
Message
Bob
Eve
An Enemy , A very smart Person

The protection of the information that might be derived from observation of traffic flows.

Data protected from Eve

Alice, Bob, Eve Framework

Data Integrity

Assurance that data received are exactly as sent by an authorized sender i.e. no modification, insertion, deletion or replay.

PRACTICAL NETWORKING .NET
Sender
Receiver

Data Integrity

Five types of Integrity:

- Connection Integrity with Recovery
- Connection Integrity without Recovery
- Selective-Field Connection Integrity
- Connectionless Integrity
- Selective-Field Connectionless Integrity

Non-repudiation

It is the concept of protection against denial by one of the parties in a communication.

There are two types of non-repudiation:

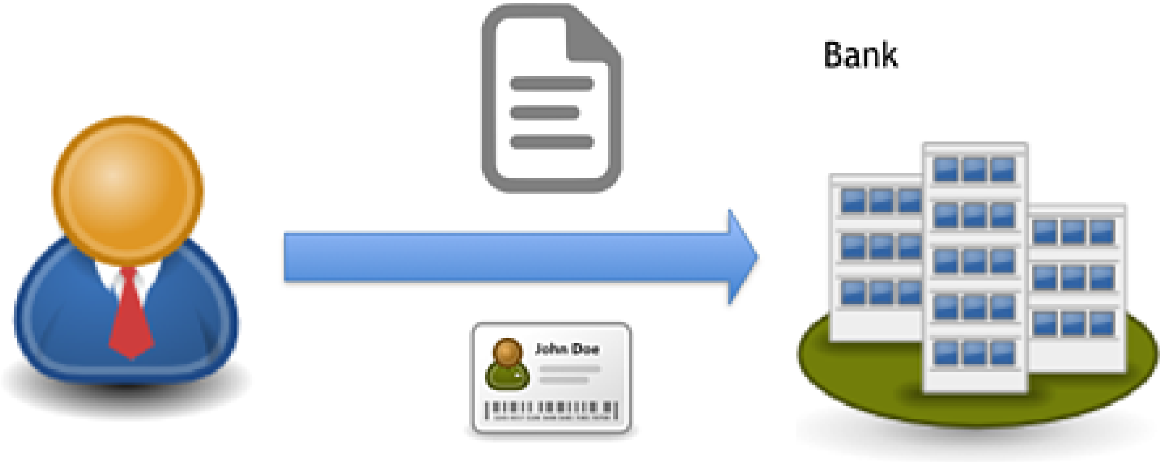
1. **Origin non-repudiation**

   It is the proof that the message was sent by the specified party.

2. **Destination non-repudiation**

   It is the proof that the message was received by the specified party.

Origin non-repudiation

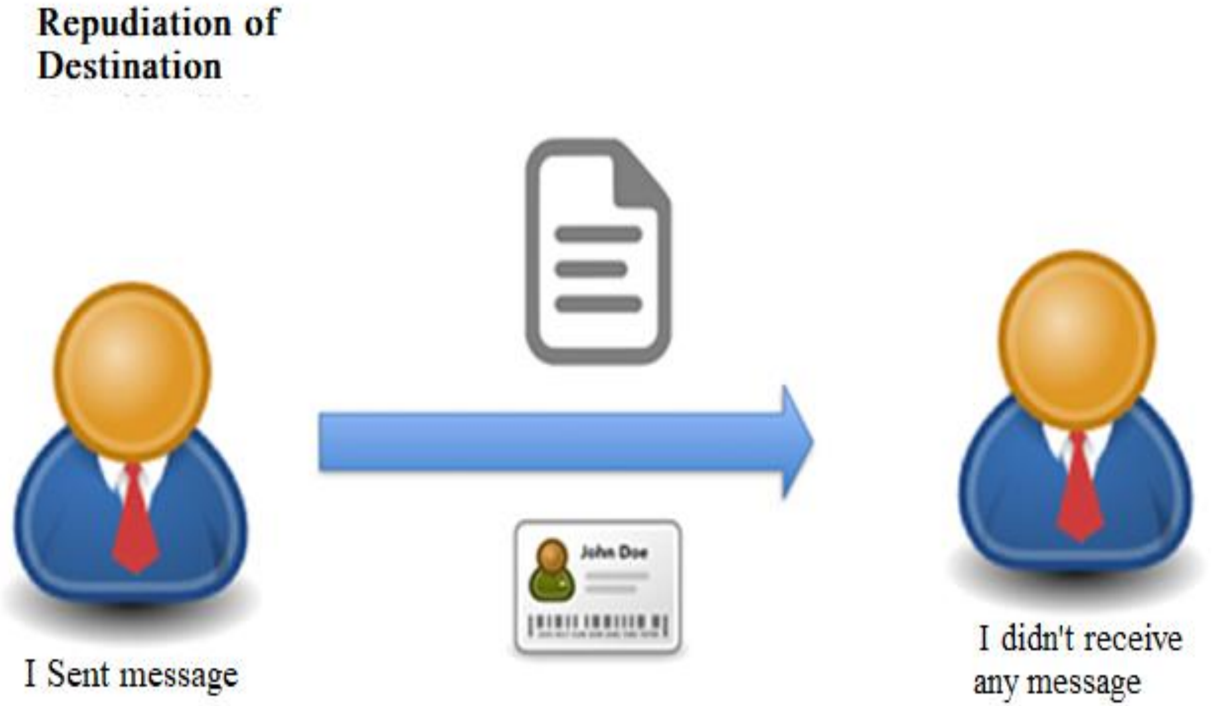


Repudiation
of Origin

Bank

I didn’t send
that transfer

Destination non-repudiation



Security Mechanisms

Encipherment

Data Integrity

Digital Signature

Authentication Exchange

Traffic Padding

Access Control

Notarization

Routing Control

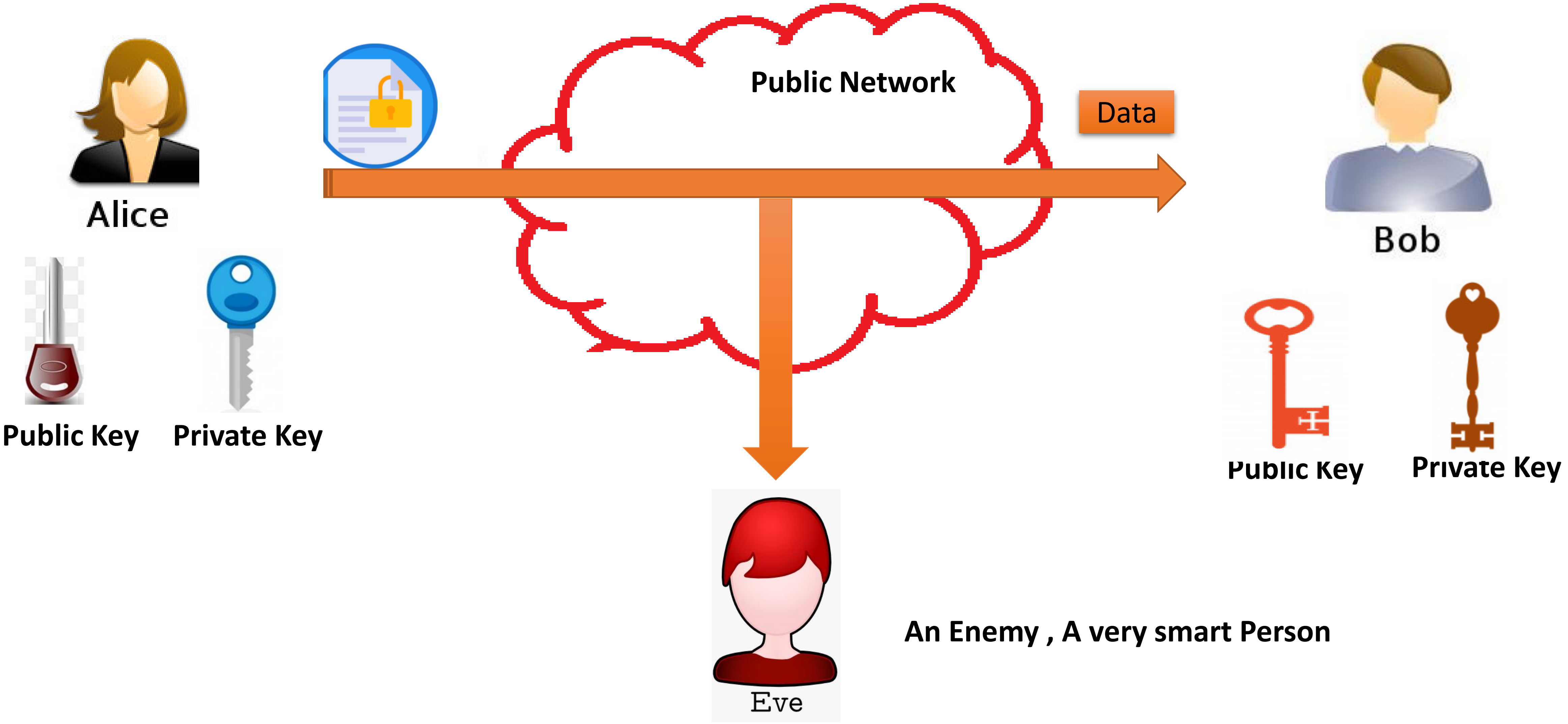
Encipherment

- Encipherment is the process of translating plaintext into ciphertext.

The two main types of Encryption are:

- **Asymmetric encryption**
- **Symmetric encryption**

Encipherment - Asymmetric encryption



Alice

Public Key

Private Key

Public Network

Data

Bob

Public Key

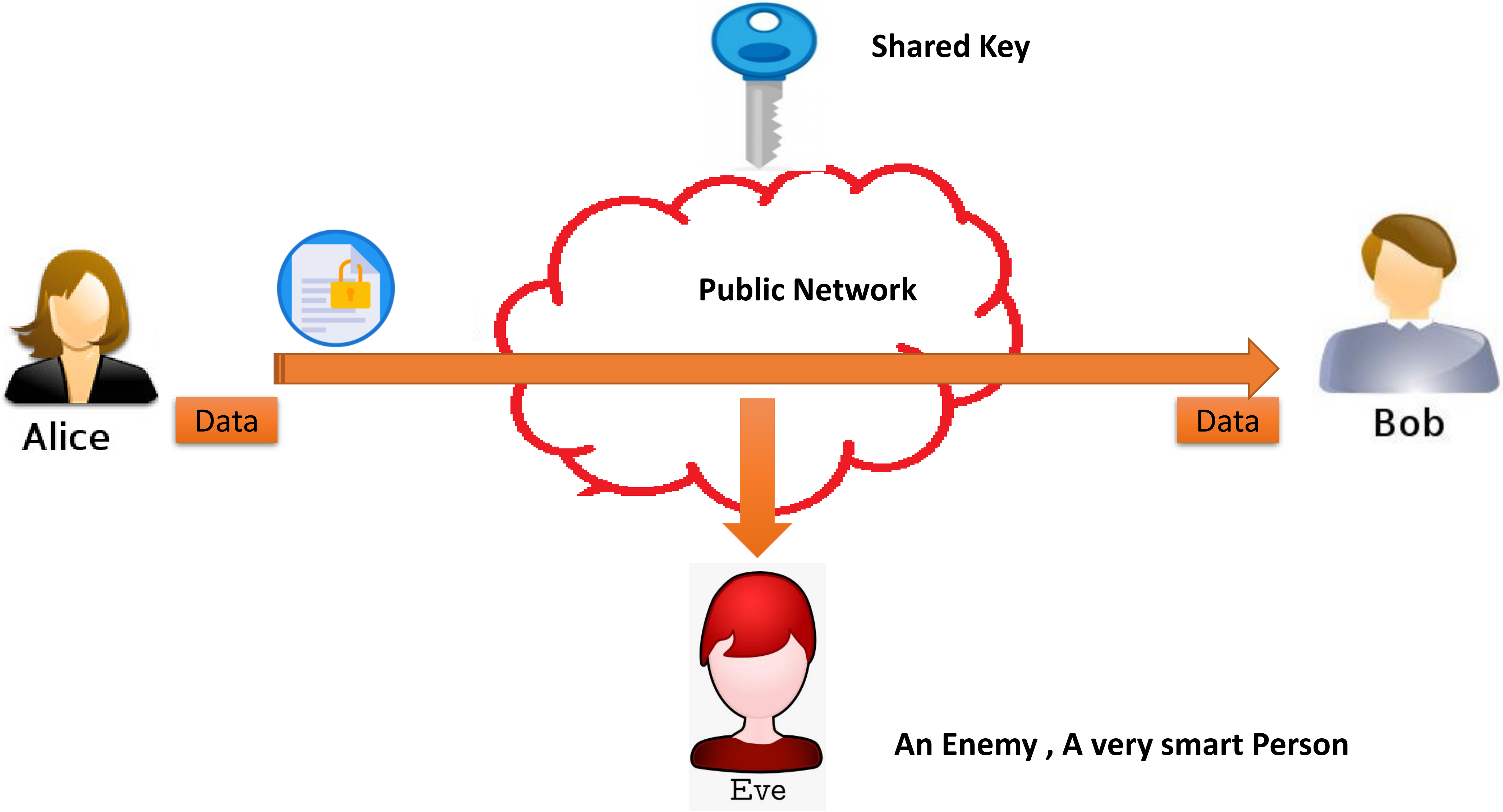
Private Key

Eve

An Enemy , A very smart Person

Alice, Bob, Eve Framework

Encipherment – Symmetric encryption



Alice, Bob, Eve Framework

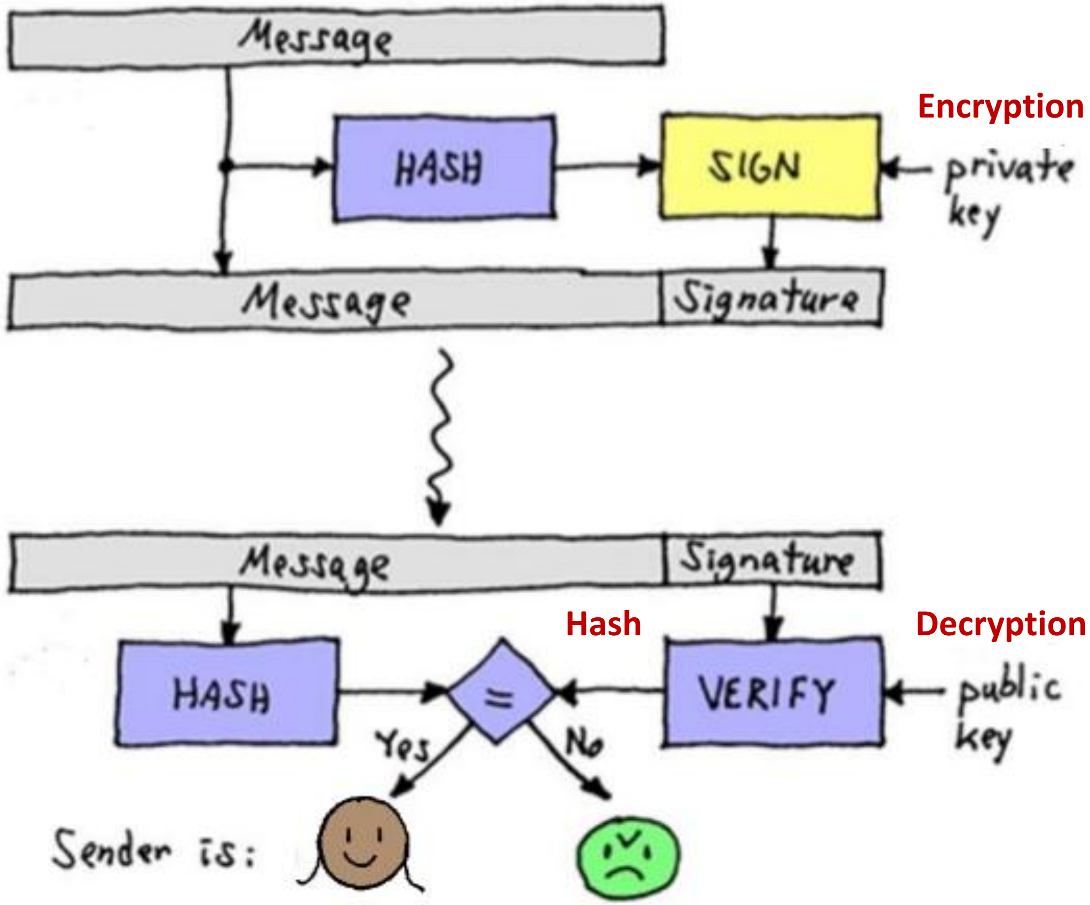
Data Integrity

Assurance that data received are exactly as sent by an authorized sender i.e. no modification, insertion, deletion or replay.

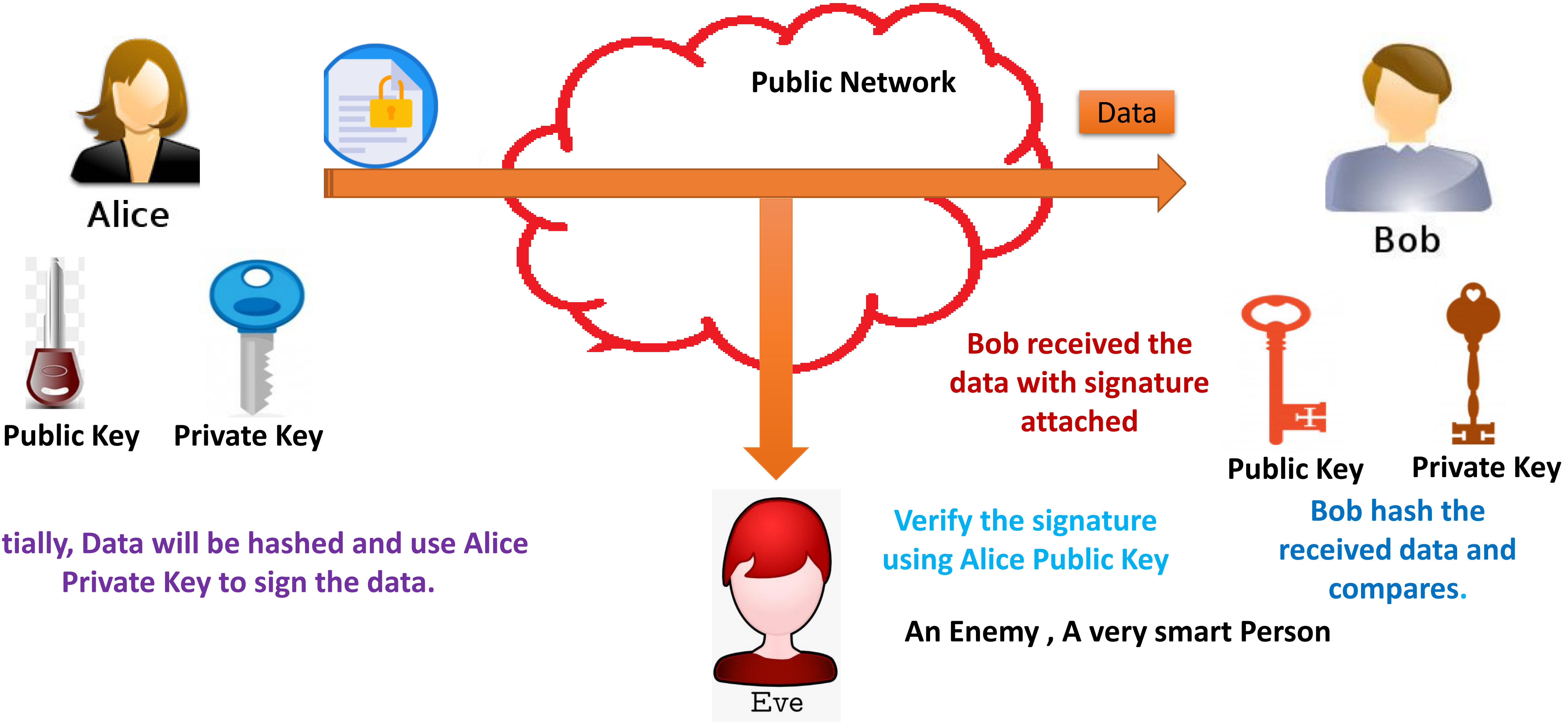
PRACTICAL NETWORKING .NET
Sender
Receiver

Digital Signature

- **Digital signatures** are the public-key primitives.
- **Message authentication**. It proves source authentication (Assures recipient that the message is from the source)
- **Data Integrity.** It provides integrity of the data.
- Protect against intruder.



Digital Signature



Initially, Data will be hashed and use Alice Private Key to sign the data.

Bob received the data with signature attached

Verify the signature using Alice Public Key

Bob hash the received data and compares.

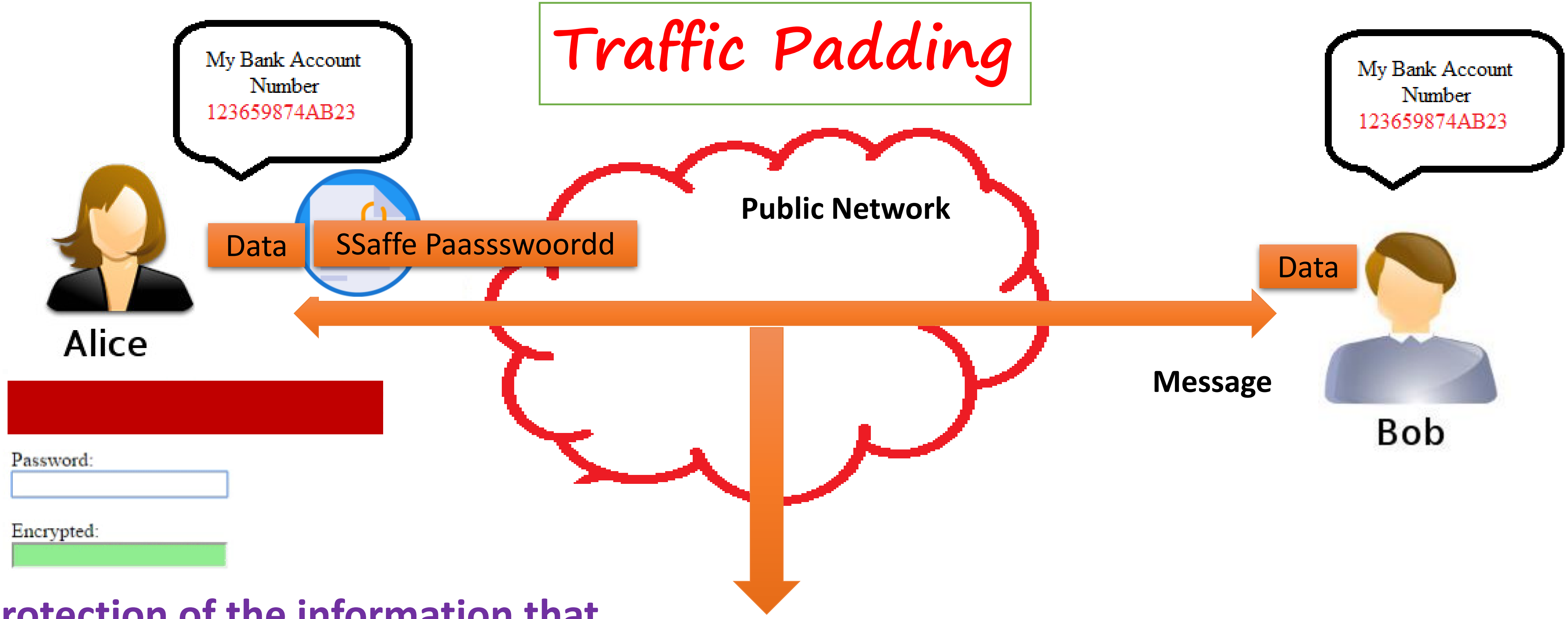
An Enemy , A very smart Person

Alice, Bob, Eve Framework

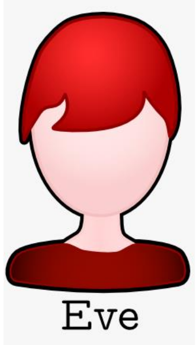
Authentication Exchange

- A mechanism intended to ensure the identity of an entity by means of information exchange

Traffic Padding



The protection of the information that might be derived from observation of traffic flows.



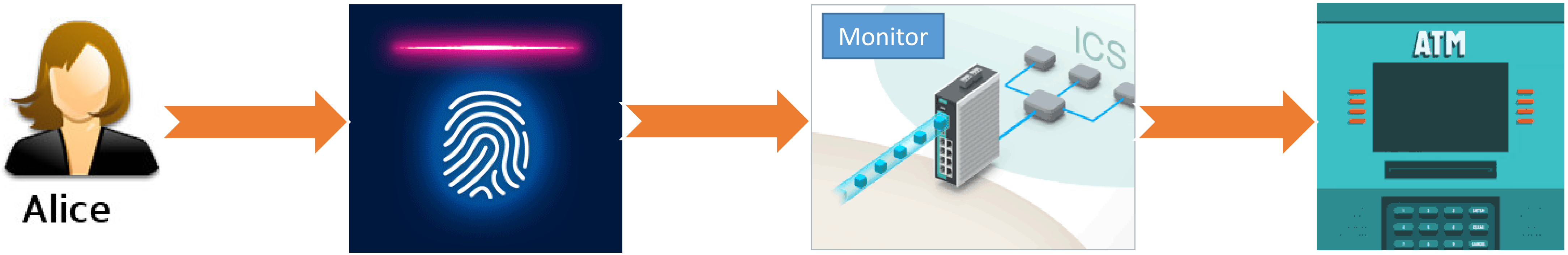
An Enemy , A very smart Person

Data protected from Eve

Alice, Bob, Eve Framework

Access Control

The prevention of unauthorized use of a resource (i.e. this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).



Access Request

Guard

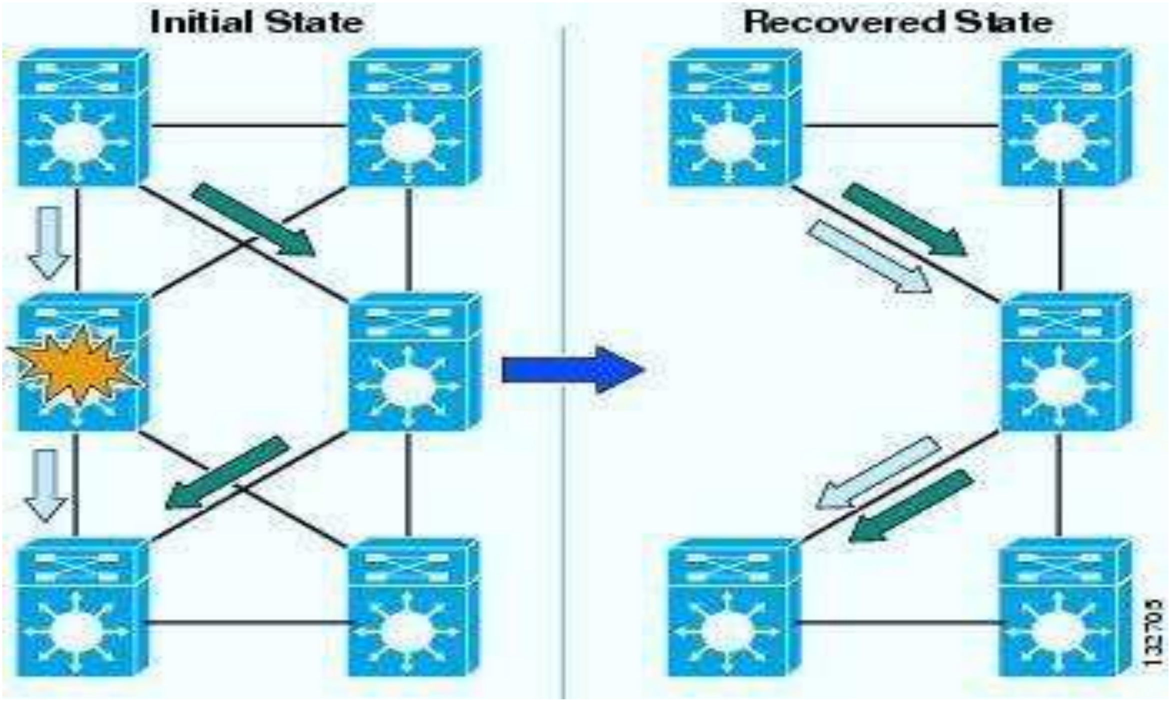
Resources

Notarization

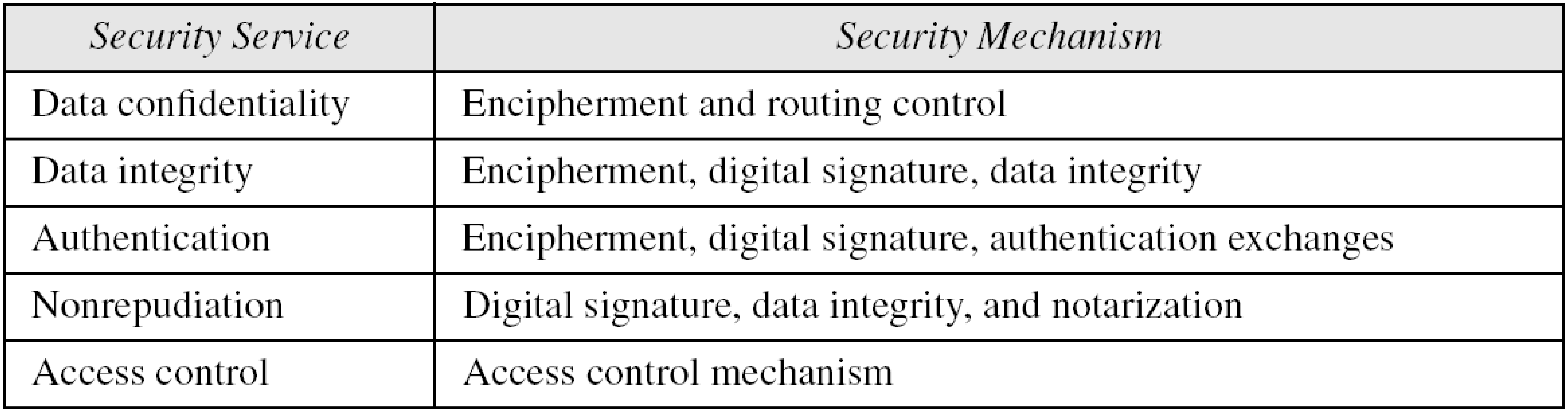
- The use of trusted third party to assure certain properties of a data exchange.
- The receiver involved a third party to store the sender request in order to prevent the sender from later denying that he has not made such request

Routing Control

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

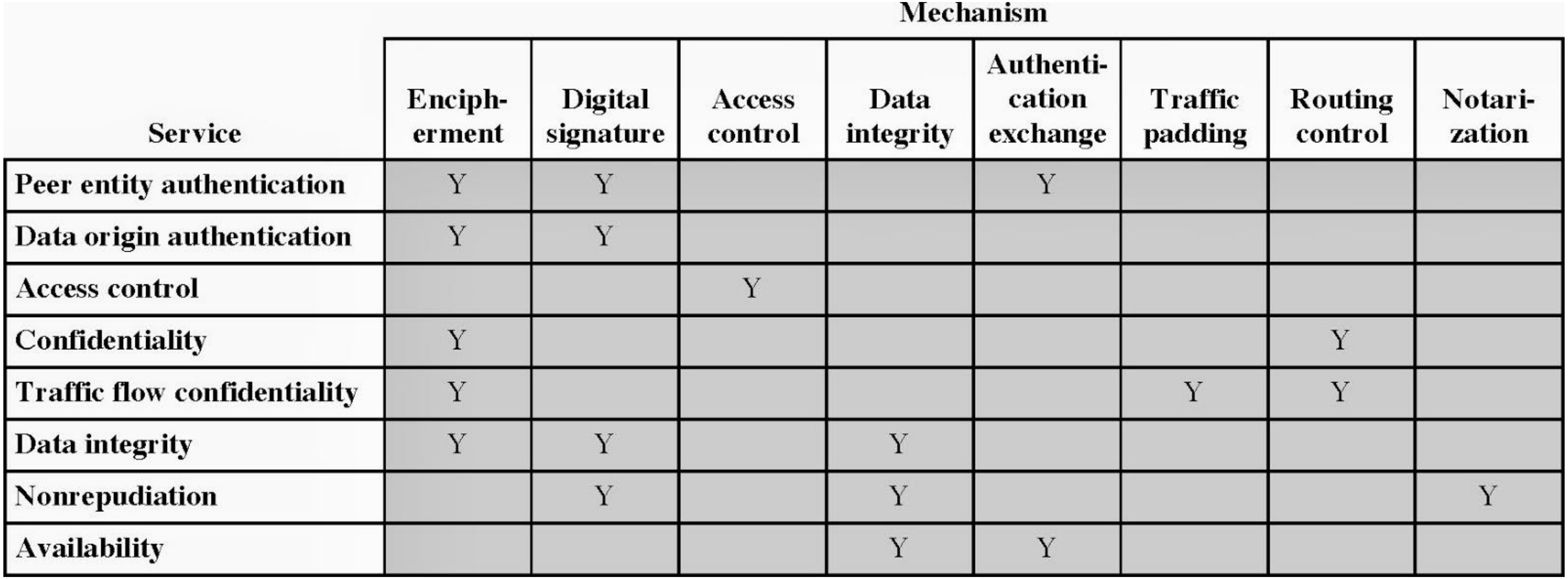


Relationship between security services and mechanisms



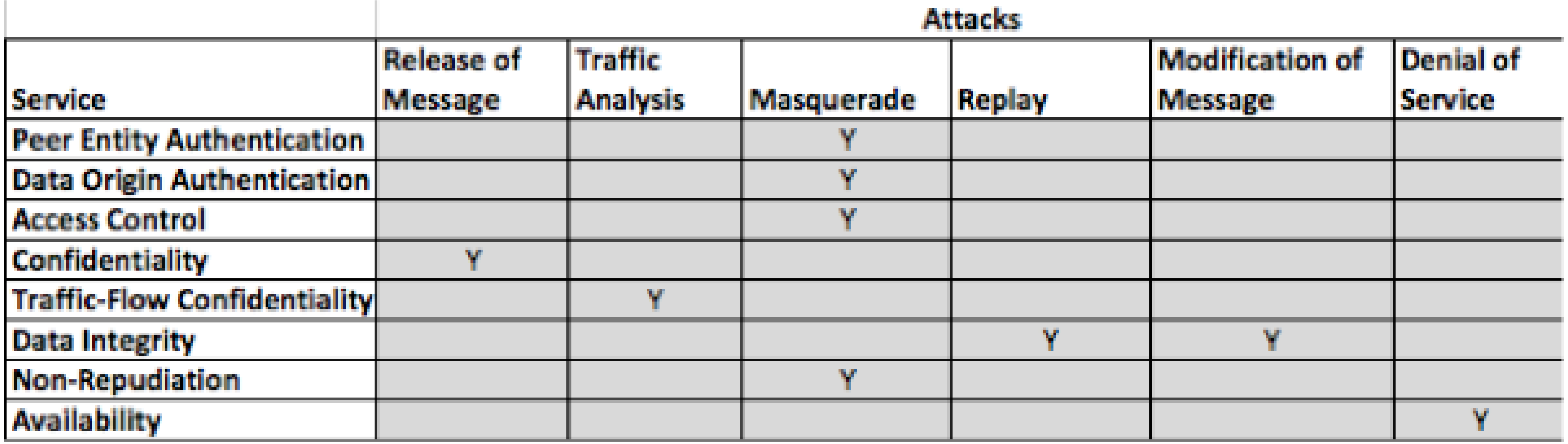
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Relationship between security services and mechanisms



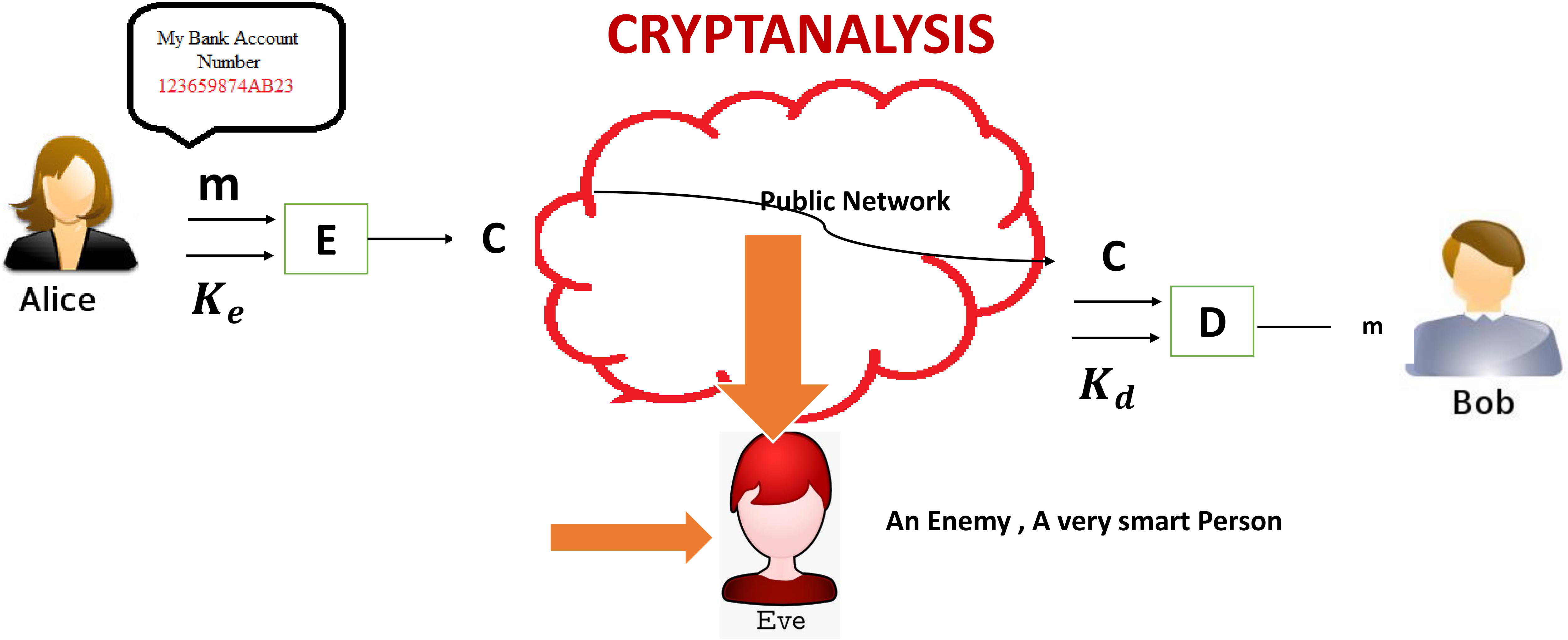
	Mechanism							
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Relationship between security services and Attacks



	Attacks					
Service	Release of Message	Traffic Analysis	Masquerade	Replay	Modification of Message	Denial of Service
Peer Entity Authentication			Y			
Data Origin Authentication			Y			
Access Control			Y			
Confidentiality	Y					
Traffic-Flow Confidentiality		Y				
Data Integrity				Y	Y	
Non-Repudiation			Y			
Availability						Y

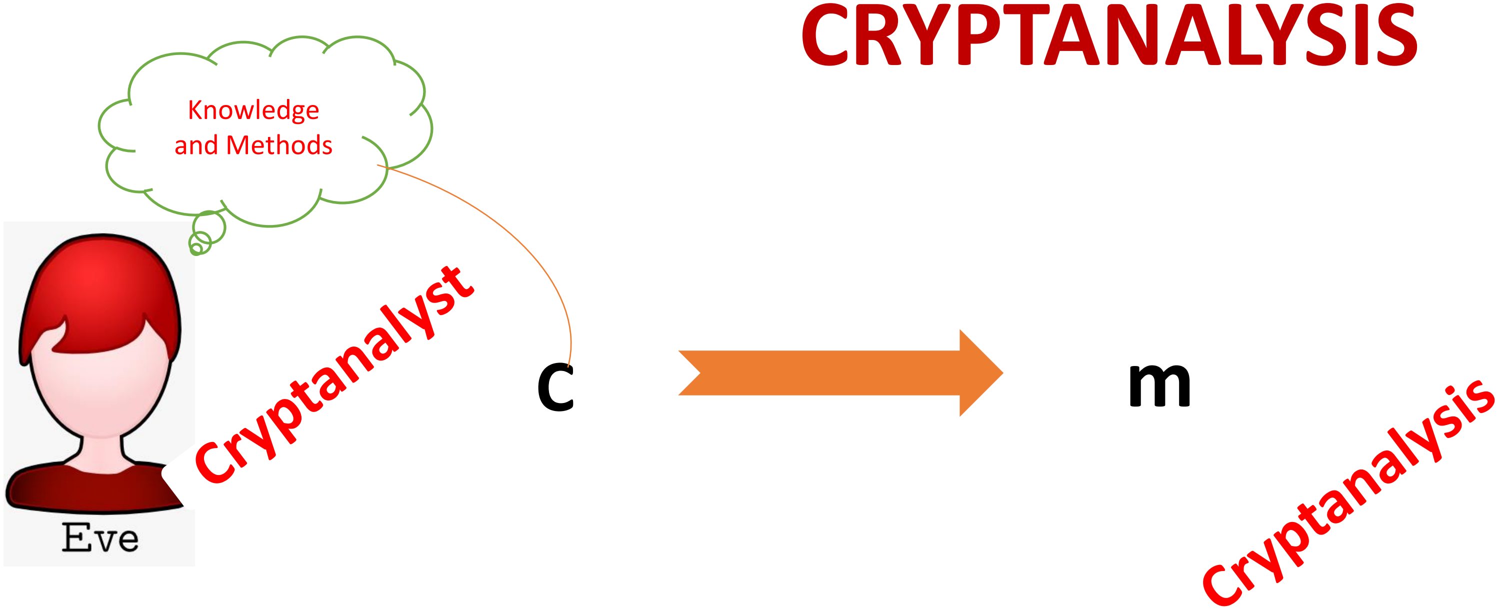
CRYPTANALYSIS



An Enemy , A very smart Person

The process of trying to break any cipher text message to obtain the original plain text message itself is called as Cryptanalysis, and the person attempting a cryptanalysis is called a cryptanalyst

CRYPTANALYSIS



Knowledge and Methods

Eve

Cryptanalyst

c

m

Cryptanalysis

An Attacker , A very smart Person

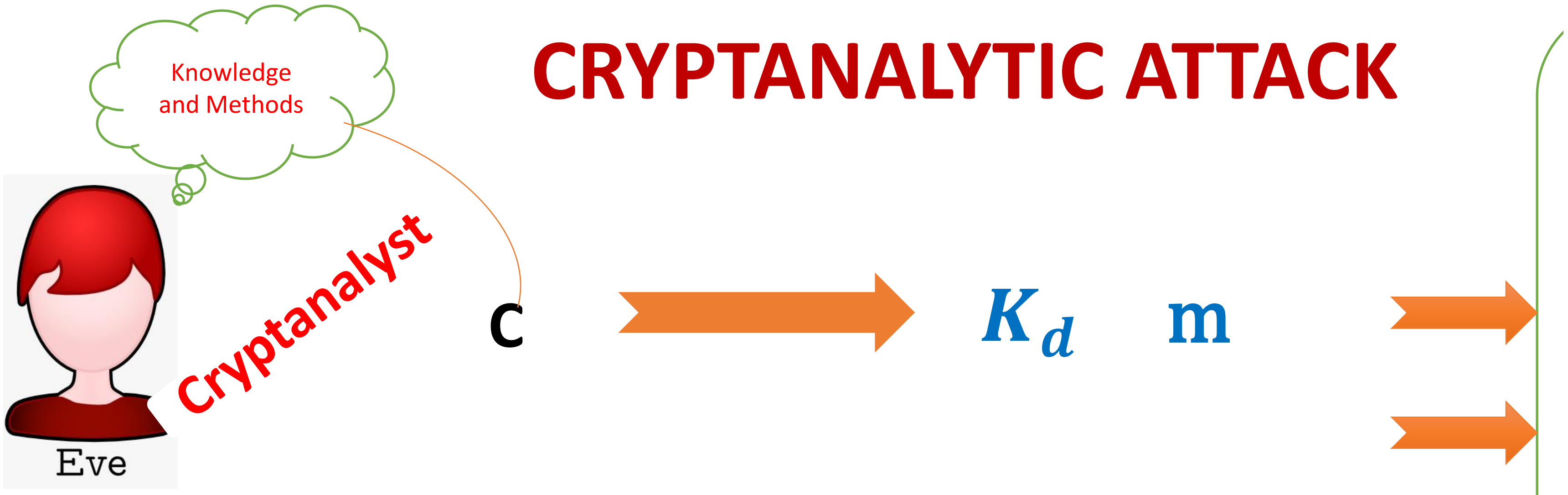
The process of trying to **break** any **cipher text** message to obtain the original **plain text** message itself is called as **Cryptanalysis**, and the person attempting a cryptanalysis is called a **cryptanalyst**

CRYPTANALYTIC ATTACKS

- Based on the amount of **information known** to Cryptanalyst, apply various types of cryptanalytic attacks. Few of them are:

1. **Ciphertext Only**
2. **Known plaintext**
3. **Chosen plaintext**
4. **Chosen Ciphertext**

CIPHERTEXT ONLY - CRYPTANALYTIC ATTACK



An Attacker , A very smart Person

Crypto System

m : Plain Text

C : Cipher Text

E: Encryption Algorithm

D: Decryption Algorithm

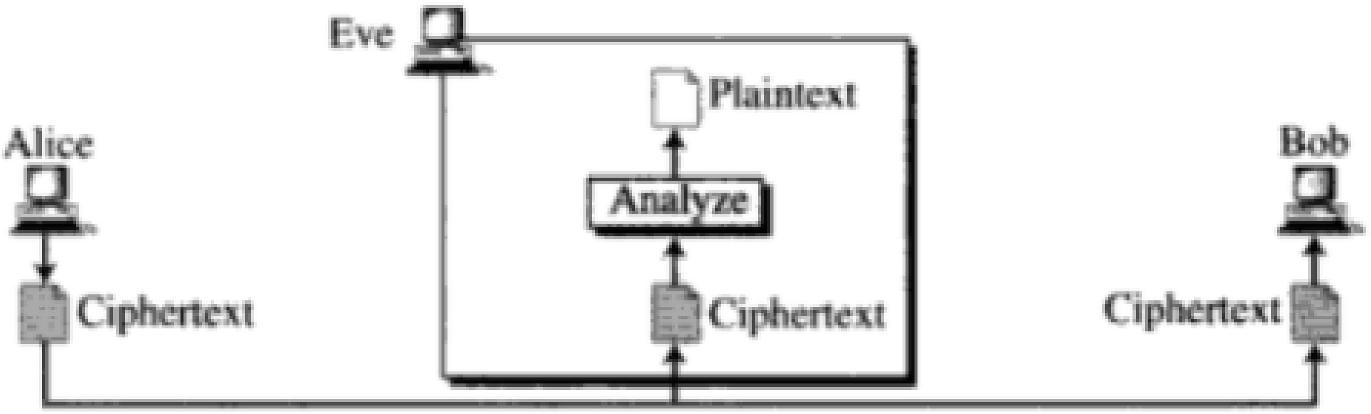
K_e:Encryption Key

K_d: Decryption Key

Cipher Text Only

A copy of cipher text is known to the cryptanalyst.

CIPHERTEXT ONLY - CRYPTANALYTIC ATTACKS



Methods used in **Ciphertext-Only attack :**

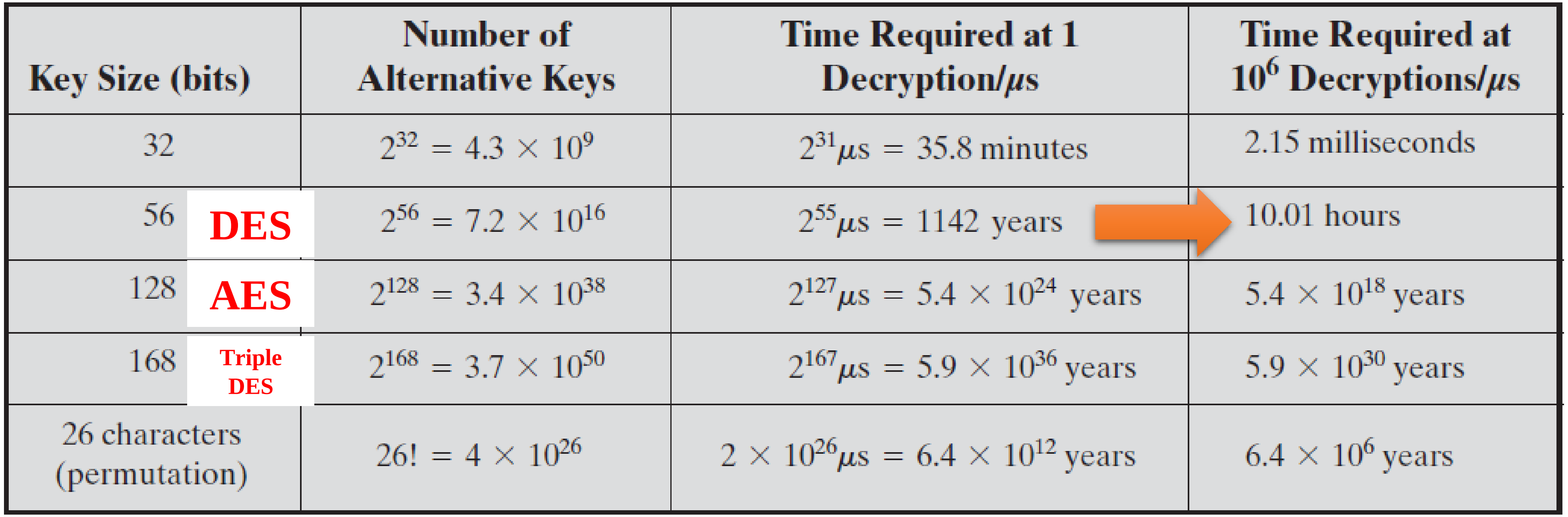
1. **Brute force Attack**
2. **Statistical Attack**

CIPHERTEXT ONLY - CRYPTANALYTIC ATTACK

Brute force Attack

- The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
- If the key space is very large, brute force attack becomes impractical.

CIPHERTEXT ONLY - CRYPTANALYTIC ATTACKS



Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56 DES	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128 AES	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168 Triple DES	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

considers the results for a system that can process 1 million keys per microsecond.
As you can see,
at this performance level, DES can no longer be considered computationally secure

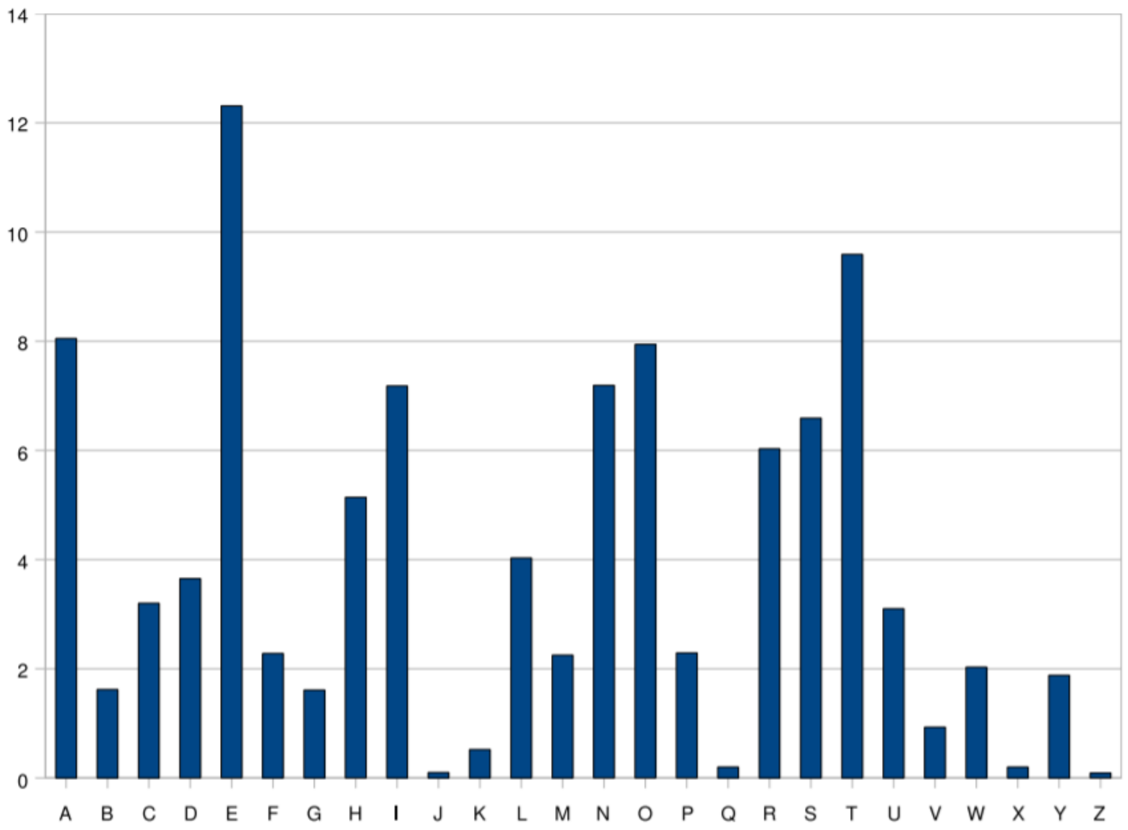
CIPHERTEXT ONLY - CRYPTANALYTIC ATTACK

Statistical Attack

- Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it.
- To use this approach, the opponent must have some general idea of the type of plaintext that is concealed, such as English or French text, an EXE file, a Java source listing, an accounting file, and so on.

CIPHERTEXT ONLY - CRYPTANALYTIC ATTACK

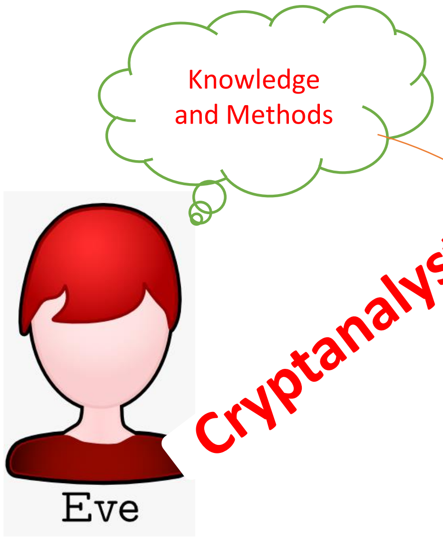
Relative frequency of the letters in English text



For Example: Letter E is the most frequently used letter in English text

Early to bed, and early to rise, makes a man healthy, wealthy and wise.

KNOWN PLAINTEXT - CRYPTANALYTIC ATTACK



Cryptanalyst

{m, c} → Key

An Attacker , A very smart Person

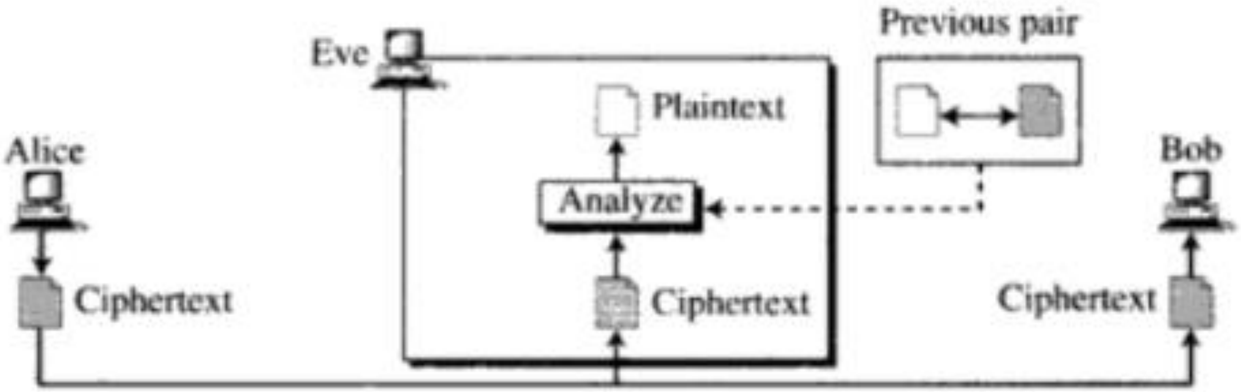
Crypto System

- m : Plain Text
- C : Cipher Text
- E: Encryption Algorithm
- D: Decryption Algorithm
- K_e:Encryption Key
- K_d: Decryption Key

Known plain Text

The cryptanalyst has a copy of the cipher text and the corresponding plaintext

KNOWN PLAINTEXT - CRYPTANALYTIC ATTACK



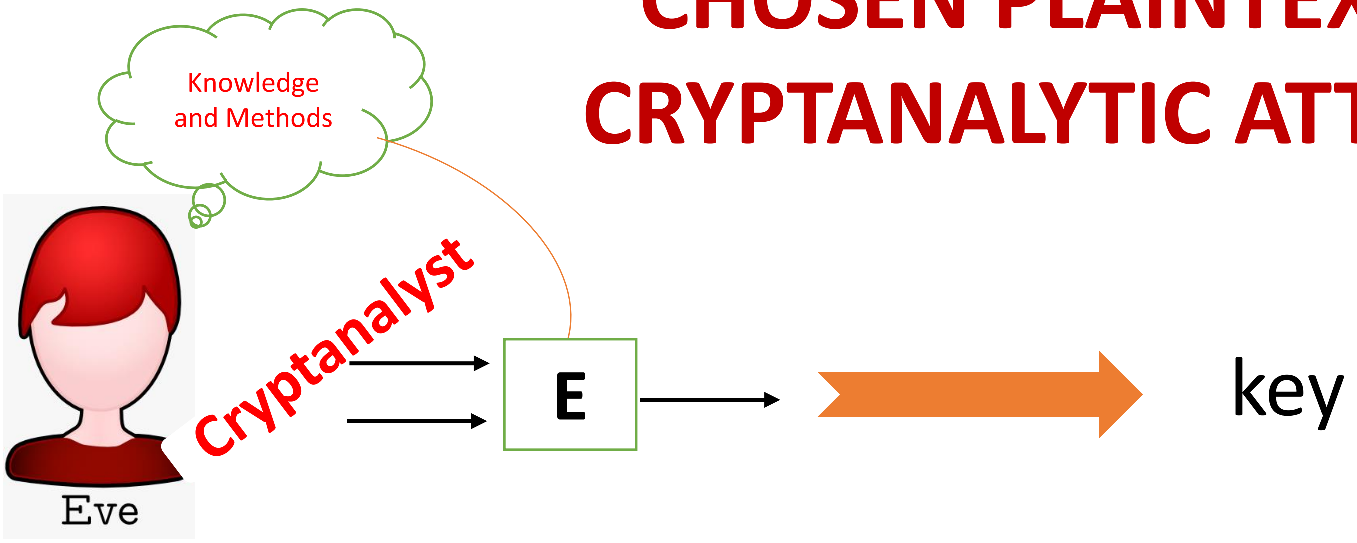
- **The plaintext/ciphertext pairs have been collected earlier.**

For example:

Alice has sent a secret message to Bob, but he/she has later made the contents of the message public.

- With this knowledge, the analyst may be able to deduce the key.
- If attack succeeds in deducing the key, the effect is **catastrophic**.
- All future and past messages encrypted with that key are **compromised**.

CHOSEN PLAINTEXT - CRYPTANALYTIC ATTACK



An Attacker , A very smart Person

Crypto System

m : Plain Text

C : Cipher Text

E: Encryption Algorithm

D: Decryption Algorithm

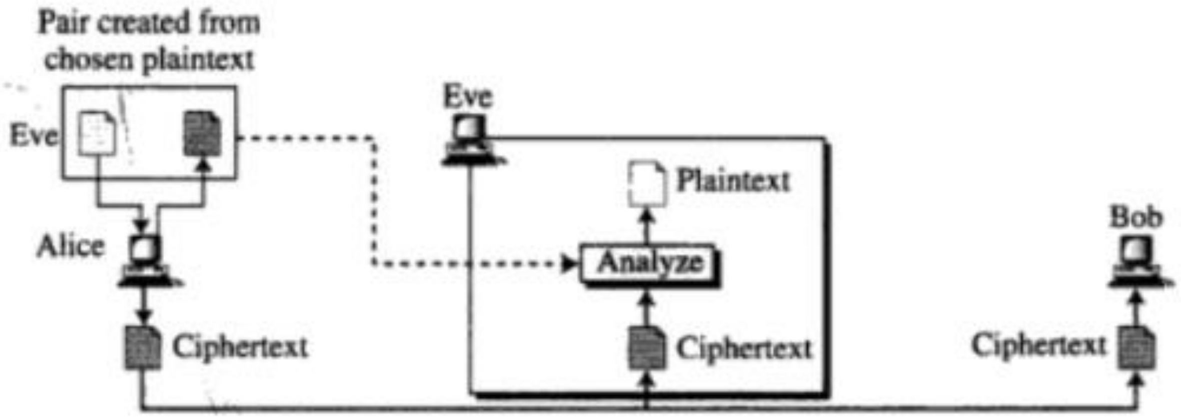
K_e:Encryption Key

K_d: Decryption Key

Chosen Plain Text

The cryptanalysts gains temporary access to the encryption machine

CHOSEN PLAINTEXT - CRYPTANALYTIC ATTACK

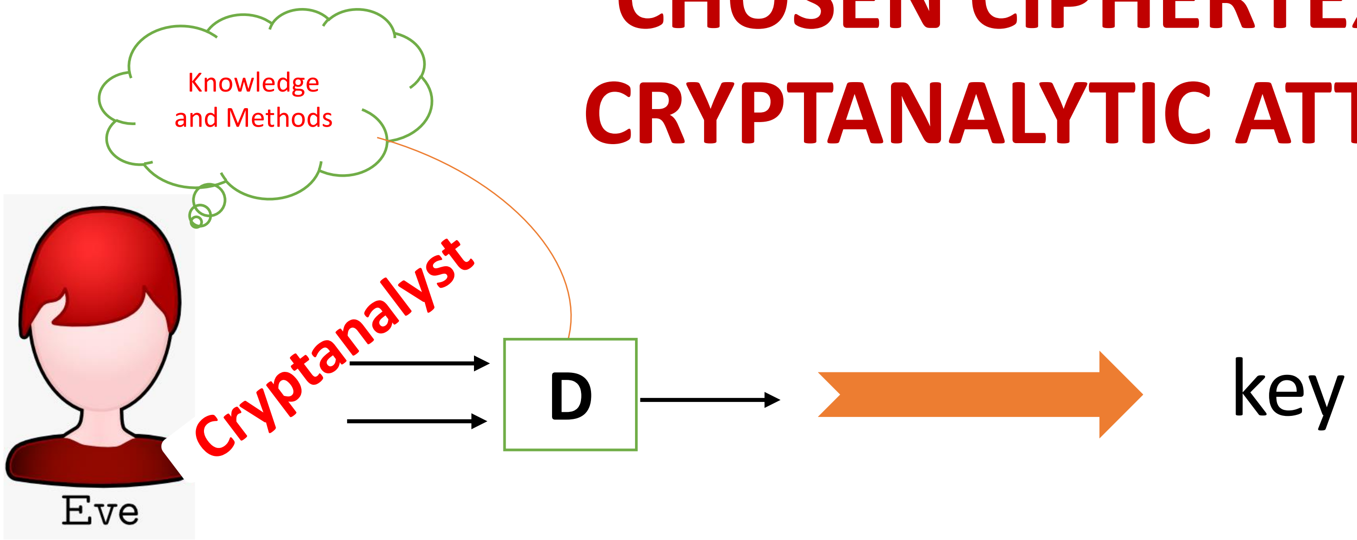


- Method used in Chosen Plaintext attack is Differential Cryptanalysis

For example

If Eve has access to Alice’s computer, Eve can choose some plaintext and intercept ciphertext.

CHOSEN CIPHERTEXT - CRYPTANALYTIC ATTACK



An Attacker , A very smart Person

Crypto System

m : Plain Text

C : Cipher Text

E: Encryption Algorithm

D: Decryption Algorithm

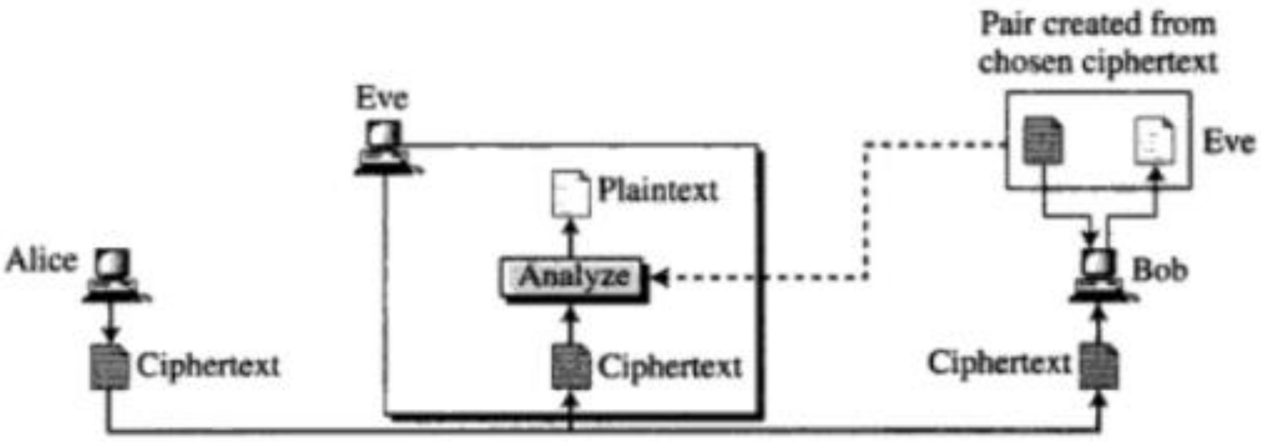
K_e:Encryption Key

K_d: Decryption Key

Chosen Cipher Text

The cryptanalysts gains temporary access to the decryption machine

CHOSEN CIPHERTEXT - CRYPTANALYTIC ATTACK



- Method used in Chosen Ciphertext attack is Differential Cryptanalysis

For example

If Eve has access to Bob's computer, Eve can chooses some ciphertext and decrypt it to form a ciphertext/plaintext pair.

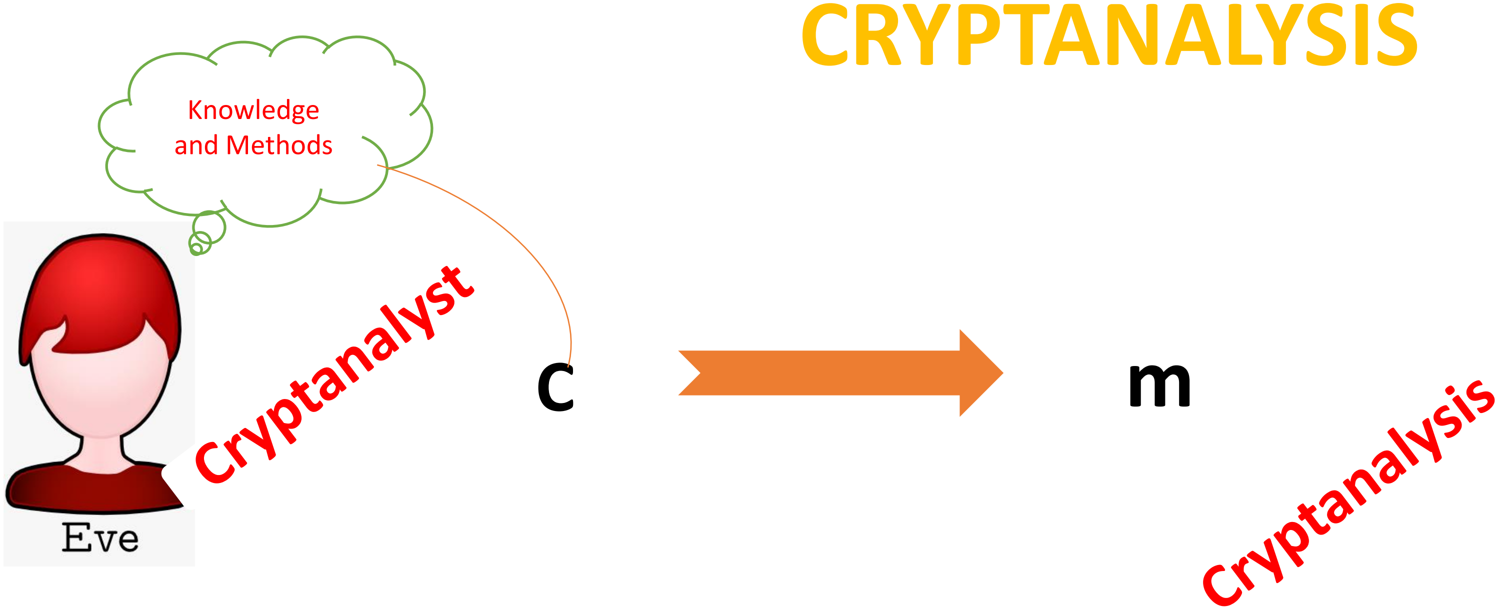
CRYPTANALYSIS

- There is no encryption algorithm that is unconditionally secure except one time pad.
- **But encryption algorithm can strive if meets one or both of the below criteria:**

1. **The cost of breaking the cipher text exceeds the value of encrypted information.**
2. **The time required to break the cipher exceeds the useful lifetime of the information.**

These encryption algorithm said to be computationally secure

CRYPTANALYSIS



Knowledge and Methods

Cryptanalyst

c → m

Cryptanalysis

An Attacker , A very smart Person

The art or process of deciphering coded messages without being told the key

A