What is Cryptography

- Cryptography
  - In a narrow sense
    - Mangling information into apparent unintelligibility
    - Allowing a secret method of un-mangling
  - In a broader sense
    - Mathematical techniques related to information security
    - About secure communication in the presence of adversaries
- Cryptanalysis
  - The study of methods for obtaining the meaning of encrypted information without accessing the secret information
- Cryptology
  - Cryptography + cryptanalysis

Security Attacks

- Passive attacks
  - Obtain message contents
  - Monitoring traffic flows

- Active attacks
  - Masquerade of one entity as some other
  - Replay previous messages
  - Modify messages in transmit
  - Add, delete messages
  - Denial of service

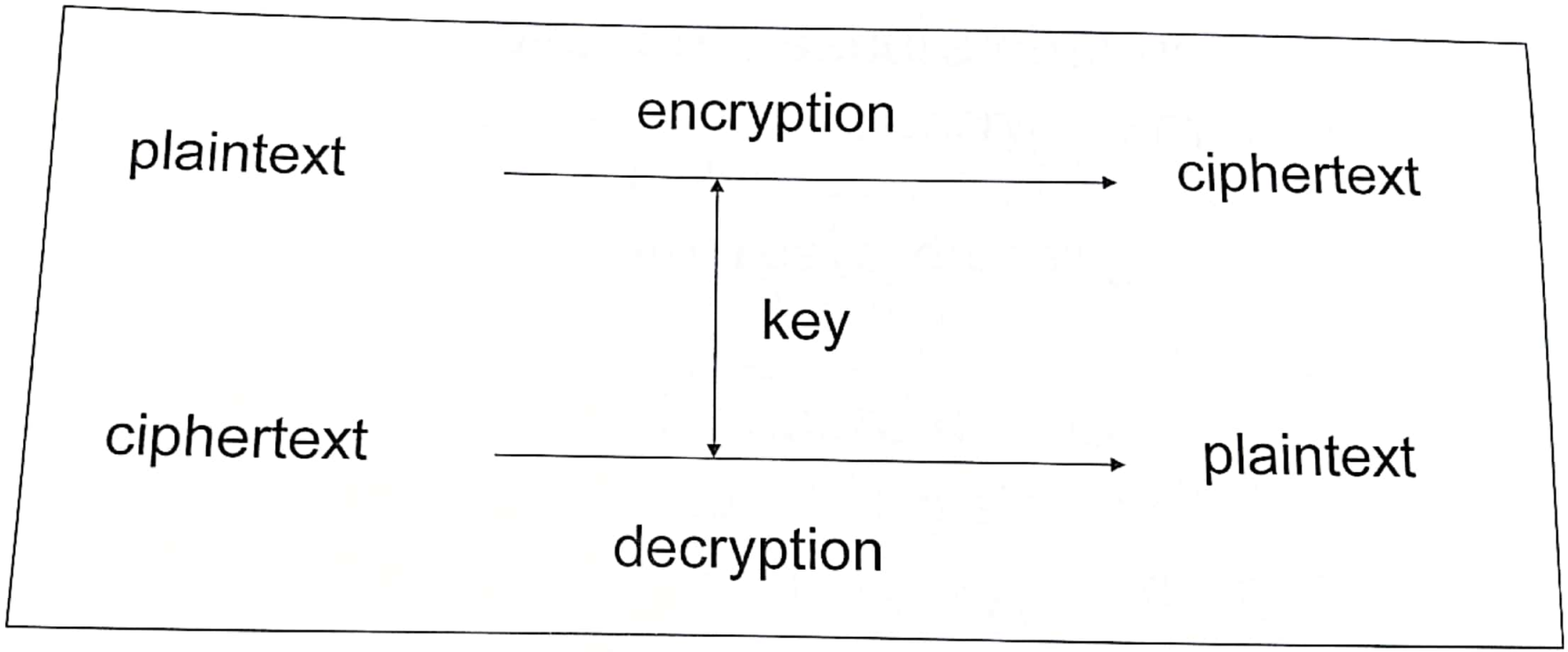
Objectives of Information Security

- Confidentiality (secrecy)
  - Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication
  - Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity
  - The content of their communication is not altered, either maliciously or by accident, in transmission.
- Availability
  - Timely accessibility of data to authorized entities.

Types of Cryptographic Functions

- Secret key functions
- Public key functions
- Hash functions

Secret Key Cryptography



- *Using a single key for encryption/decryption.*
- *The plaintext and the ciphertext having the same size.*
- *Also called symmetric key cryptography*

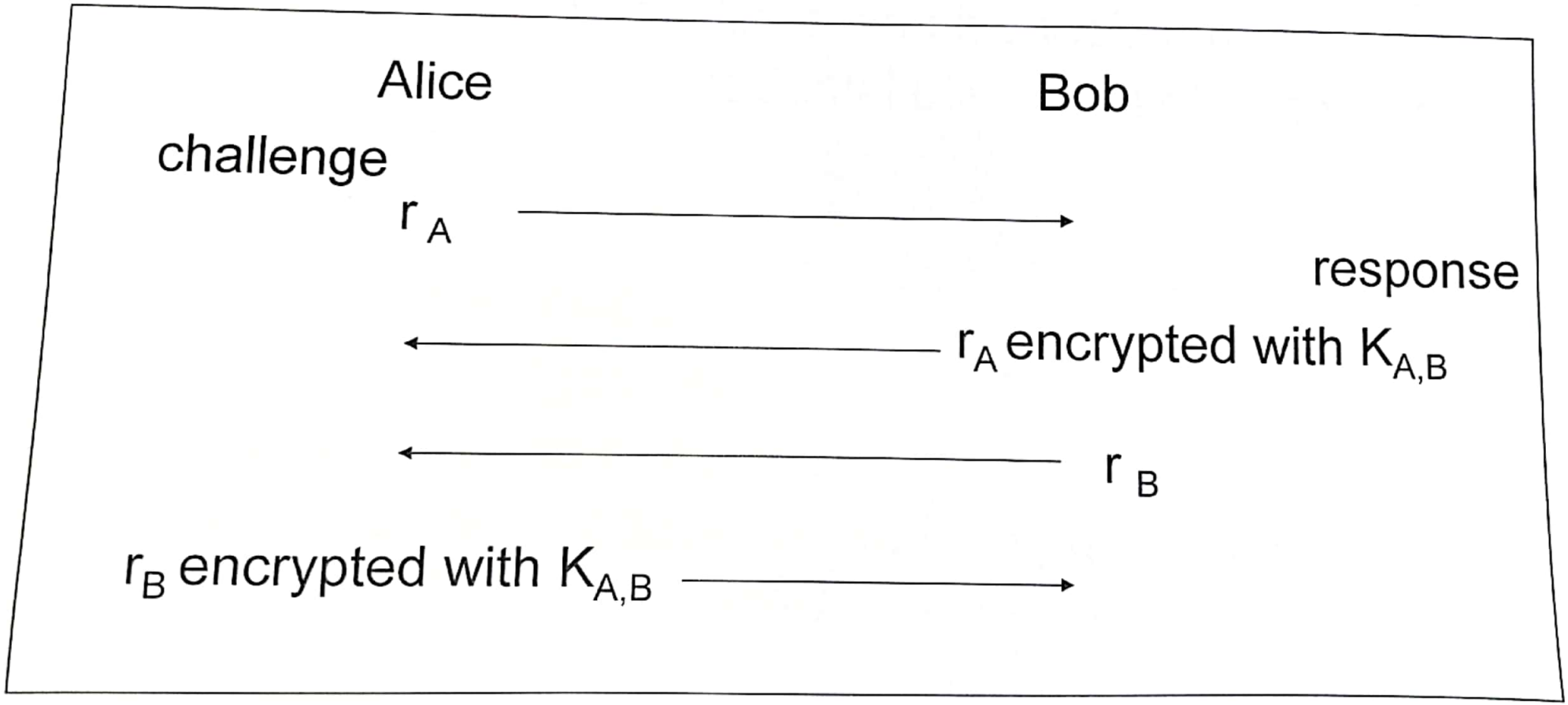
SKC: Security Uses

- Transmitting over an insecure channel
  - The transmitted message is encrypted by the sender and can be decrypted by the receiver, with the same key
  - Prevent attackers from eavesdropping

- Secure storage on insecure media
  - Data is encrypted before being stored somewhere
  - Only the entities knowing the key can decrypt it

SKC: Security Uses

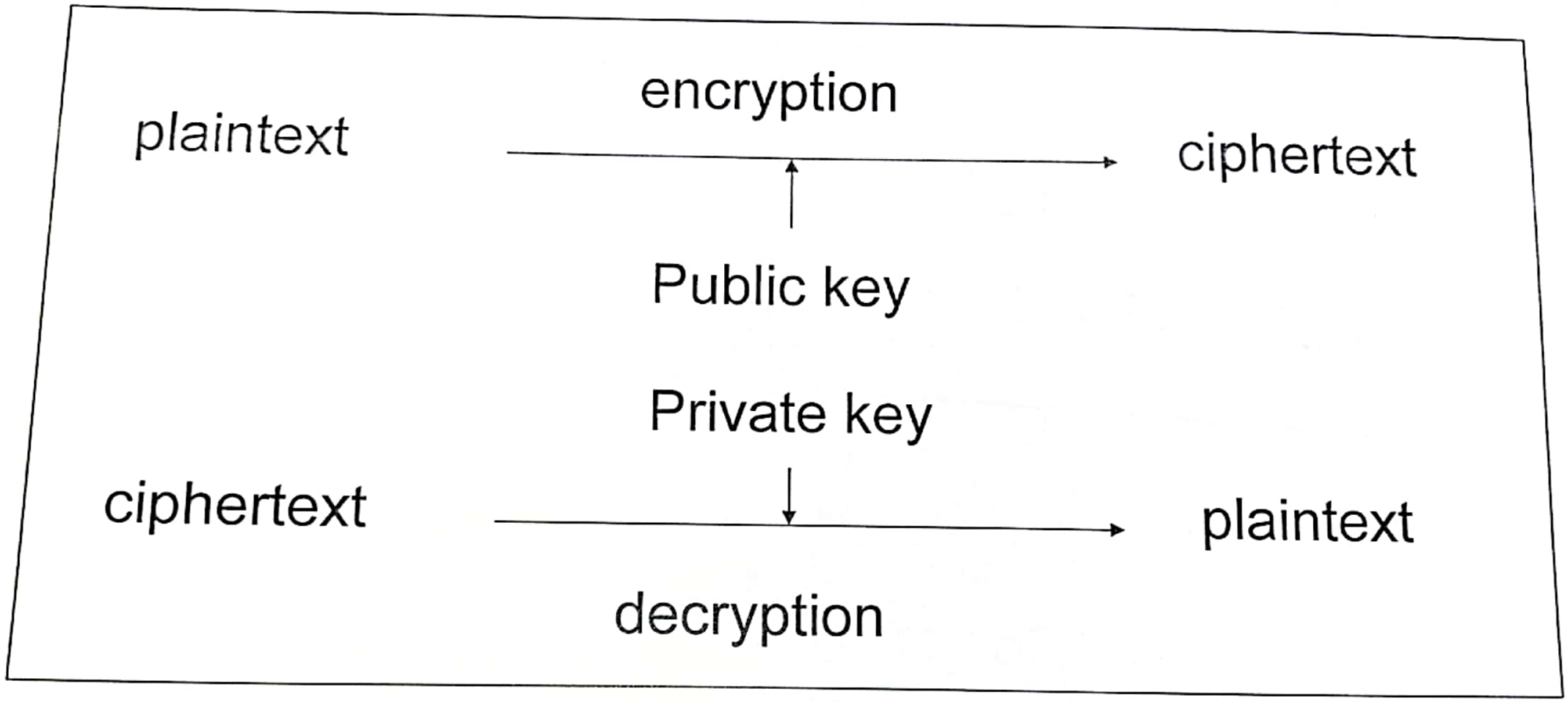
- Authentication
  - Strong authentication: proving knowledge of a secret without revealing it.



SKC: Security Uses

- Integrity Check
  - Noncryptographic checksum
    - Using a well-known algorithm to map a message (of arbitrary length) to a fixed-length checksum
    - Protecting against accidental corruption of a message
    - Example: CRC
  - Cryptographic checksum
    - A well-know algorithm
    - Given a key and a message
    - The algorithm produces a fixed-length message authentication code (MAC) that is sent with the message

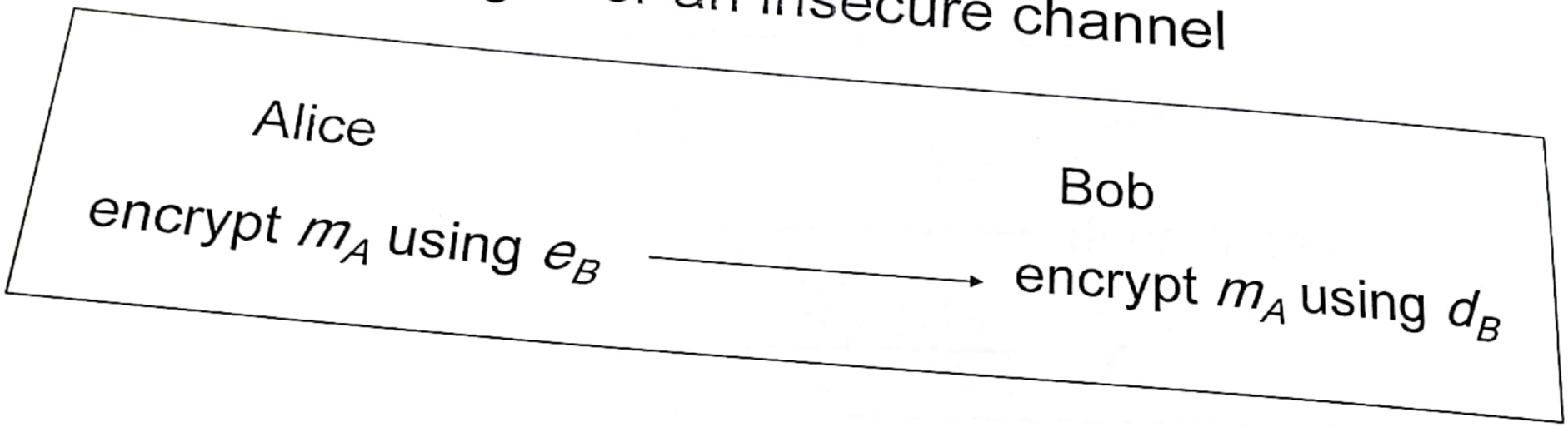
Public Key Cryptography



- *Each individual has two keys*
  - *a private key* (d): need not be reveal to anyone
  - *a public key* (e): preferably known to the entire world
- *Public key crypto is also called asymmetric crypto.*

PKC: Security Uses

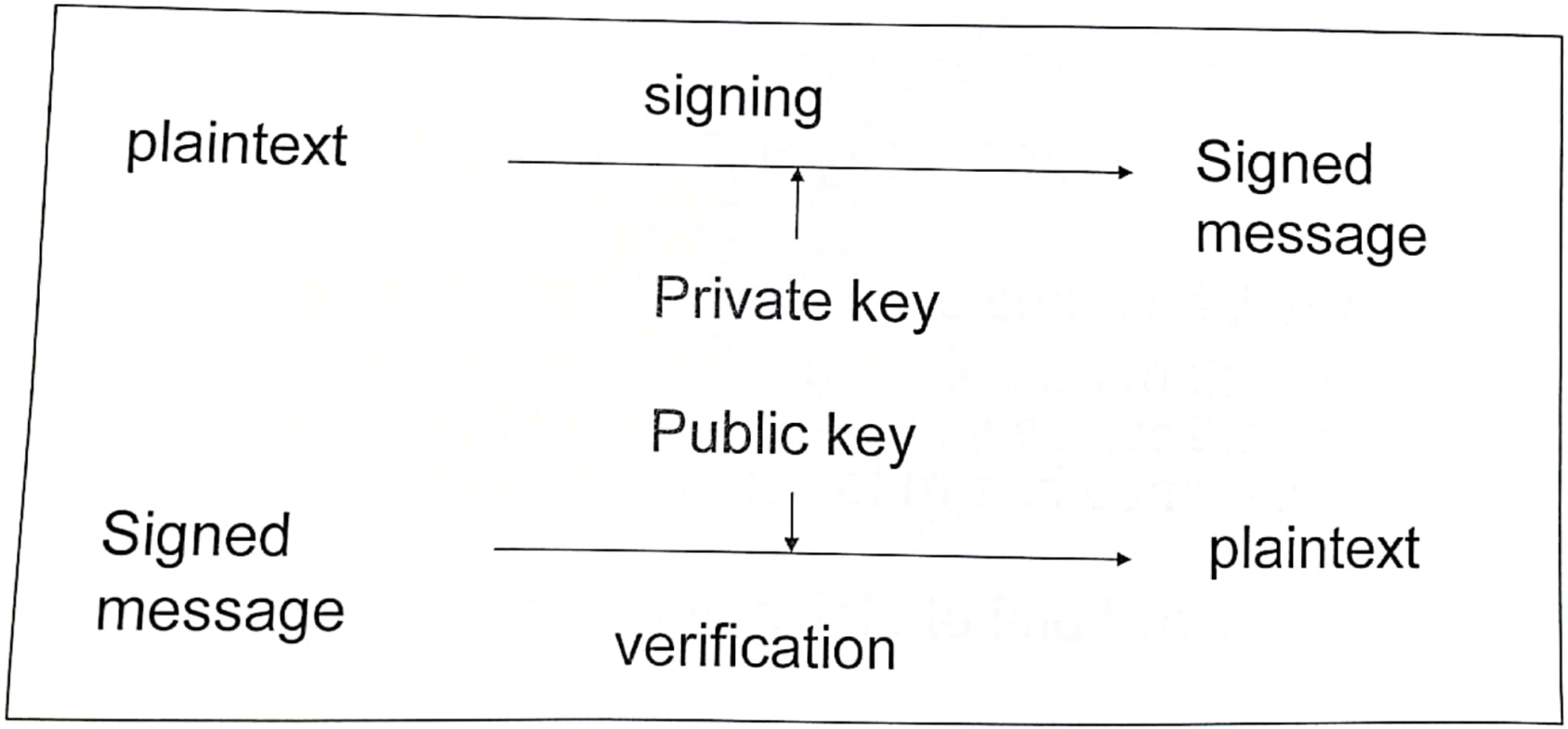
- Transmitting over an insecure channel



- Secure storage on insecure media
  - Data is encrypted with the public key of the source, before being stored somewhere
  - Nobody else can decrypt it (not knowing the private key of the data source)

PKC: Security Uses

- Digital Signatures
  - Proving that a message is generated by a particular individual
  - Non-repudiation: the signing individual can not be denied, because only him/her knows the private key.



Hash Functions

- Cryptographic hash function
  - A mathematical transformation that takes a message of arbitrary length and computes it a fixed-length (short) number.

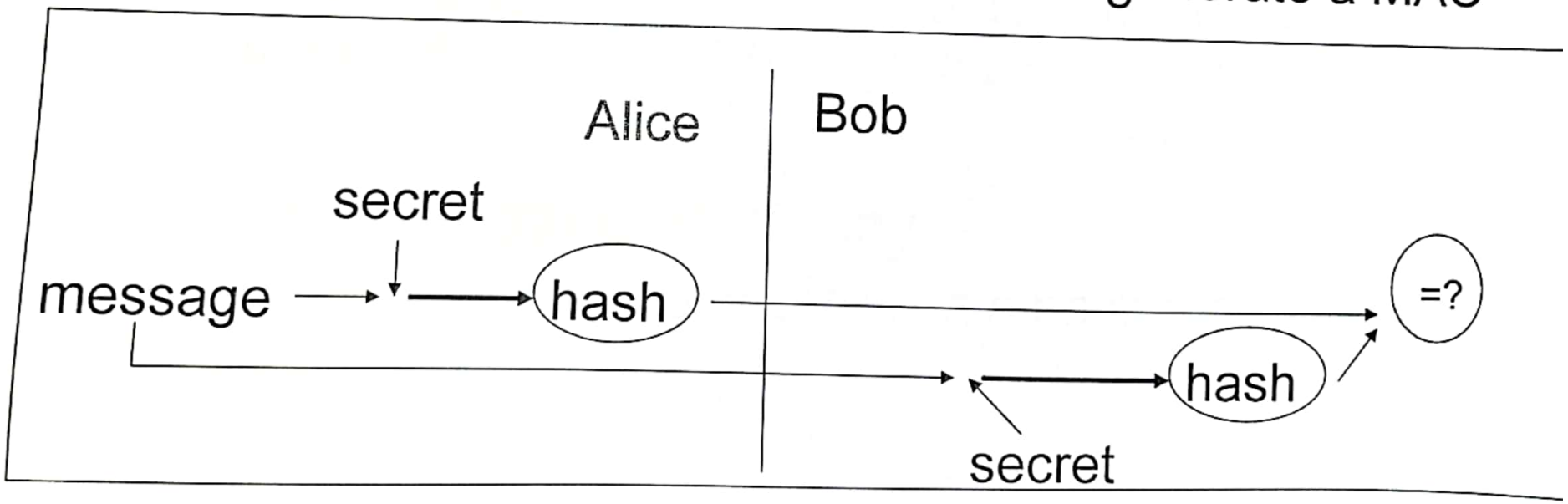
- Properties

  (Let the hash of a message *m* be *h(m)*)

  - For any *m*, it is relatively easy to compute *h(m)*
  - Given *h(m)*, there is no way to find an m that hashes to *h(m)* in a way that is substantially easier than going through all possible values of m and computing *h(m)* for each one.
  - It is computationally infeasible to find two values that hash to the same thing.

Hash Functions: Security Uses

- Password hashing
  - The system store a hash of the password (not the password itself)
  - When a password is supplied, it computes the password's hash and compares it with the stored value.
- Message integrity
  - Using cryptographic hash functions to generate a MAC



Hash Functions: Security Uses

- Message fingerprint
  - Save the message digest of the data on a tamper-proof backing store
  - Periodically re-compute the digest of the data to ensure it is not changed.

- Downline load security
  - Using a hash function to ensure a download program is not modified

- Improving signature efficiency
  - Compute a message digest (using a hash function) and sign that.

Attacks: Types

- Brute force search
  - Assume either know/recognize plaintext
  - Simply try every key

- Cryptoanalysis
  - Ciphertext only
    - With the ciphertext
    - Plaintext is recognizable
  - Known plaintext
    - <cipher, plaintext> pairs are known
  - Chosen plaintext
    - Select plaintext and obtain ciphertext to attack

Security Definition

- Unconditional Security
  - The system cannot be defeated, no matter how much power is available by the adversary.

- Computational security
  - The perceived level of computation required to defeat the system using the best known attack exceeds, by a comfortable margin, the computational resources of the hypothesized adversary.
  - e.g., given limited computing resources, it takes the age of universe to break cipher.

Security Definition

- Provable security
  - The difficulty of defeating the system can be shown to be essentially as difficult as solving a well-known and supposedly difficult problem (e.g., integer factorization)

- Ad hoc security
  - Claims of security generally remain questionable
  - Unforeseen attacks remain a threat

Secret Key Cryptographic Algorithms

- DES (Data Encryption Standard)
- 3DES (Triple DES)
- IDEA (International Data Encryption Algorithm)
- AES (Advanced Encryption Standard)

Glossary

LAN - Local Area Network.

WAN - Wide Area Network.

IOT - Internet of Things.

SDN - Software-Defined Networking.

VoIP - Voice over IP.

HTTP - Hypertext Transfer Protocol.

IP - Internet Protocol.

RTOS - Real Time Operating System.

ANSI - American National Standards Institute.

EMIE – Electromagnetic Interference.

SMS - Short Message Service.

SMSC - Short Message Service Center

HSDPA - High-Speed Downlink Packet Access

PPP - Point-to-Point Protocol

NTP - Network Time Protocol

NDMP - Network Data Management Protocol

HSM - Hierarchical Storage Management

AIC - Add-In Card

TCP/IP - Transmission Control Protocol/Internet Protocol.

HDDs - Hard Disk Drives

Assignment #2

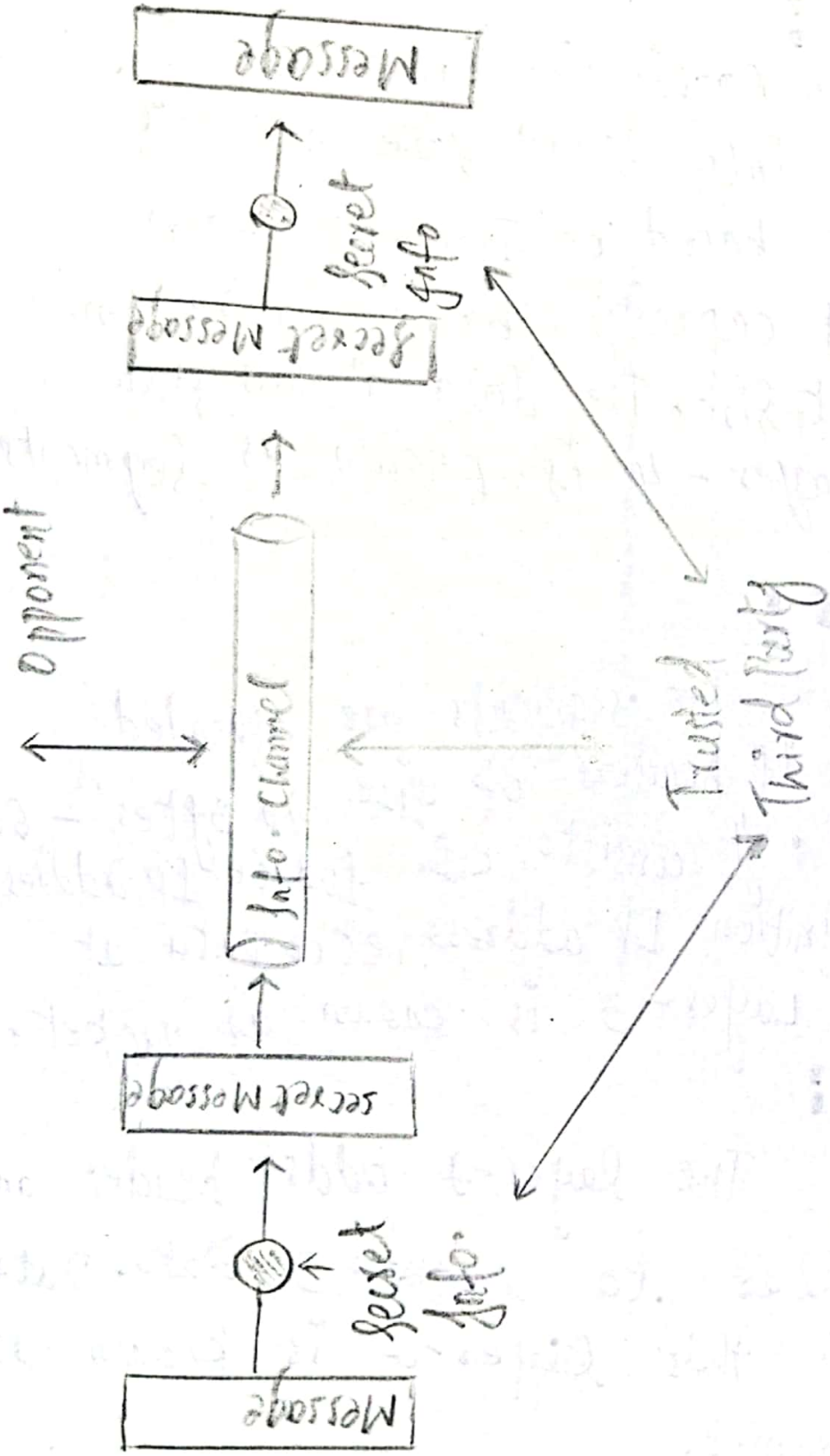
Question #1:

Diff b/w Active and Passive Attacks

Active Attacks	Passive Attacks
→ In Active attack, information is modified.	→ In Passive Attack, the message is observed and copied.
→ Active Attack is dangerous for integrity and availability	→ Dangerous for Confidentiality
→ Attention to be paid on detection.	→ Attention to be paid on prevention.
→ System can be damaged and resources can be changed during Active Attack.	→ There's no effect on system and system resources.

Question #2:

Network Security Model



Question #3

i) Segment:

Application Layer Data is broken into small size segments by TCP based on Transport Layer's carrying capacity, based on Maximum Segment Size. The data at this stage at Layer-4 is known as Segments.

ii) Packets:

The segments are appended with IP headers of size 20 Bytes - 60 Bytes. It consists of source IP address, Destination IP address, etc. Data at this Layer-3 is known as packet.

iii) Frames:

The layer-2 adds header and trailer to layer-3 data. Data of this layer-2 is known as Frames.

"Exercise"

Question#1;

DSL	Cable
i) DSL internet runs through standard phone line that are commonly wired at home.	goes through cable lines.
ii) Provides less bandwidth thus is slower.	Provides more bandwidth.

"Adding Router"

Adding a router in network requires the following steps.

i) Decide where to put router.
ii) Connect with network through wire.
iii) Configure wireless router gateway.
iv) Connect gateway to router.
v) Use web dashboard.
vi) Create Username/Password.
vii) Create wi-fi Password.
viii) Use auto Configuration tools when possible.
ix) Setup Security.

Question #3:

Types of Ethernet w.r.t Data Rates:

(i) Fast Ethernet:

It can recieve or transfer at about 100 Mbps, operates at 10/100 base Ethernet and 100 base on fibre.

ii) Gigabit Ethernet:

It can transfer upto 1000 Mbps. It can handle 10/100/1000 base speed Ethernet, 1000 base gigabit speed on fiber.

iii) 10-Gigabit Ethernet:

It is even fast and advanced providing speed upto 10 Gbps. By using fibre optic can be extended upto 10,000 meters.

iv) Switch Ethernet:

This type of network requires switch or hub. Network switches are used for transfering data from one device to another, without inputing any device in network.

Question #4:

Straight Cable :

1st End

orange
orange - white
white - green
white-blue
blue
green
brown
white- brown

2nd End

orange
orange - white
white - green
white - blue
blue
green
brown
white - brown.

Cross over

1st End

white orange
orange
white green
blue
white blue
green
white brown
brown

2nd End

white green
green
white orange
blue
white blue
orange
white brown
brown