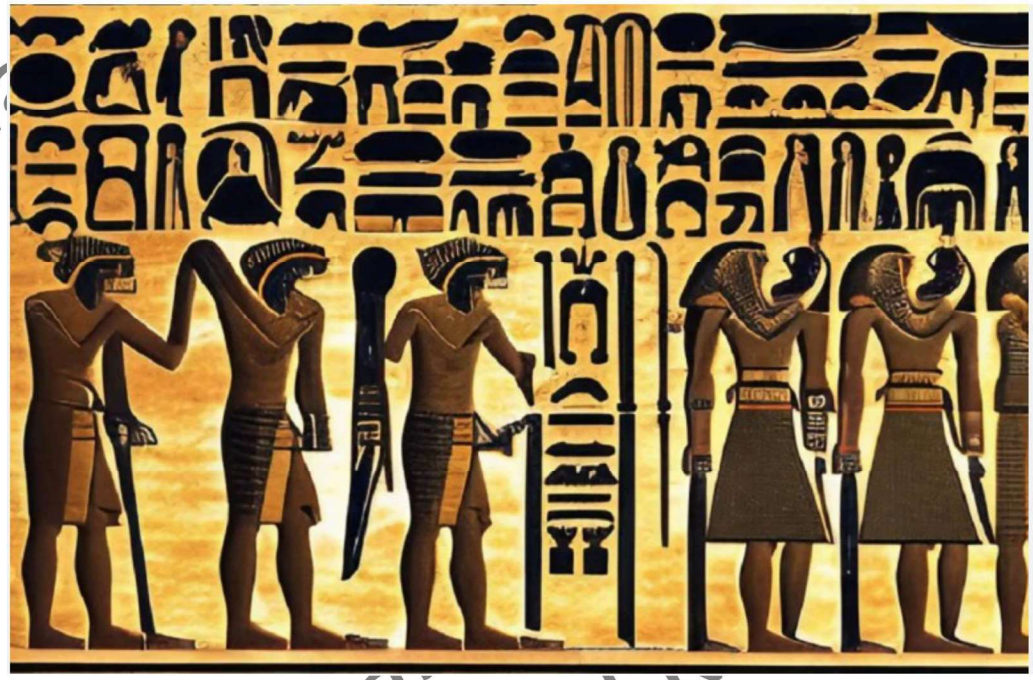
# Cryptography

Block cha pto Currencies
pto Curre
Kumar
lock c Dr. A

# Ancient Cryptography



to Currencie
Dr. Ahlad

Ancient Cryptography

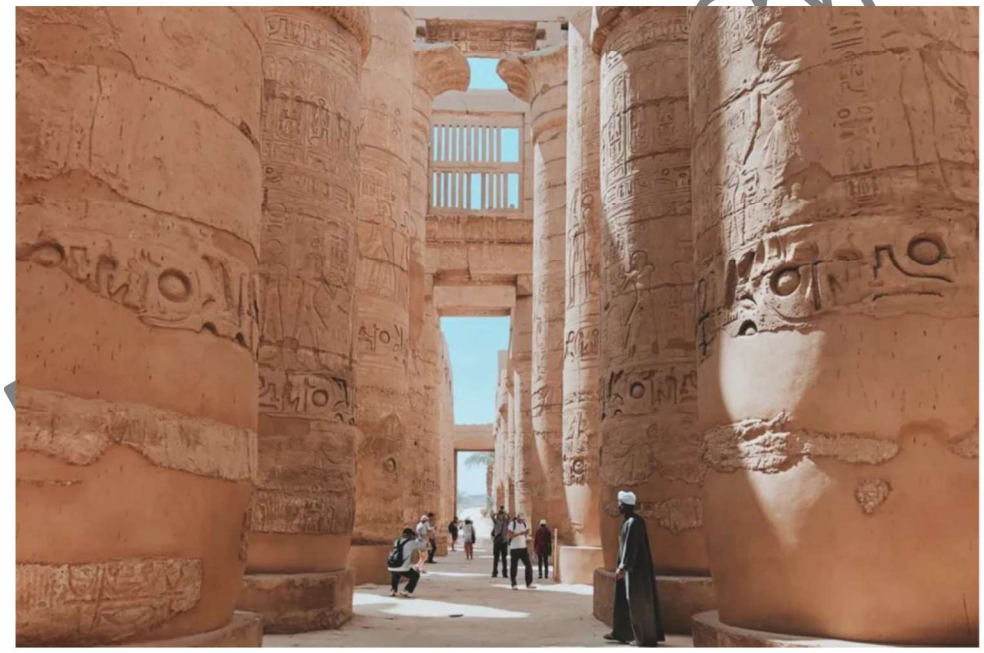
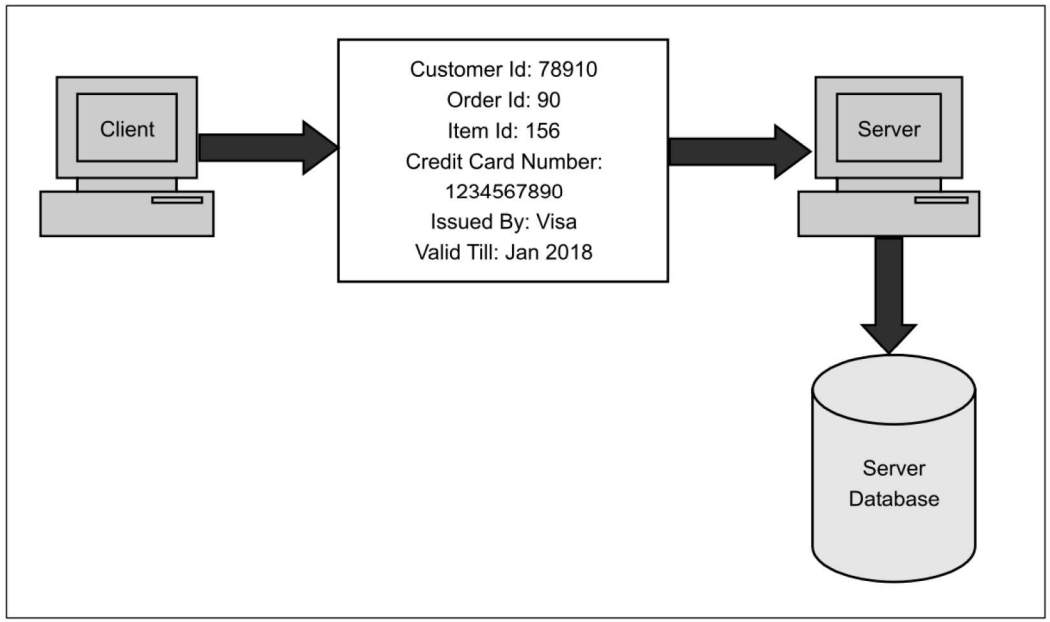


**Fig. 2. Symbols used by Ancient Egypt**

# Need for Security

- Earlier computers had no or a best very little security
- This continued for number of years.
- Need for Security realized when financial and personal data needs security and privacy.




Block chain and Crypto Currencies
Dr Jagadish Kumar

# Need for Security

- Provide a user identification and password to every user, and use that information to authenticate a user.
- Encode information stored in the databases in some fashion, so that it is not visible to users who do not have the right permission.

What are the various Security Holes?

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

# Security Holes

- Intruder can capture the credit card details
- Merchant database can be hacked
- Example: Russian attacker (maxim) managed to intrude merchant site and obtained 300,000 credit card members. Demanded protection money $100,000 from the merchant

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

# Modern Nature of Attacks

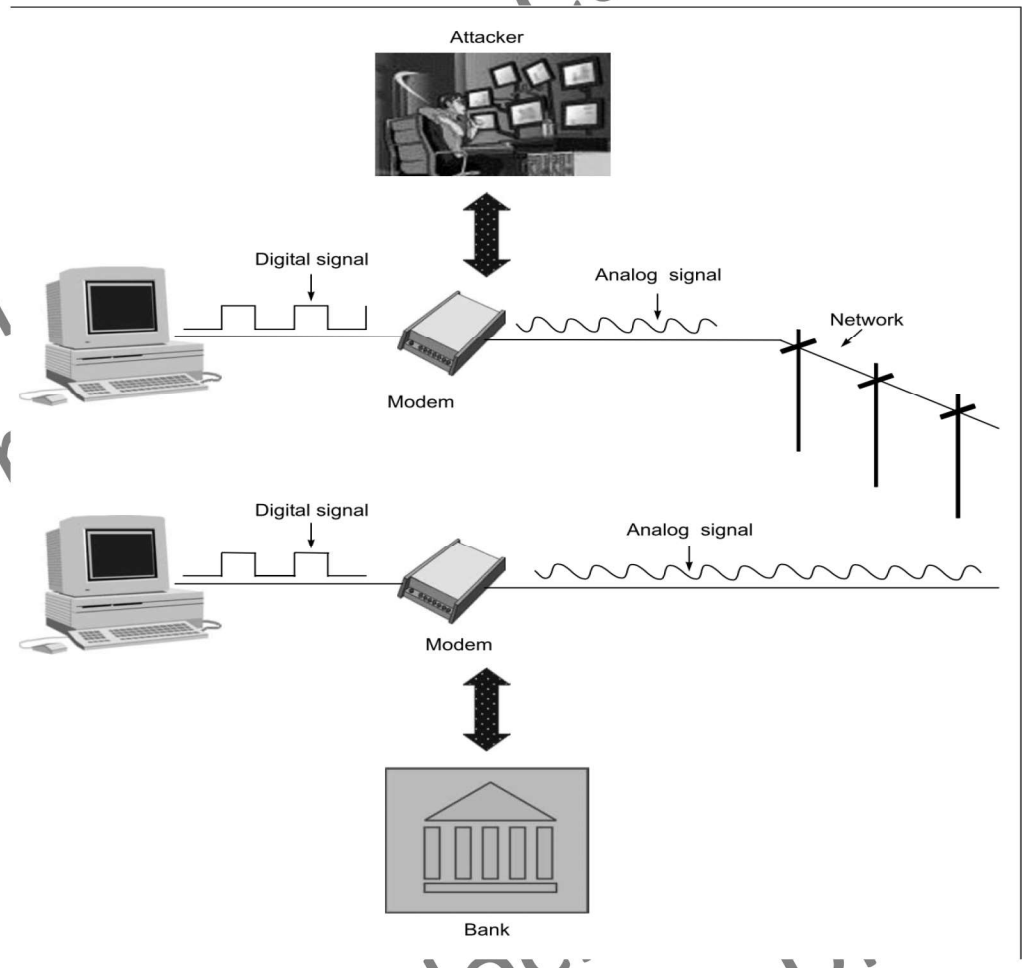
Automating attacks

Traditional attack: Produce coins using some machinery and bring them into circulation.

Modern attack: Steal half a dollar digitally from a million accounts in a few minutes.

Block
pto Currencies
ypto Curre
Kumar

# Distance does not matter




Block chain
Currencies
Crypto Curre
lad Kumar

# Principle of Security

- Let us assume that a person A wants to send a check worth $\$100$ to another person B. Normally, what are the factors that $A$ and $B$ will think of, in such a case? A will write the check for $\$100$, put it inside an envelope, and send it to B.

What can be the possible ways we can enforce security?

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

# Principle of Security

- Let us assume that a person A wants to send a check worth $\$100$ to another person B. Normally, what are the factors that $A$ and $B$ will think of, in such a case? A will write the check for $\$100$, put it inside an envelope, and send it to B.
  - A will like to ensure that no one except B gets the envelope, and even if someone else gets it, he/ she does not come to know about the details of the check.
  - B would like to be assured that the check has indeed come from A, and not from someone else posing as A (as it could be a fake check in that case).
  - $\mathrm{A}$ and $\mathrm{B}$ will further like to make sure that no one can tamper with the contents of the check (such as its amount, date, signature, name of the payee, etc.).
  - What will happen tomorrow if B deposits the check in his/her account, the money is transferred from A's account to B's account, and then A refuses having written/sent the check? The court of law will use A's signature to disallow A to refute this claim, and settle the dispute.

Block chain and Crypto Currencies
Dr. Ahlad Kumar

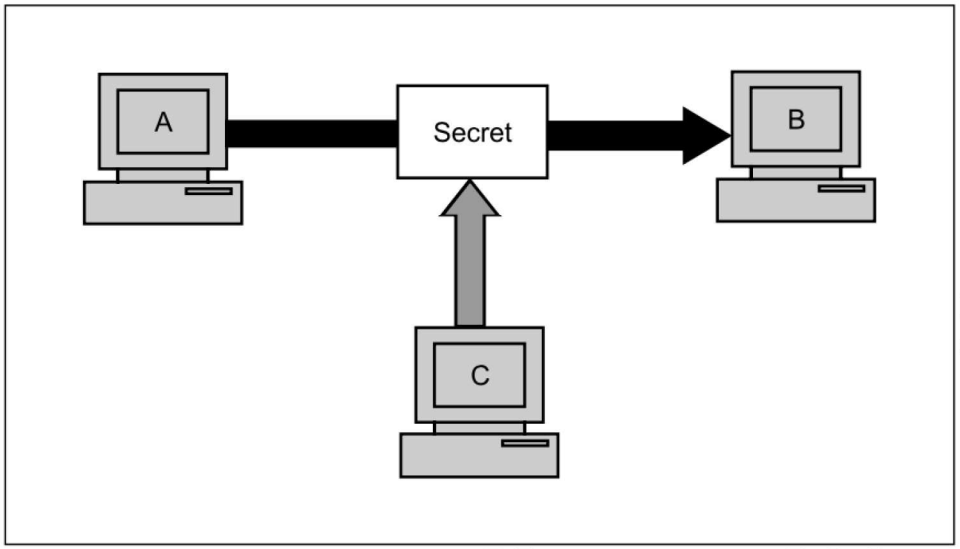
# Principles of Security

## (1) Confidentiality

Only the sender and the intended recipient should be able to access the content of a message

Example:

Email message sent by A to b which is accessed by C without permission or knowledge of A and B. This type of attack is interception



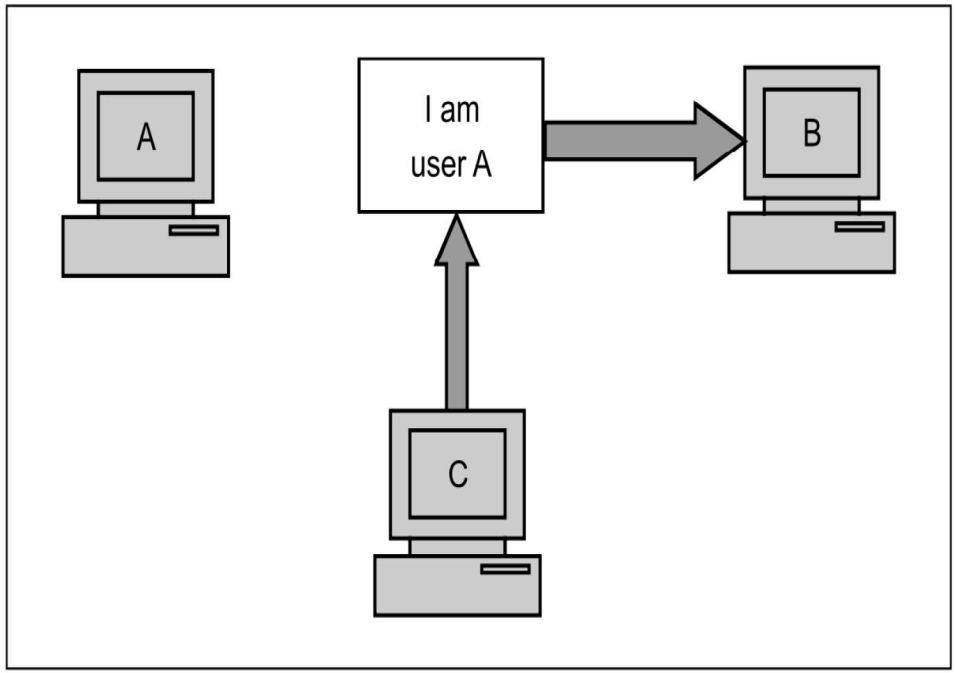

Block chain and Crypto Currencies
Dr. Ahlad Kumar

# (b) Authentication

(1) This mechanism helps establish proof of identities.
(2) Ensures origin of electronic message or document is correctly identified.

(3) Example: Fund transfer request by C posing as A

(4) This type of attack is fabrication attack.

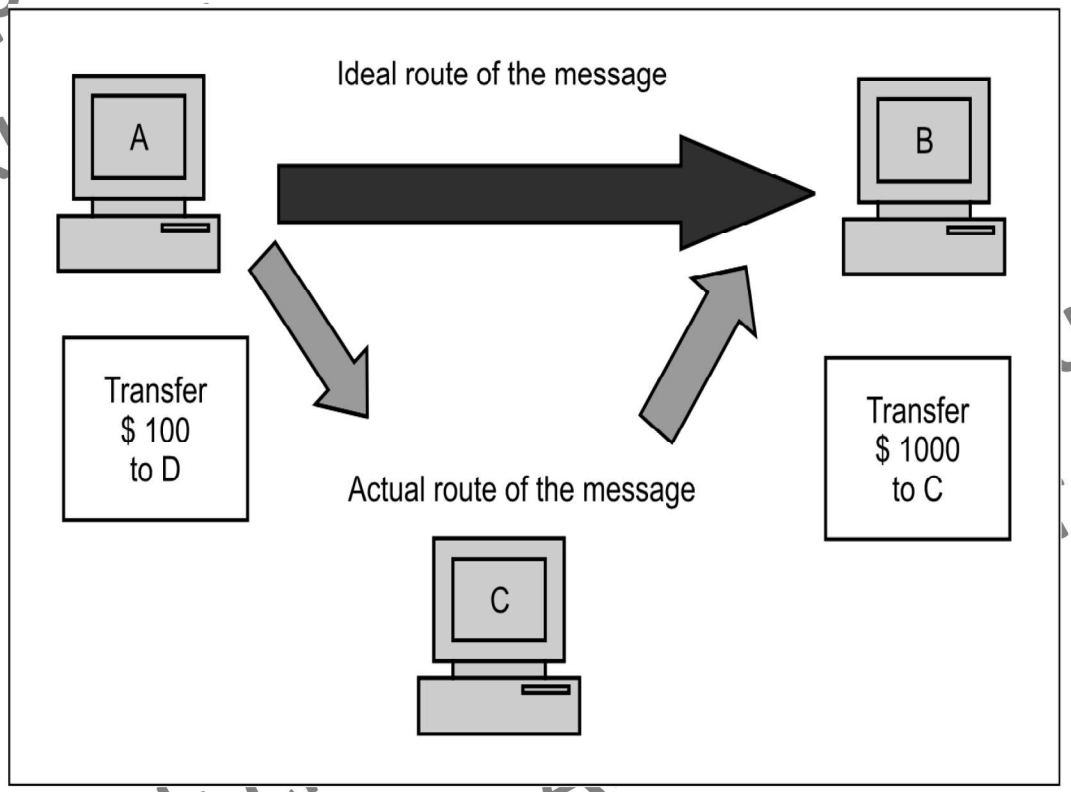



Block chain and Crypto Currencies
Dr. Ahlad Ku

# (c) Integrity

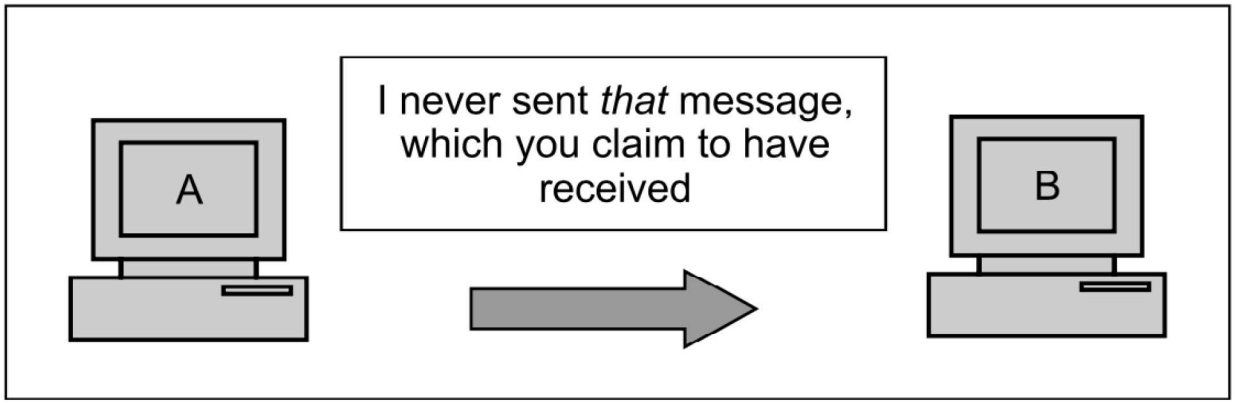
(1) When the content of a message are changed after the sender sends it, but before it reaches the intended recipient, integrity of the message is lost.

(2) This type of attack is called modification.




Block chain and Crypto Currencies
Dr. Ahlad K

# (d) Non-repudiation



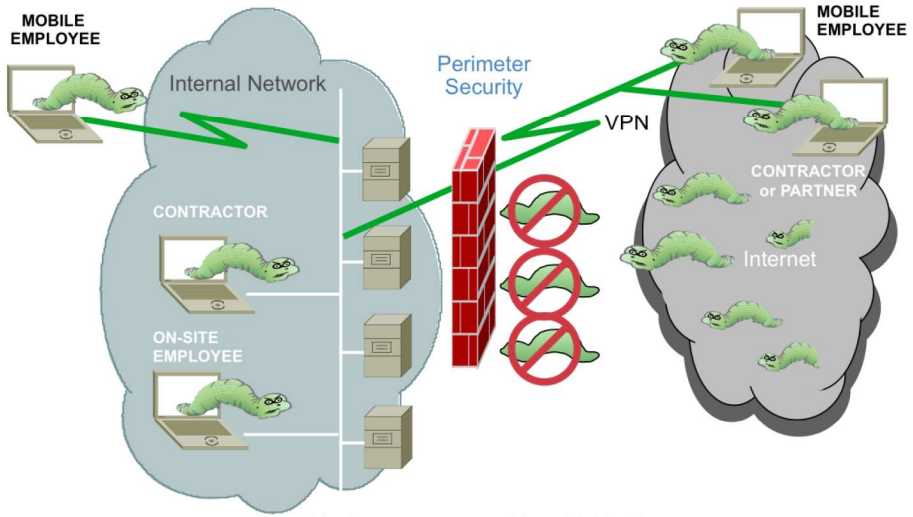

(1) There are situations where a user sends a message, and later on refuses that she had sent that message. For instance, user A could send a funds transfer request to bank B over the Internet. After the bank performs the funds transfer as per A's instructions, A could claim that he/she never sent the funds transfer instruction to the bank! Thus, A repudiates, or denies, his/her funds transfer instruction. The principle of non-repudiation defeats such possibilities of denying something after having done it.

(2) Non-repudiation does not allow the sender of the message to refute the claim of not sending the message

Block chain and Crypto Currencies
Dr. Ahlad Kumar

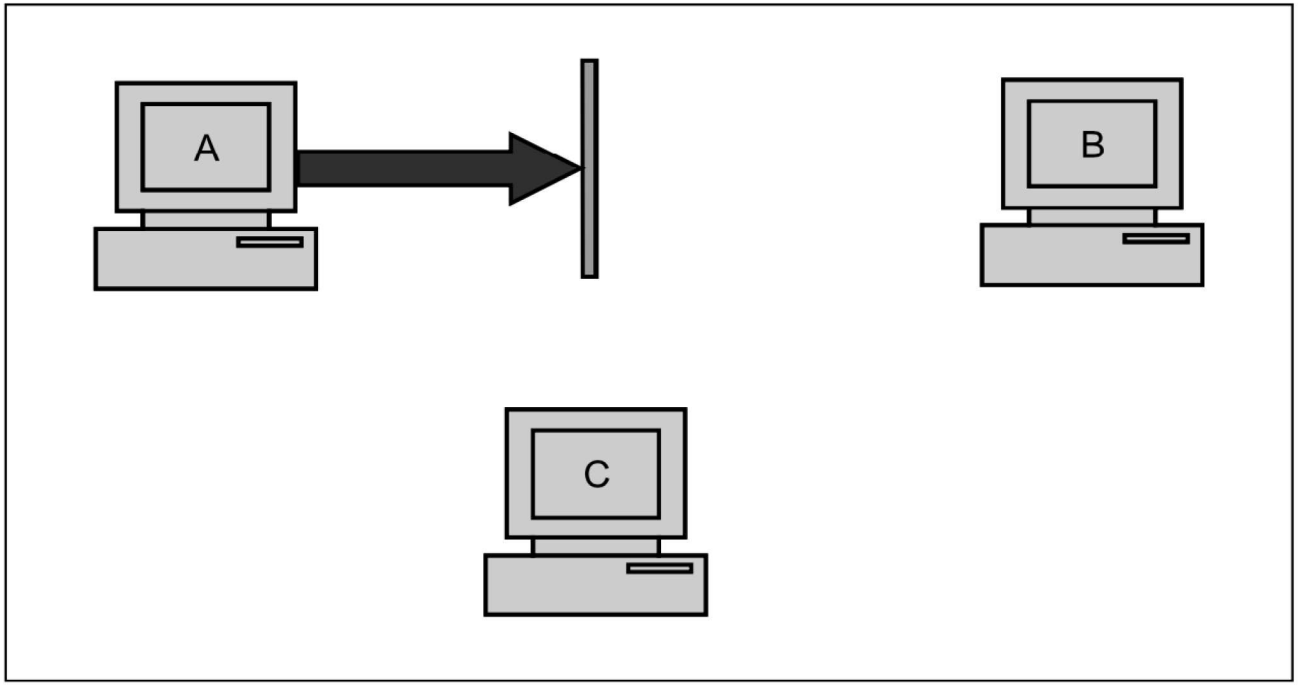
# (e) Access Control

- **Access control** is the prevention of unauthorized use of a resource
- 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).




Block chain and Crypto Currencies
Dr. Ahlad Kumar

# (f) Availability




The principle of availability states that resources (i.e. information) should be available to authorized parties at all times. For example, due to the intentional actions of another unauthorized user C, an authorized user A may not be able to contact a server computer B. This would defeat the principle of availability. Such an attack is called interruption.

Block chain Currencies
Block chain and its Current
Dr. Ahlad Kumar

# Principle of Security

- Let us assume that a person A wants to send a check worth $\$100$ to another person B. Normally, what are the factors that $A$ and $B$ will think of, in such a case? A will write the check for $\$100$, put it inside an envelope, and send it to B.
  - A will like to ensure that no one except B gets the envelope, and even if someone else gets it, he/ she does not come to know about the details of the check. This is the principle of confidentiality.
  - A and B will further like to make sure that no one can tamper with the contents of the check (such as its amount, date, signature, name of the payee, etc.). This is the principle of integrity.
  - B would like to be assured that the check has indeed come from A, and not from someone else posing as A (as it could be a fake check in that case). This is the principle of authentication.
  - What will happen tomorrow if B deposits the check in his/her account, the money is transferred from A's account to B's account, and then A refuses having written/sent the check? The court of law will use A's signature to disallow A to refute this claim, and settle the dispute. This is the principle of non-repudiation.

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

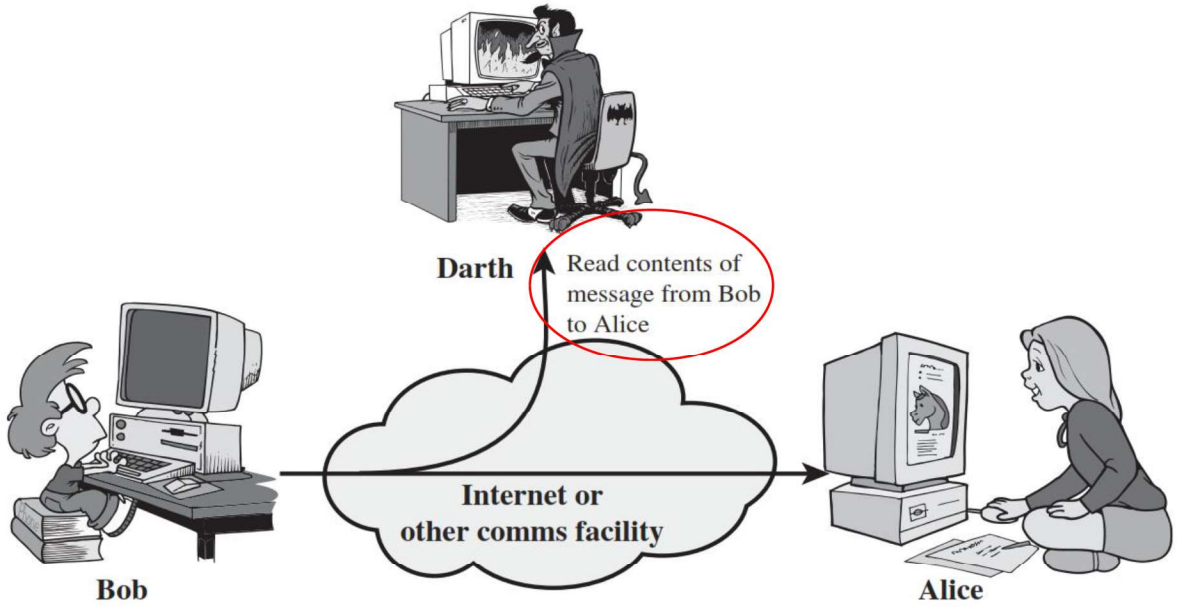
# Security Attacks

- A **passive attack**
  - Passive Attacks are those wherein the attacker indulges in eavesdropping or monitoring of data transmission i.e. the attacker aims to obtain information that is in transit.
  - The term passive indicates that the attacker does not attempt to perform any modifications to the data.
  - That is why passive attacks are harder to detect.
  - The general approach to deal with passive attacks is to think about prevention, rather than detection or corrective actions.

- Types of Passive Attacks
  1. Release of message contents
  2. Traffic analysis

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

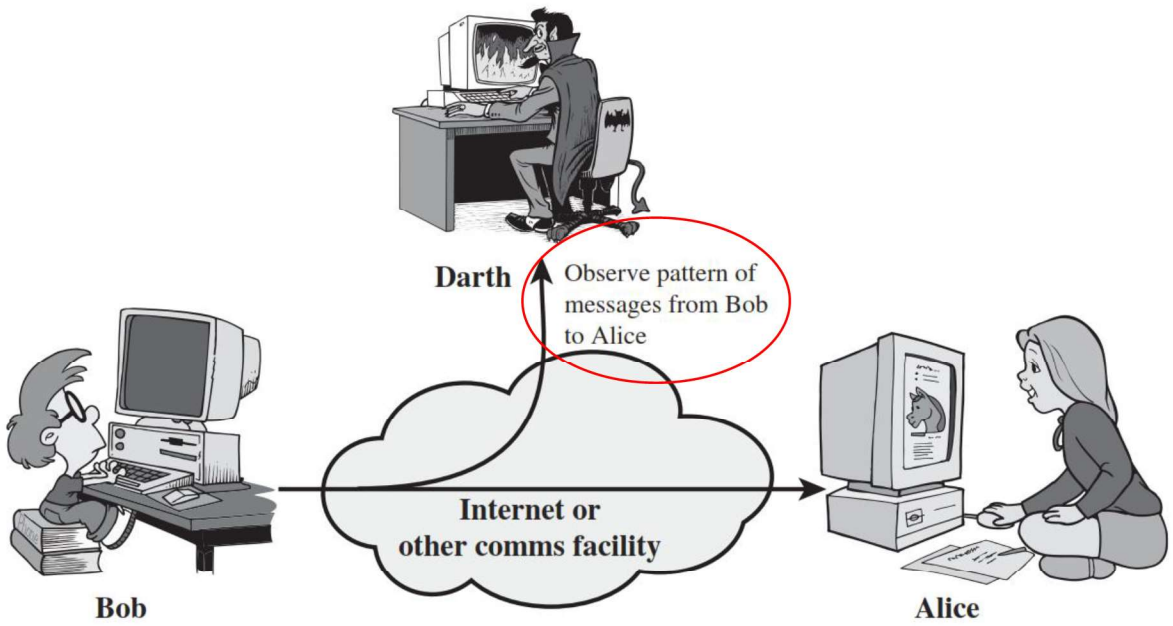
# 1) Release of message contents (Passive Attack)




- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from learning the contents of these transmissions.

Block chain and Crypto Currencies
Dr. Ahlad Kumar

# 2) Traffic Analysis (Passive Attack)




- In such attacks, an adversary, capable of observing network traffic statistics in several different networks, correlates the traffic patterns in these networks.

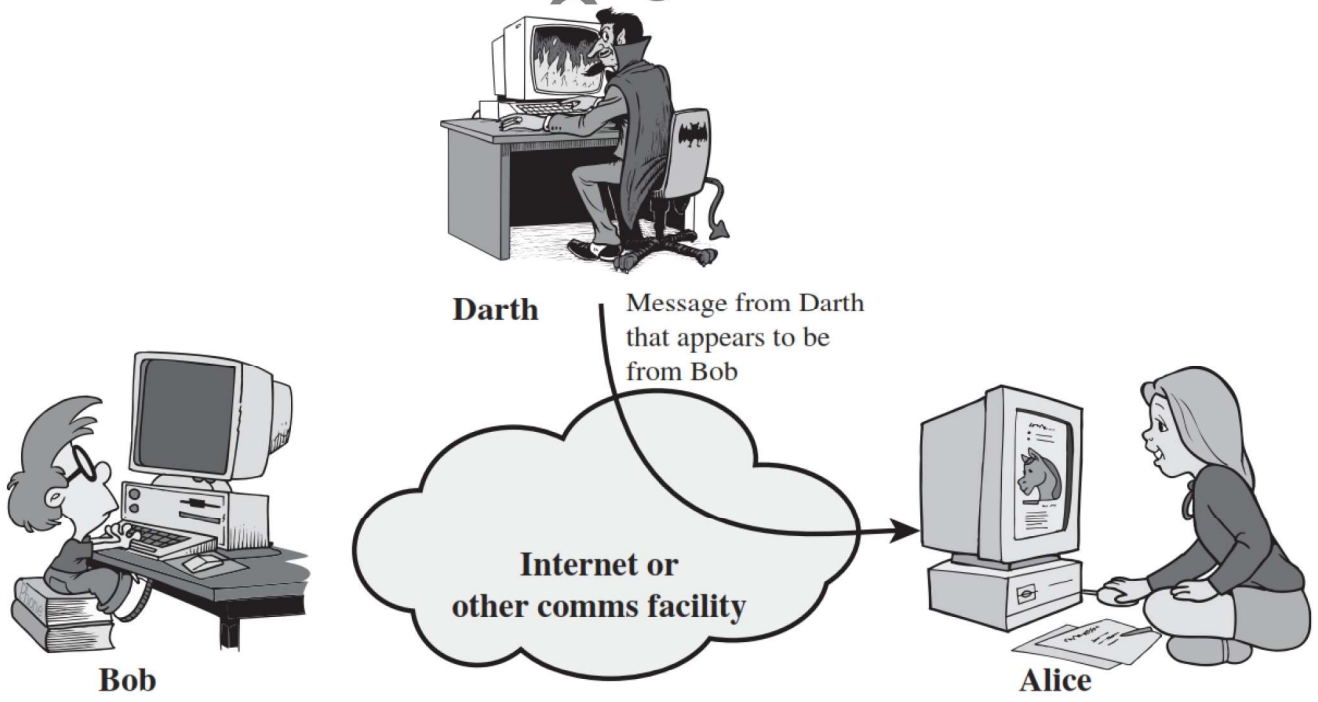
Block chain and Crypto Currencies
Dr. Ahlad Kumar

# Security Attacks

- An **active attack :** are based on the modification of the original message in some manner, or in the creation of a false message.
  - These attacks cannot be prevented easily.
  - However, they can be detected with some effort, and attempts can be made to recover from them.
  - These attacks can be in the form of interruption, modification and fabrication.
- In active attacks, the contents of the original message are modified in some way.
  - Trying to pose as another entity involves masquerade attacks.
  - Modification attacks can be classified further into replay attacks and alteration of messages.
  - Fabrication causes Denial Of Service (DOS) attacks.

Block chain and Crypto Currencies
Dr. Ahlad Kumar
Block chain and Crypto Currencies
Dr. Ahlad Kumar

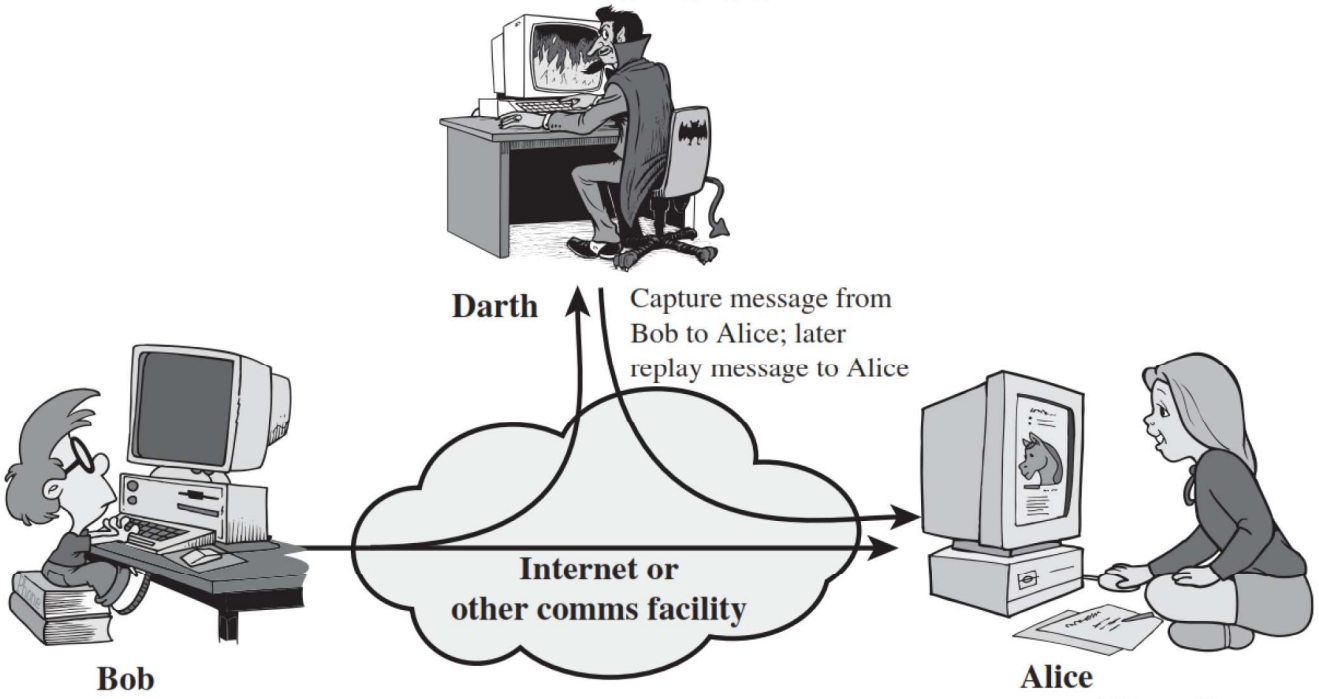
# 1) Masquerade/Spoofing Attack (Active Attack)




- A **masquerade** takes place when one entity pretends to be a different entity. tacks, usually some other forms of active attacks are also embedded. As an instance, the attack may involve capturing the user's authentication sequence (e.g. user ID and password). Later, those details can be replayed to gain illegal access to the computer system.

Block chain and Crypto Current clear
Dr. Ahmad Kumar

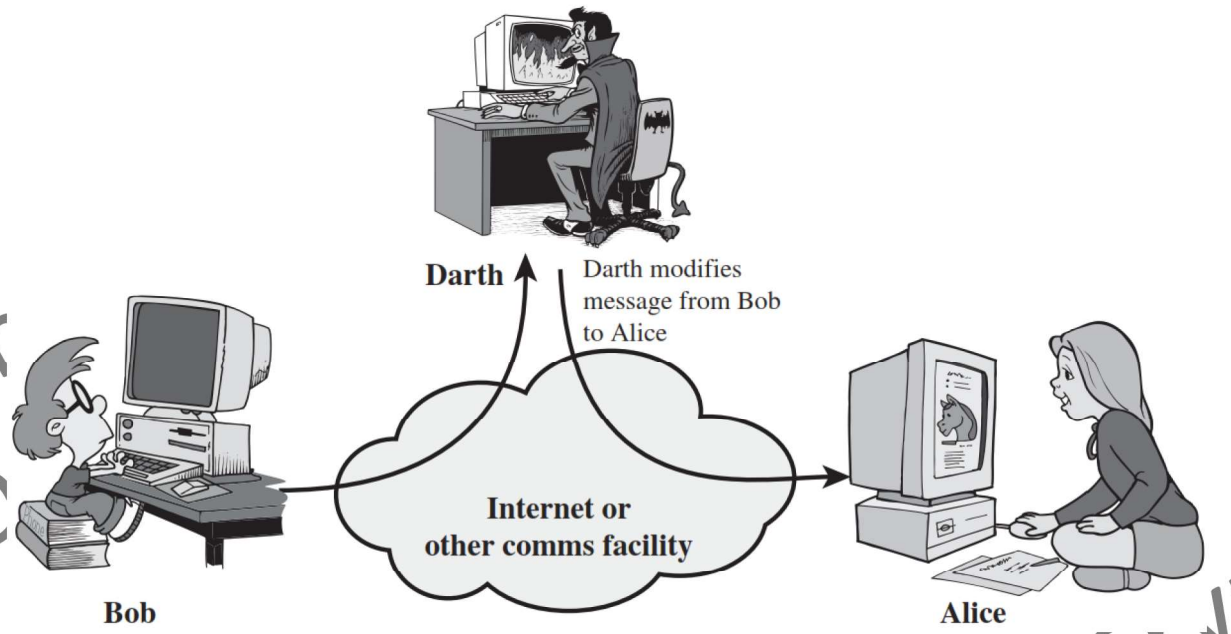
# 2) Replay Attack (Active Attack)




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

Block chain and Crypto Currencies
Dr. Ahtad Kumar

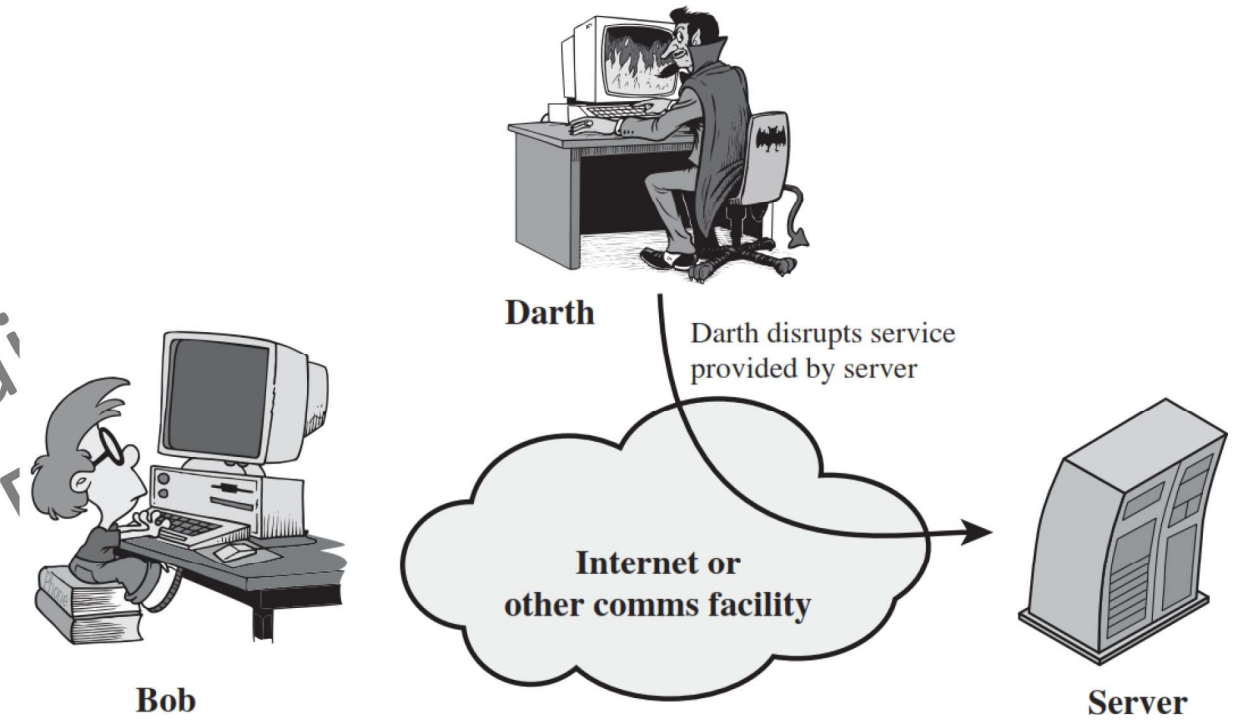
# 3) Modification of messages Attack (Active Attack)




- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

Block chain and Crypto Currencies
Dr. Ahlad Kumar

# 4) Denial of Service Attack (Active Attack)




- Denial Of Service (DOS) attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids in quick succession, so as to flood the network and deny other legitimate users to use the network facilities.

Block chain and Crypto Currencies
Dr. Ahlad Kumar