https://web.mit.edu/kerberos/

Kerberos:
Authentication protocol
Client-Server authentication by
Secret-key Cryptography
Free implementation: MIT

Internet an insecure place (many protocol don't provide security.
Tools to "Sniff" passwords off are common by use of malicious hackers

Firewall problem

"Bad" guys are outside which is bad assumption.
Most damaging incidents of computer crime are by someone inside.
Firewalls also have disadvantage, they restrict how users use the internet

Kerberos uses strong Cryptography so that a client can prove its identity to the server

https://www.webopedia.com/quick_ref/OSI_Layers.asp

OSI Model: Open system Interconnection

Not even tangible

It doesnot perform any function in networking process.

It is a conceptual framework so that we can better understand Complex interactions that are happening.

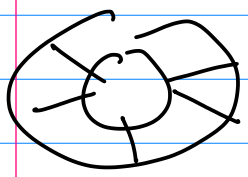
Who developed OSI model?

ISO

International standard organization

7 layers

1-4 Lower layers

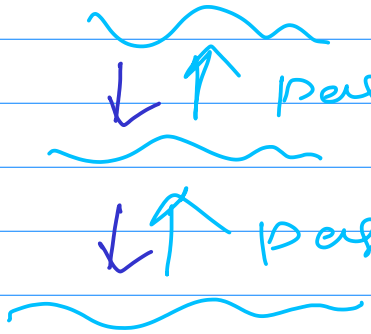


Tire
" 4

↳ moving data

5-7 upper layers

Application level data



Each layer does the specific job and passes the data onto the next layer

Layer 7 – Application

Layer 6 – presentation

Layer 5 – Session

Layer 4 – Trasport

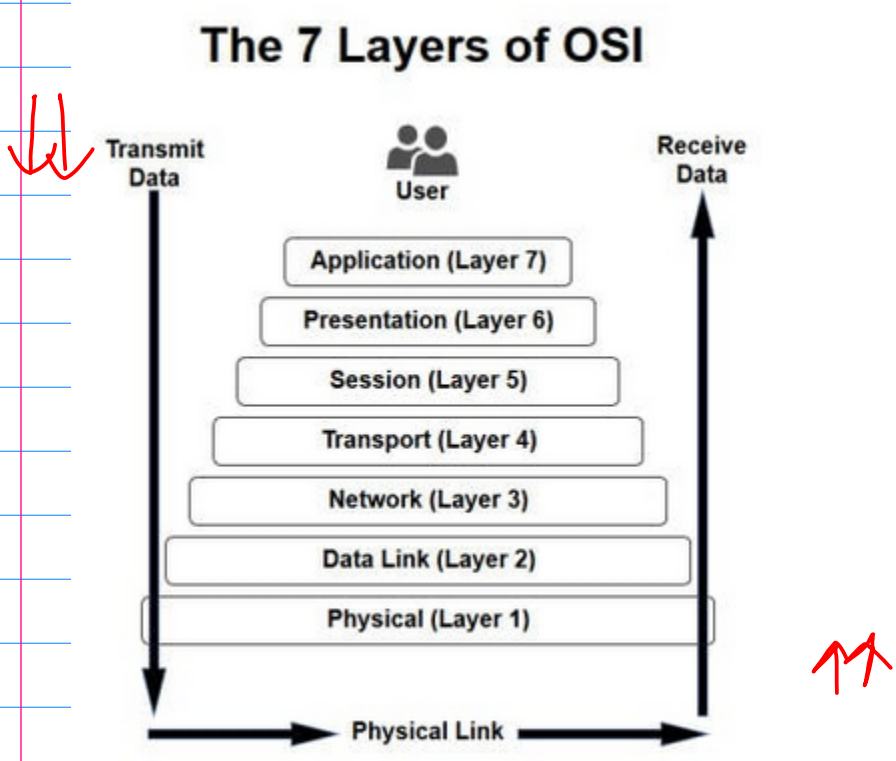
Layer 3 – Network

Layer 2 – Data Link

Layer 1 – Physical

memo

ϕ data network Trasport se present absent



Application (Layer 7)

Supports application and end-user processes.

(1) Identification

Communication partners

(2) User authentication

(3) privacy

(4) constraint on data syntax

Layer provides application services for

→ File transfers (FTP)

→ emails (SMTP)

→ network software (Telnet)

→ web HTTP

Presentation (Layer 6)

Translate data (encryption) that application layer can accept.

It formats and encrypts data to be sent across a network, providing freedom from compatibility problems

examples:-

ASCII, TIFF, GIF, JPEG, MIDI

Session (Layer 5)

Establishes
Manages
Terminates
} connections between applications

eg NFS, RPC, SQL

Transport (Layer 4)

Transparent transfer of data between end systems or hosts.

And is responsible for end to end error recovery and flow control

Network (Layer 3)

Switching and routing technologies

→ Virtual circuits

transmitting data from node to node

Data Link (Layer 2)

Data packets are encoded and decoded into bits.

Media Access Control (MAC) and Logical Link Control (LLC) layer

Physical (Layer 1)

Conveys the bit stream

→ electrical impulse, light or radio signal

It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects

Examples:

Ethernet, FDDI, RJ45

https://tinyurl.com/y9gf659r www.computerworld.com

IPsec IP Security

Comprises a suite of protocols

↓

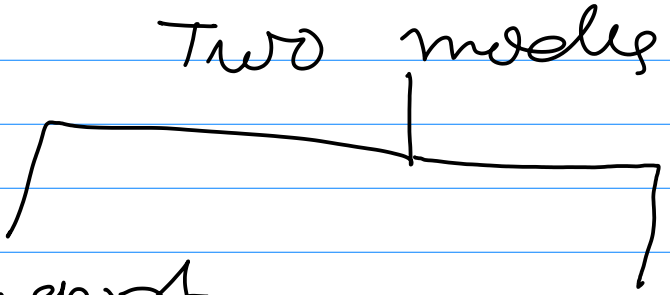
ensure the integrity, confidentiality, and authentication of data communications over an IP network.

IPSec (three different security domains)

- → Virtual private networks
- → Application-level security
- → Routing security

IPsec is predominately used in VPNs.

When used in application-level security or routing security, IPsec is not a complete solution and must be coupled with other security measures to be effective, hindering its deployment in these domains.



Transport mode

Source and destination hosts must directly perform all cryptographic operations

Encrypted data is sent through a single tunnel that is created with L2TP (Layer 2 Tunneling protocol)

Tunnel mode

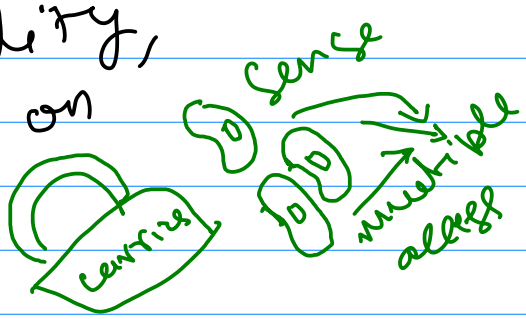
special gateways perform cryptographic processing in addition to the source and destination hosts.

Many tunnels are created in series between gateways, establishing gateway-to-gateway security

Data (ciphertext) is created by the source host and retrieved by the destination host.
This mode of operation establishes end to end security

IPSec

Authentication, integrity, confidentiality, encryption



searchnetworking.techtarget.com

CSMA/CD

Carrier sense multiple access/collision detect

Transmission access

It is a protocol for carrier transmission access in Ethernet networks

device Send a frame at a time

If another device tried to send a frame at same time

Collision occurs and frame is discarded.

Device waits for random amount of time, senses whether the line is ideal, and retries until successful in getting the transmission slot.

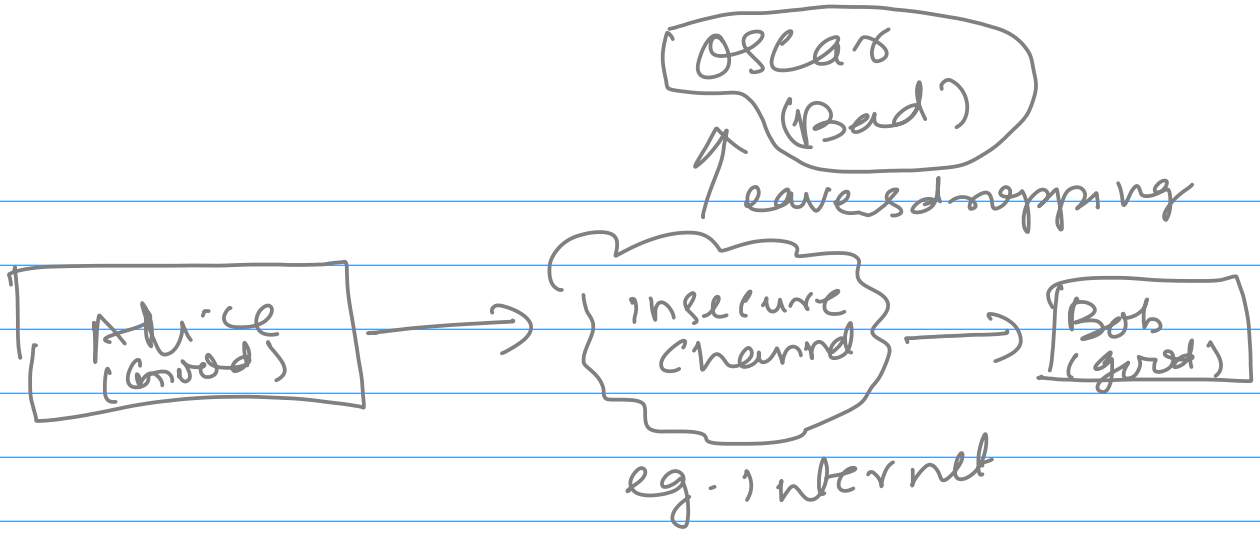
Springer- Understanding Cryptography (Christof Paar, Jan Pelzl)

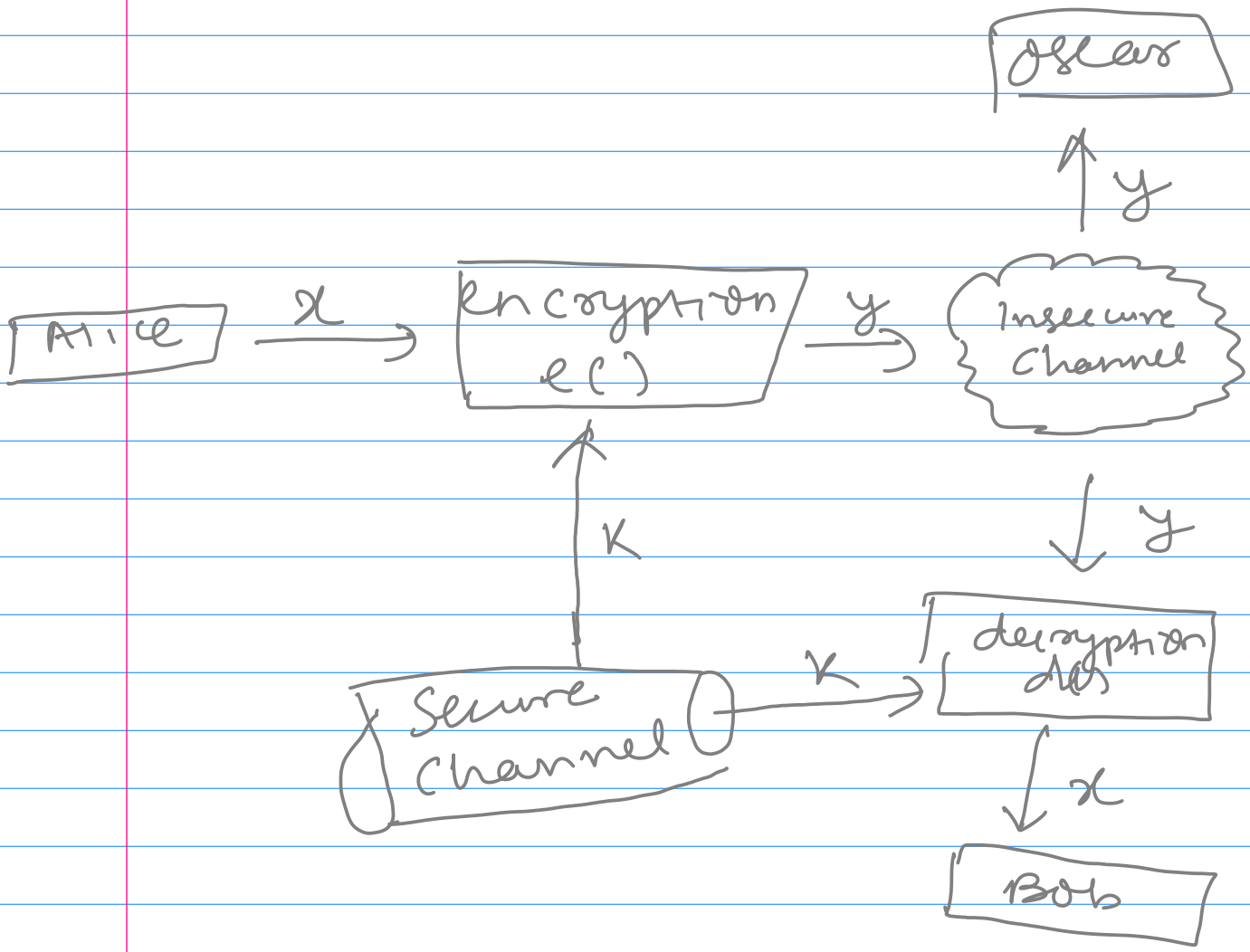
Symmetric cryptography

↓ also

Symmetric-key,
Single-key,
Secret-key

Q = Why it is called Single-key?





x is called plaintext or clear text
y is called ciphertext
K is called the key.

Asymmetric Cryptography (public-key)

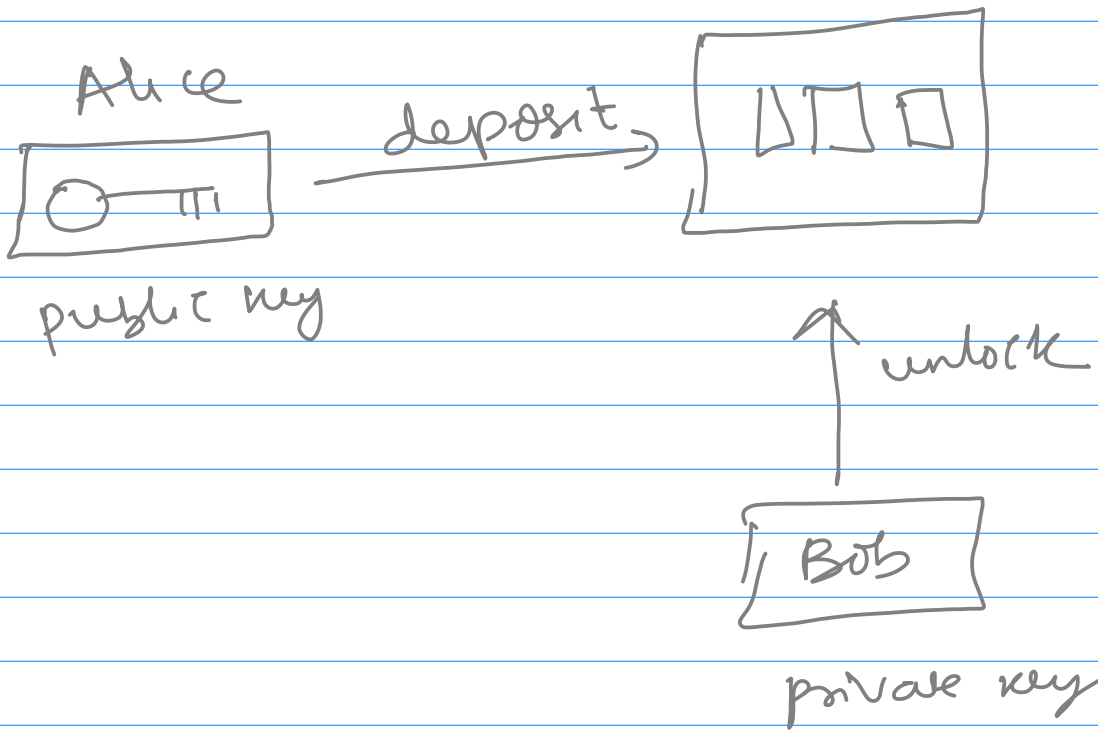
problem of Symmetric encryption:

(1) Key distribution problem

Number of keys

$$\frac{n(n-1)}{2}$$

(2) No protection against cheating by Alice or Bob.



Principles of Asymmetric Cryptography

It is not necessary that the key possessed by the person who (Alice) encrypts the message is secret Bob, the reciever, can only decrypt using a secret key.

Bob publishes a public encryption key which is known to everyone Bob also has a matching secret key which is used for decryption.

Bob's key 'k' consists of two parts, a public part, k_{pub} and a private one k_{pr}.

Alice

$y = e_{k_{pub}}(x)$

Bob

k_{pub} ← $(k_{pub}, k_{pr}) = k$

y →

$x = d_{k_{pr}}(y)$

https://searchstorage.techtarget.com/definition/RAID

RAID (Redundant array of independent disks)

It is a way of storing the same data in different places on multiple hard disks to protect data in the case of a drive failure.

However, not all RAID levels provide redundancy

Disk Striping

Disk striping is a process of dividing a body of data into blocks and spreading the data across multiple storage devices, such as hard disks or solid-state drives (SSDs)

RAID 0:
Has striping but no redundancy of data.

Striping

Best performance, but no fault tolerance.

RAID 1:

Mirroring

Also known as disk mirroring : duplicate storage of data.

No striping

RAID 2: NO longer used (striping, error checking)

Uses striping across disks, with some disks storing error checking and correcting information.

No advantage over RAID three.

RAID 3: parity and striping

Dedicates one drive to store parity information.

Data recovery is accomplished by calculating the exclusive OR (XOR) of information recorded on the other drives.

https://searchnetworking.techtarget.com/definition/TCP-IP

TCP/IP (Transmission Control Protocol/Internet protocol)

It is a suite of communication protocols used to interconnect network devices on the internet

TCP/IP can also be used as communications protocol in a private network (an intranet and an extranet)

Specifies how data is exchanged over the internet by providing end-to-end communication that identify

how it should be broken into packets, addressed, transmitted, routed and received at the destination.

TCP: How application can create channels of communication across a network. It also manages how a message is assembled into smaller packets

before they are then transmitted over the internet and reassembled in the right order at the destination address

IP : Defines how to address and route each packet to make sure it reaches the right destination.