Date : / /
Page No.:

Cryptography
Steganography

CIA → Confidentiality Integrity Availability.

Keys → Symmetric
→ Asymmetric

AES algo for encryption
↳ Advanced Encryption Standard.
IDEA

DMPG

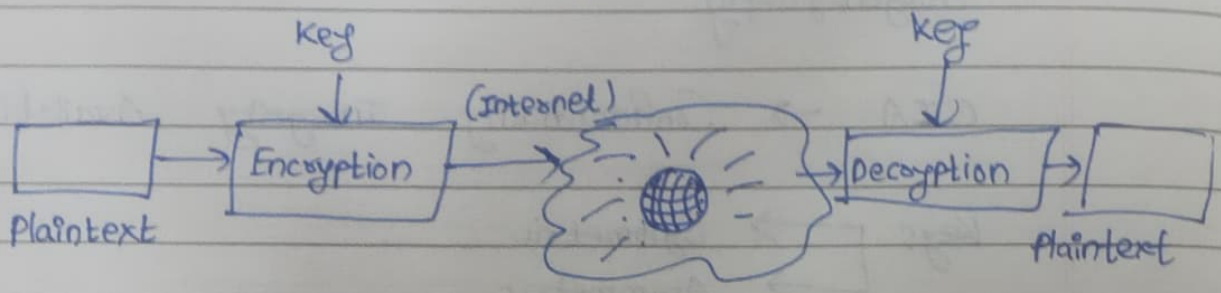
Stages of DLM
1) Data acquisition.
2) Data storage
3) Backup and Recovery.
4) Data Management/sharing
5) Data usage
6) Data retention & destruction

HPC

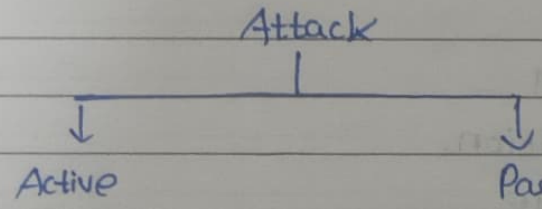
Intro to Parallel Computing
Ananth Grama, Anshul Gupta, George Karypis & Vipin Kumar.

Compute followed by communication is 11 processing.

Model of Network Security



Key(encryption) = key(decryption) ⇒ Symmetric Key.
Key(encryption) != key(decryption) ⇒ Asymmetric (Public) Key.



HPC

SPMD → Single Program Multiple Data.

Dichotomy of Parallel Computing Platforms
① Logical organization → Programmer's view.
② Physical organization → Actual hardware organiz".

T-com ⇒ Time required for process communicat".

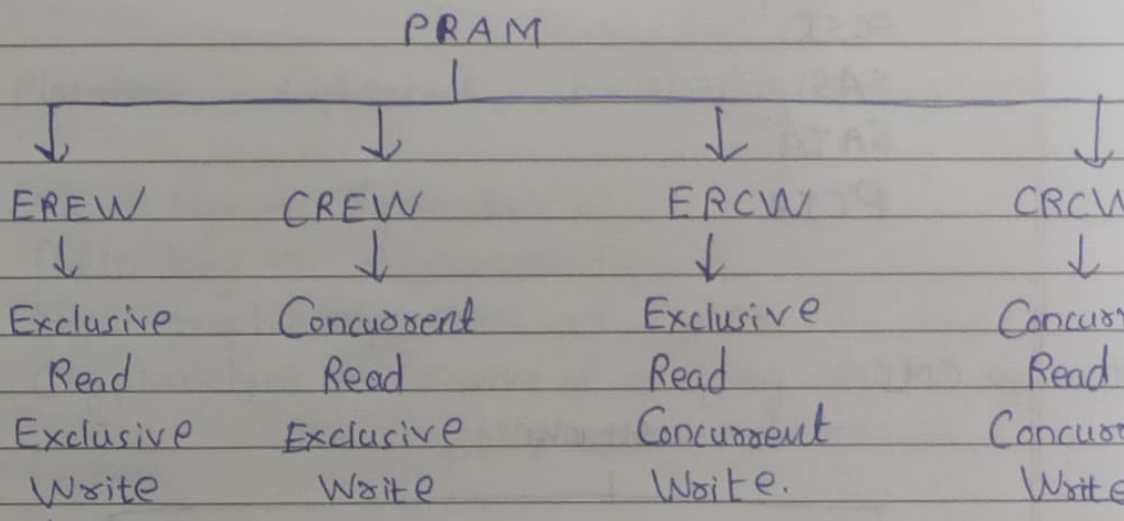
$$\text{Granularity} = \frac{\text{Computation}}{\text{Communication}}$$

PE → Processing Element.
IC → Interconnection Network.
PRAM → Parallel Random Access Machines

Coarse Grain → Small number of large sized tasks.
→ Lower Communicat^{n}.

Fine Grain → Large number of small sized task.
→ Higher Communicat^{n}.
→ Load balancing.

Memory Architectures { UMA → Uniform Memory Access
NUMA → Non-uniform -11-



- Locality of Reference.

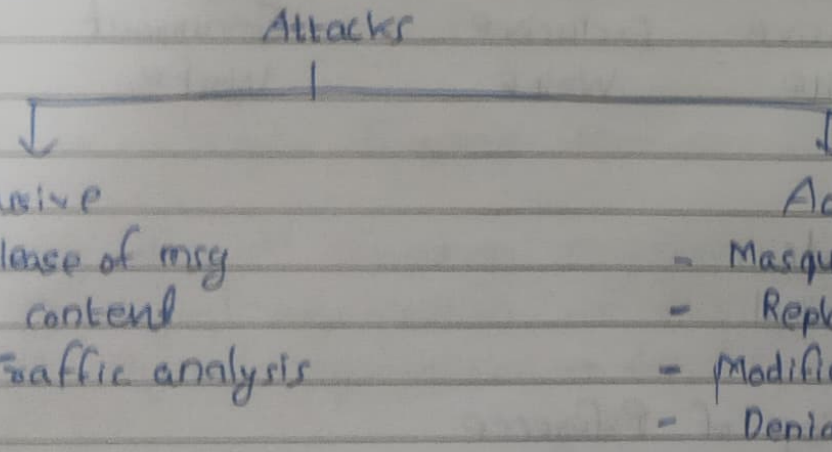
23/07/24 Tuesday

DMPG (MOD 2) → Data storage & data availability.
HDD, SSD.
SATA Device.

- What is Data Center?
  - DAS → Direct Attached Storage
  - NAS → Network -11- -11-
  - SAN → Storage Attached Network.

DAS Interface
SCSI
SAS
SATA
PCIe

11 CNS



HCI

WIMP → Windows Icons Menus Pointers.
Interface
OR
Windows Icons Mice & pull-down menus.

20/07/24 Tuesday

CENS

Classical Encryption Techniques

Plaintext, Ciphertext, Enciphering (Encryption),

Secret key → Symmetric.
Public key → Asymmetric.
Cryptographic algorithms → Cipher.
Cryptanalysis → Science of studying attacks against cryptographic systems

⊙ Cipher

Symmetric Cipher — Asymmetric Cipher.

- Block cipher → encrypt data block of plaintext at a time (64 or 128 bit) → DES, AES.
- Stream Cipher → encrypts data one bit or byte at a time.

① Symmetric Encryption.

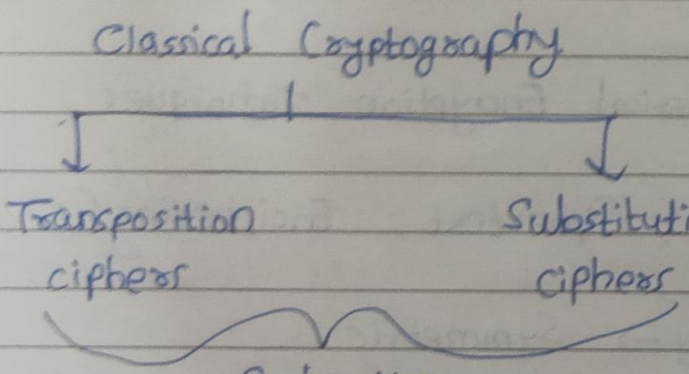
$Y = E_K(X)$ or $Y = E(K, X)$

algo.

key

plaintext.

$X = D_K(Y)$ or $X = D(K, Y)$



- All modern ciphers are "product ciphers".

DMPG

Storage Network Industry Association (SNIA)

RAID types

- H/W RAID
- S/W RAID

HCI Activity

Word processor for blind people.

Design a UI for word processor for blind people.

HPC Lab.

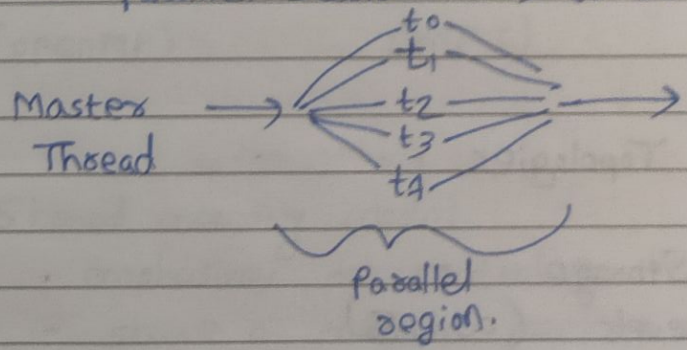
OpenMP

MPI

Cuda

⊙ OpenMP.

- portable shared memory programming
- pragmas for C/C++
- parallel section has to be defined by developer.



omp_get_num_threads() → Total no. of threads.

omp_get_thread_num() → thread no. for specific thread.

```
# pragma omp parallel
{
    // parallel section.
}
```

To set no. of threads:

① export OMP_NUM_THREADS=2 // env. variable.

② In program.

ANT Analyzer.

D D M M Y Y Y Y

Q.1).

```
#include<stdio.h>
#include comp.h>
```

inA su

31/07/24 Wednesday

DMPG

- Storage attachment strategies
  - DAS
  - SAN
  - NAS
- Network Topologies
- VM's
- Cloud Storage
- RAID levels (0, 1, 5).
  - RAID 0 → Stripping.
  - RAID 1 → Mirroring
  - RAID 5 → Stripping with parity.
  - RAID 6 → Stripping with distributed parity.

(Explain any 2 RAID levels given).

- Storage pooling
  - Primary Storage Pool.
  - Copy Storage Pool.
- Storage Provisioning.

HPC

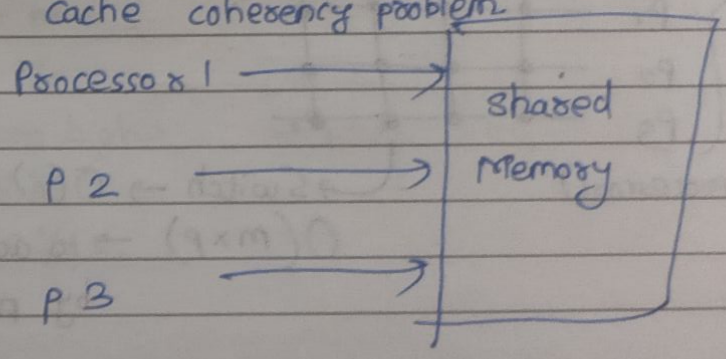
PRAM → Parallel Random Access Machine.

↑ also stands for no. of processors.

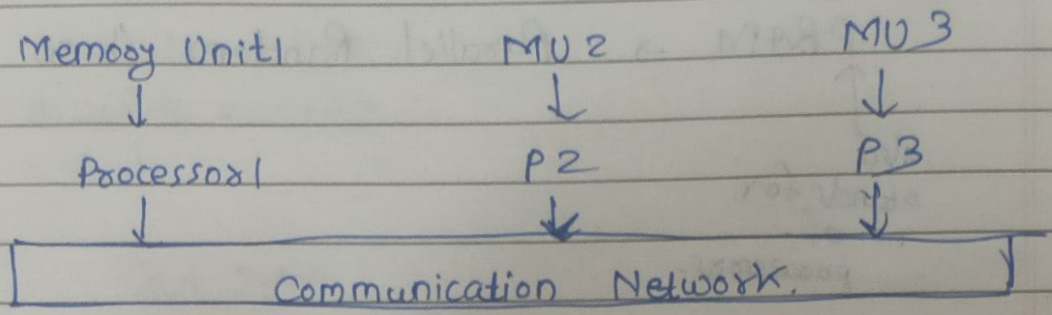
PRAM Model Implementation.

- Shared memory model (OpenMP)
- Message passing model (MPI)
- Distributed memory model

① Shared memory model
- emphasizes on control parallelism.
- share a common memory space.
- Cache coherency problem

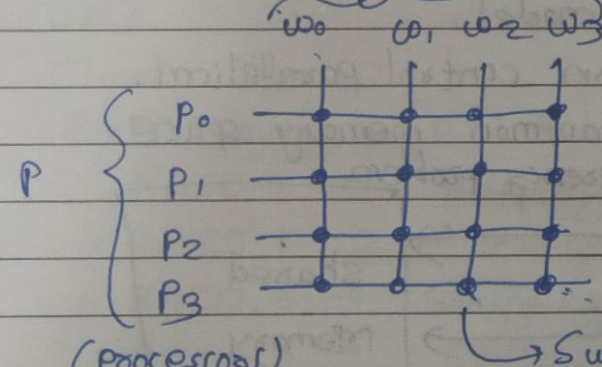


② Message Passing Platform
- MPI
- distributed memory approach.
- interaction through message passing.



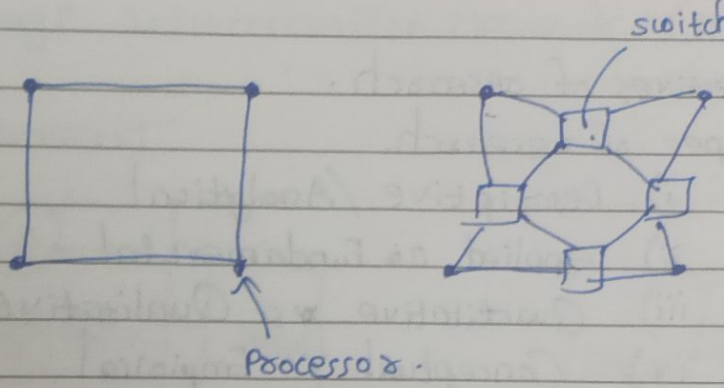
③ Distributed Memory.
- processors have their local memory.
- no issue of cache coherency.
- explicitly need to define sub-tasks by programmer.

- Physical Complexity of 11^{el} computer.



$O(m \times p)$ → to access memory by processor.

- Interconnection Network.
  - made up of switches & links.
  - carry data bet^n processor & memory.
  - static / dynamic.
    - Direct network
    - Indirect network



HCI

Usability goals & measures:

1. Time to learn.
2. Speed of performance.
3. Rate of errors by users.
4. Retention over time.
5. Subjective satisfaction

ERP Evaluation

1 30 m.
2 60 %
3 very high.
4 90 %.
5 40 %.

RM.

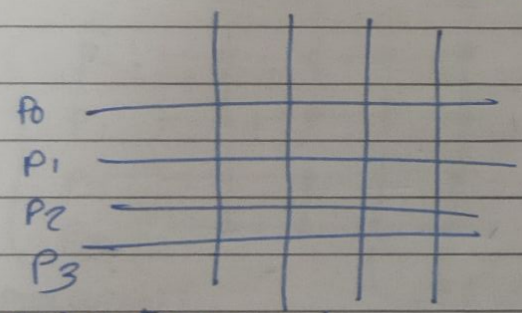
- Objectives of research.
- Types of research.
  - i) Descriptive / Analytical
  - ii) Applied or Fundamental
  - iii) Quantitative vs Qualitative.
  - iv) Conceptual vs Empirical.

01/08/24 Thursday

HPC

- Network Topologies (static / dynamic).
- Topologies tradeoff performance for cost.

- Crossbars network topologies



(p × m)

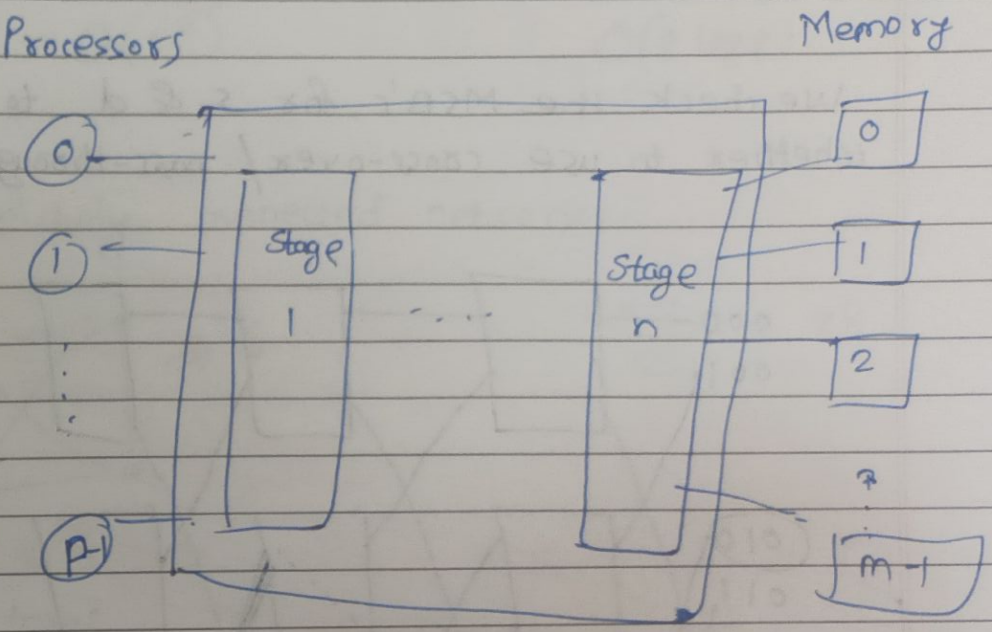
cost complexity = $O(p^2)$ (crossbar)

Networks

- Blocking
- Non-blocking.

Cost of switch = (degree of switch)^2

- Multistage Interconnection Network (MIN)



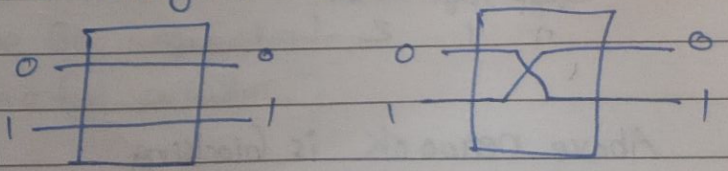
- Omega network (most commonly used MIN)
- $\log_2 P$ stages
- i/p i is connected to o/p j

$$j = \begin{cases} 2i & 0 \le i \le P/2 - 1 \\ 2i+1-P & P/2 \le i \le P-1 \end{cases}$$

$P = 8,\ i = 4 \Rightarrow \text{stages} = \log P = \log_2 8 = 3.$

Perfect Shuffle patterns connected using 2x2 switches.

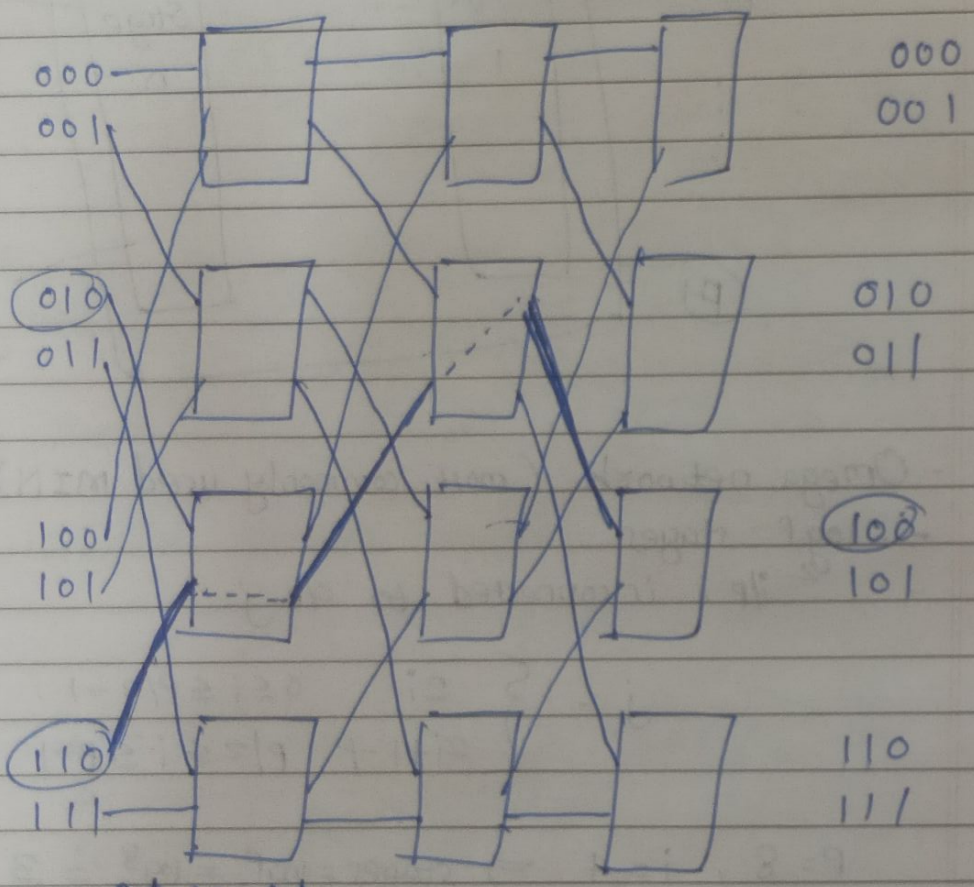
2 modes → Pass through, Cross over.



n(switching nodes) = $P/2 \times \log P$

s → binary repres^n of source.
d → —11— dest^n.

We check the MSB's for s & d to decide whether to use cross-over / pass-through.

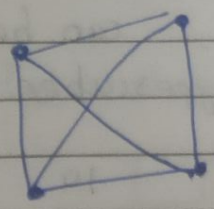


Cost complexity = O(p log p)

Above network is blocking

Crossbar network	Multistage network
$O(p^2)$	$O(p \log p)$

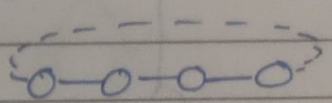
- Completely connected network:



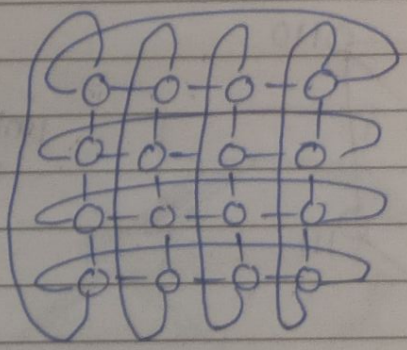
→ 6

$$\frac{8 \times 7}{2} = 28.$$

1-D- torus



2-D-torus



(2-D mesh with wrap around link).

$p = 16$.

02/08/24 Friday

- Dense or Sparse architecture.

$T_s \rightarrow$ Time for sequential
$T_p \rightarrow$ Time for parallel.

- Parallelism go hand in hand with Concurrency.

if ($T_p > T_s$)

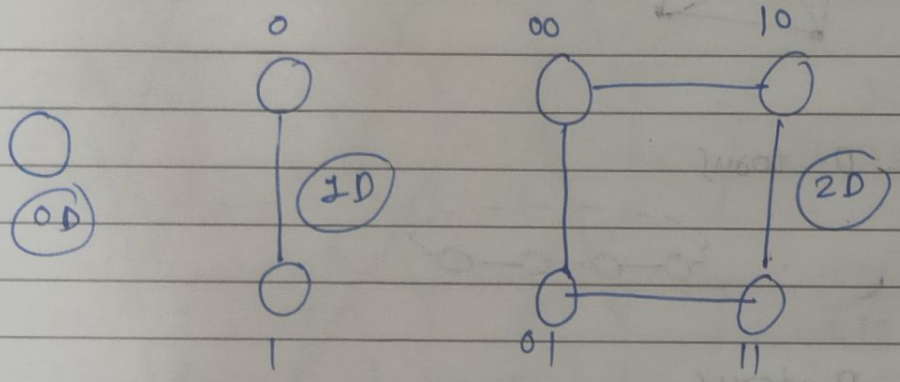
use parallel

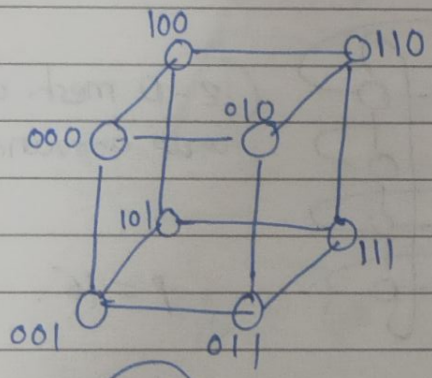
else

use sequential

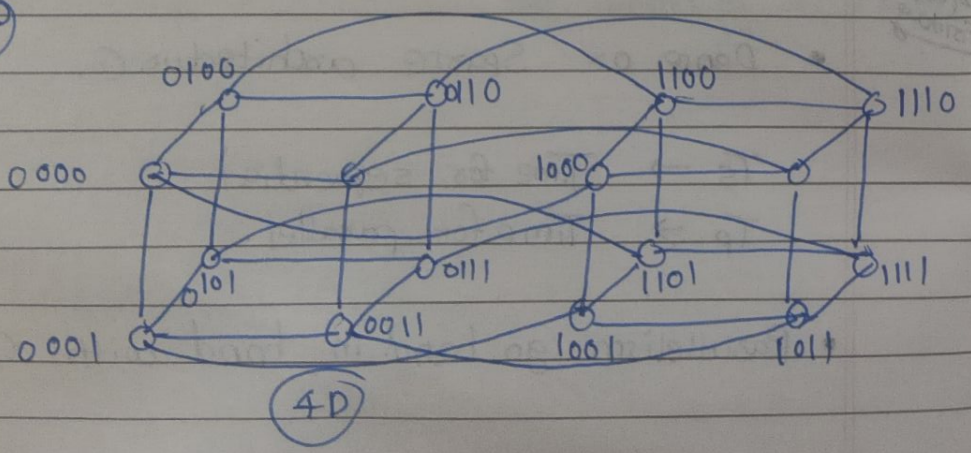
⊙ Hypercube.

- Every D dimentional hypercube has 2^D nodes.
- Every hypercube with $D > 0$, can be formed by connecting 2 D-1 hypercuber.





$$\text{links} = \frac{P \times \log P}{2}$$



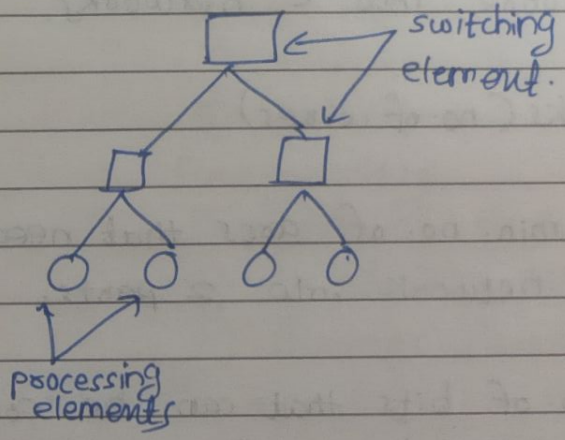
Dist^n bet^n P's is bit difference (Hamming distance)

Farthest dist^n bet^n 2 nodes = $\log_2^P$

e.g. (0000, 1111) = 4 links

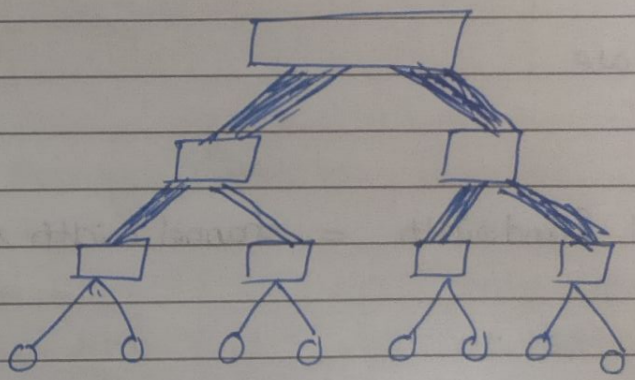
$\log_2^{16} = 4$

⊙ Tree-Based Network.



Drawback: Traffic through root only.

Fat Tree:



? How to evaluate architecture

Diameter → dist^n bet^n 2 farthest points

Linear arr = $p-1$

mesh = $2(\sqrt{p}-1)$

tree = $\log p$

hypercube = $\log p$.

complete connected = $O(1)$.

Bisection Width → min wires to be cut to divide network into 2 networks.

Cost → no. of links (no. of wires)

Arc Connectivity → min. no. of arcs that need to be removed to divide network into 2 parts.

Channel width → no. of bits that can be communicated over a channel simultaneously, bet^n 2 nodes.

Peak Rate

Channel Bandwidth = channel width x peak rate.

Cache Coherence in multiprocessor system

- Every processor may have different cache copy

HCI → MS Dynamics, SAP

06/08/24 Tuesday

DMPG

Cloud Storage
- low cost high bandwidth.
- CSPs (Cloud Storage Providers)
- public & private clouds.
- safety
- Cloud Types:
  1) Public 2) Private 3) Hybrid 4) Community
  5) Mobile
- Functionality
  1) Syncing 2) Enhanced Security
  3) Collaboration Tools 4) Space efficiency
  5) Disaster Recovery 6) Pay-as-you-Go (cost)

07/08/24 Wednesday

Cache Coherency

08/08/24 Thursday

HPC.

Message Passing Costs in Parallel Computers.

1) Startup time (ts) → only once.
2) Per hop time (th) → at each hop, latency.
3) Per-word transfer time (tw) → m(words) × tw.

⊙ Store & forward Routing

$$t_{comm} = t_s + (mt_w + t_h)l.$$

↑ multiplicative term.

where, t_{comm} ⇒ Communication time.
t_s ⇒ Startup time.
m ⇒ no. of words.
t_w ⇒ per word transfer time.
t_h ⇒ per hop time.
l ⇒ no. of links traversed.

If t_h is very small then,

$$t_{comm} = t_s + ml t_w.$$

09/08/04

Human Relations at work

Father of mgmt studies - Fredrick Taylor.
Henry Fayol - 14 principles.

1) Division of work
2) Authority
3) Desciplin e
4) Unity in command.
5) Unity in direction
6) Alignment of personal & general interests
7) Renumeration
8) Centralization.
9) Scalar Chains
10) Order
11) Equality
12) Stability in tenure
13) Stability of tenure
14) Initiatives
15) Harmony

HPC

⊙ Packet Routing
- message is broken down into packets & pipelined them through the network.
- errors checking, sequencing & header information.

total communication cost $= t_{comm} = t_s + t_h l + t_w m$.

$t_h l$: additive term.

- Disadv: Each packet will carry more information.

⊙ Cut-through Routing
- message divided into flits (basic unit)
- flits are too small, thus also header.
- traces msg decides path & all flits are routed in same path.

$t_{comm} = t_s + t_h l + t_w m$.

t_w is very small

if l is large, use cut through routing.
if l is smaller, use store & forward (overhead is less)

- Simplified cost model for communicating messages:

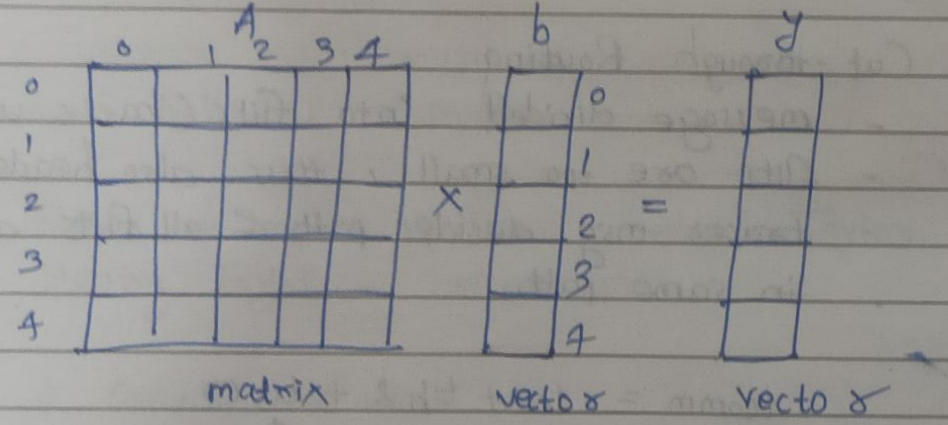
$$t_{comm} = t_s + lt_h + t_w m \approx t_s + t_w m.$$

(Mod 1 Complete)

Mod 2 Principles of Parallel Algorithm Design.

(authors: Ananth Grama, Anshul Gupta, George Karypis & Vipin Kumar)

Step 1: Decompose the task into sub-tasks.

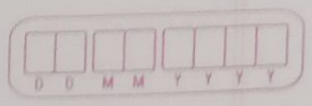


Here, decomposition can be done in 'n' no. of ways.
Tradeoff bet^n memory & communication overheads.

- Maximum degree of concurrency: no. of tasks (max) running parallely.
- Algorithms differ for dense & sparse matrices.

* → except loop iterator.

set omp_num_threads = 5



HPCL Session.

- loop iterator variables are private to each thread.

① private ② shared (by default everything is shared *)
③ firstprivate ④ lastprivate

~~Private~~ ~~firstprivate~~.

~~Sum =~~

$$\text{Speedup} = \frac{\text{Sequential time}}{\text{parallel time}}$$

- Any code can't be totally parallelized.
- Sequential section affects the speedup.

- Synchronization & Communication
  - ↓ wait for all threads to finish work
  - ↓ to communicate all the partial answers.

Work Sharing : Scheduling

- work sharing constructs.
- #pragma omp parallel for construct.
- by default chunk size = 1.
- Dynamic & Static allocation of iterations.

Accounting & Finance for Engineers.

Mod1: Financial accounting
Mod2:
Mod3:

MOD - 1

Accounting :-

Management Accounting - Robert Antony

Characteristics

1) Science & arts
2) Accounting Service
3) Concerned with future
4) Selective by nature
5) Related to costs.
6) Cause & effect analysis
7) Precise & universal
8) To take decisions
9) Purpose is to achieve objectives

Statements

- Income-Expenditure Stmt
- Balance Sheets

Principles

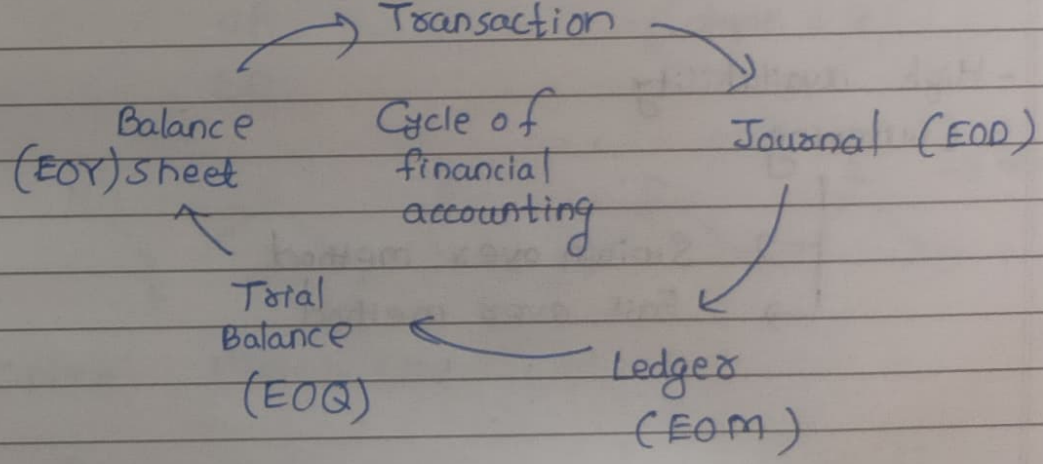
- Accounting Concepts
- Accounting Conventions.

- Accounting Concepts

1. Business Entity vs Owner → are different.
2. Going on (takeovers & acquisitions)
3. Cost concept.
4. Purchasing machinary (dual aspect)
5. Money measurement
6. Acyl Concept (do not write pending transaction).
7. Match making concept

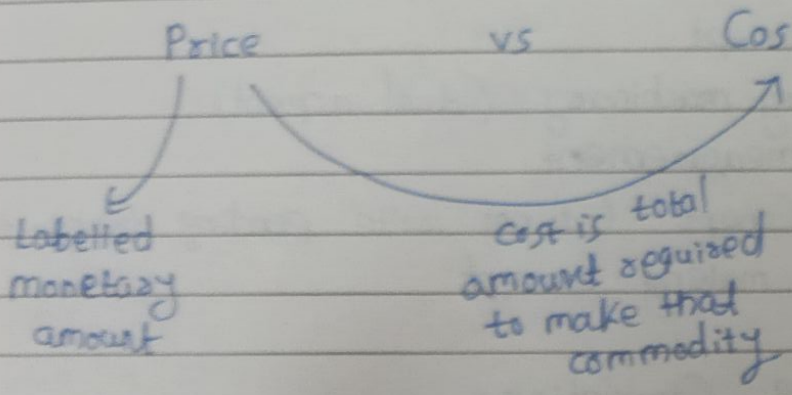
- Accounting Conventions

1. Convention of disclosure
2. —11— consistency
3. Measure of conservatism.
4. Convention of materiality (keep it simple.



9325703697

MOD - 3 [Cost Accounting]



- Fixed Cost vs Variable Cost vs Mixed Cost

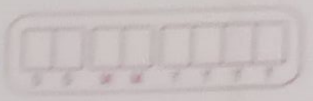
DMPG

- High availability
- Clustering
  - Switch over method
  - Fail over method

Recovery Point Objective (RPO) } Disaster Recovery.

Recovery Time Objective (RTO)

Cryptology → Cryptography → To encode msg.
→ Cryptanalysis → To guess or hack key



CNS

Classical Cryptography

- Substitution cipher → e.g. Caesar cipher
- Transposition (permutation) cipher
- Product Cipher

Transposition Cipher
- Rail-Fence Cipher } Lab.
- Columnar transposition }

eg-1) Plaintext : HELLO WORLD

col1 col2

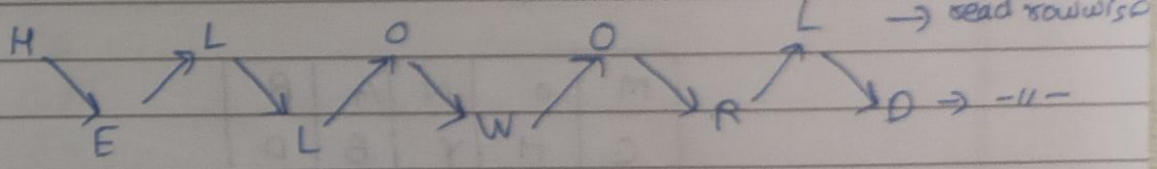
HE col col2

LL HLOOL ELWRD

OW

OR depth = 2

LD



Cipher : HLOOL ELWRD

e.g. 2) Generalize to n columns.

n = 3.

HEL
LOW
ORL
DXX

padding

Lab: Decoding the cipher text with brute force.

- Monoalphabetic Substitution Cipher
  - every letter is replaced by single letter.
  - mapping is one-to-one
  e.g. a → e
  b → z

- Polyalphabetic Substitution Cipher
  - one letter can be replaced with different characters.

- Playfair Algo.

I/P : Plaintex , Key.

Key = MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

1) Write key without duplicate, row wise
2) Now write remaining characters from alphabets.
3) i/j
4) Plaintext encrypted 2 letters at a time.

5) If a pair is a repeated letter, insert filler like 'X'
6) If both letters are in same row of matrix, then replace by next letters (last char circular).

Find out cipher text
Plaintext: TREE IS GREEN
Key: ENVIRONMENT

E	N	V	I/J	R
O	M	T	B	C
D	F	G	H	K
L	P	Q	S	U
W	X	Y		

E	N	V	I/J	R
O	M	T	A	B
C	D	F	G	H
K	L	P	Q	S
U	W	X	Y	Z

TR
EX
EX
IS
GR
EX
EX
NX

12/08/24
Monday

HCI : Schneidesman's 8 golden rules.

1) Strive for consistency
2) Enable frequent users to use shortcuts.
3) Offer informative feedback for every user action
   - use overlays
   - use focus
4) Design dialogs to yield closure.
5) Error prevention & handling
6) Permit easy reversal of actions (undo)
7) Provide internal locus of control.
8) Reduce short-term memory load.

13/08/24
Tuesday

C&NS

- Vigenere Cipher.

key → deceptive.

plaintext → wearediscoveredsaveyourself
+ deceptivedeceptivedeceptive
Ciphertext → zicvtwq

a + d = 25 ⇒ z
e + e ⇒ 8 ⇒ i

0	1	2	3	4	5	6	7	8	9	10
a	b	c	d	e	f	g	h	i	j	k

11	12	13	14	15	16	17	18	19	20
l	m	n	o	p	q	r	s	t	u

21	22	23	24	25
v	w	x	y	z

Make key length same as plaintext

- Product Ciphers (Substitution + Transposition)

- Unconditional & Computational security.

MoD II (Symmetric Key Cryptography)

Modern Ciphers → Bit Oriented
Stream cipher or Block cipher

DES - 64 Bits } Block
AES - 128 Bits } Ciphers.

Data Encryption Standard (DES)

14/08/24 Wednesday

ISEI → Assignment - Describe any 4 principles of management - on WCE assignment sheets - Last date 8th sept.

1) Communication
2) Empathy
3) Stress Management
4) Conflicts Resolution

DMPG

- Building Blocks of Disaster Recovery
1) Global Clusters
2) Wide area connectors
3) Heartbeats
4) Private Networks
5) Configuration.

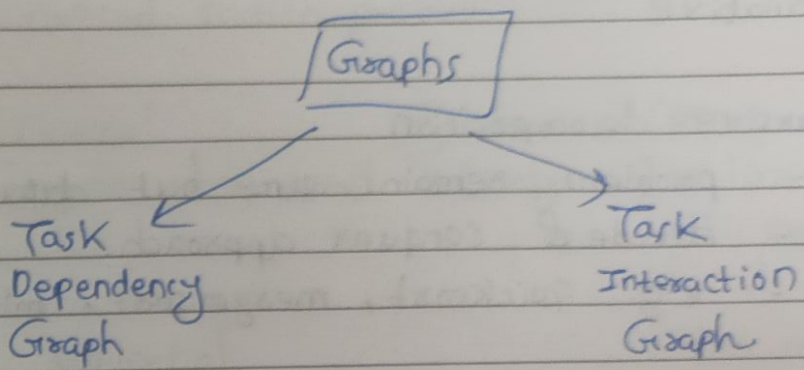
HPC

- Degree of Concurrency : Number of tasks that can be executed in parallel is the degree of concurrency of a decomposition.

- Critical Path Length - A directed path in the task dependency graph represents a sequence of tasks that must be processed one after the other.

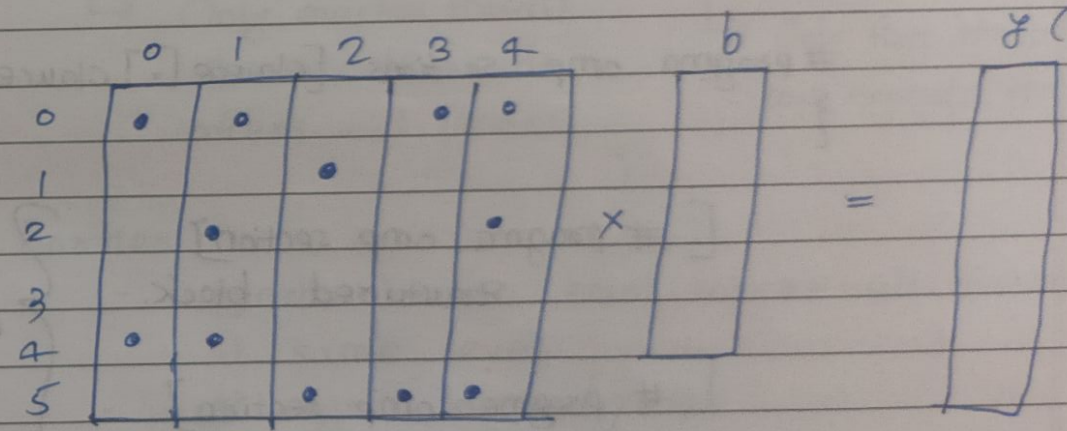
We consider longest path. (bet" starting & ending nodes)

Average degree of concurrency = $\frac{\text{Total work done}}{\text{Critical path length}}$.



16/08/24
Friday

Sparse matrix & vector multiplication.



- Processes & Mapping:
  - must minimize parallel execution time by:
    1) mapping independent tasks to diff^{n} processes.
    2) assigning tasks on critical path.
    3) map dense interactions to the same process.

• Decomposition Techniques
- Recursive
- Data
- Exploratory
- Speculative

(1) Recursive decomposition
- problem remains same but data size changes
- divide & conquer approach.
- e.g. quicksort, merge sort, min. max nos.

HPC Lab Session

Work sharing: Sections.

```
#pragma omp sections [clause[,] clause] ...
{
    [#pragma omp section]
        structured block.
    [#pragma omp section]
        -11-
}
```

} Blocks are independent.

Synchronization

Why ?
- race conditions
- critical section problem.

(1) Critical (# pragma omp critical)
↓
Problem becomes sequential

(2) Atomic (#pragma omp atomic) (only single line can be executed sequentially)
↓
H/w support.

- Master & ~~Fors~~ Single Constructs
  - → Only master thread executes the code, others will ignore
  - → Only first thread will execute the section.

- Barriers
  - synchronization point where all threads are at same level.
  - # pragma omp barrier

- Reduction Clause (for ease of programming)

  reduction (operator / intrinsic : varlist)

• Tasks → are sections but can be scheduled dynamically

19/08/24 ~~Monday~~

AF

Mod 3: Cost Accounting

Price = Total cost + Profit

Cost = Amount required to produce an item. (e.g. raw materials, labour cost, etc).

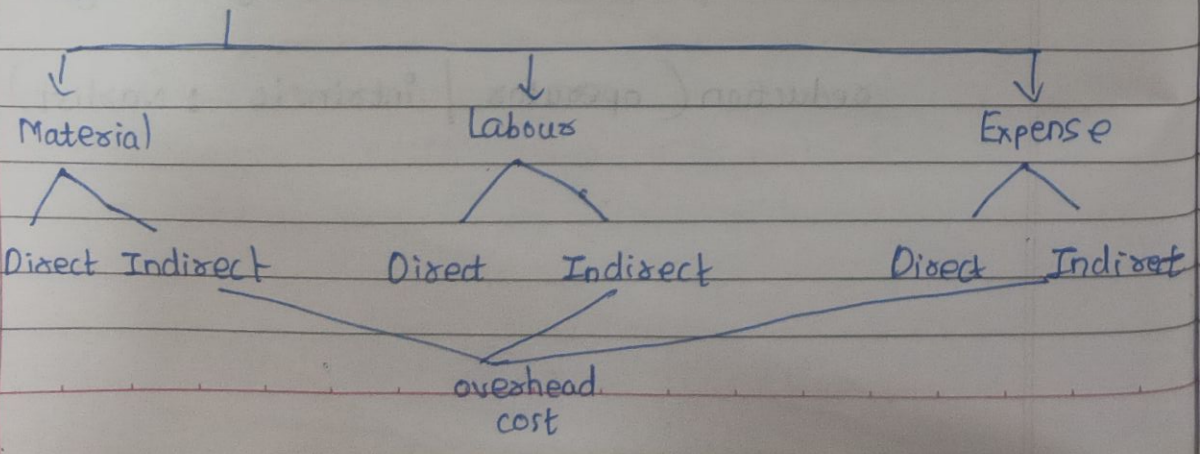
Cost Accounting

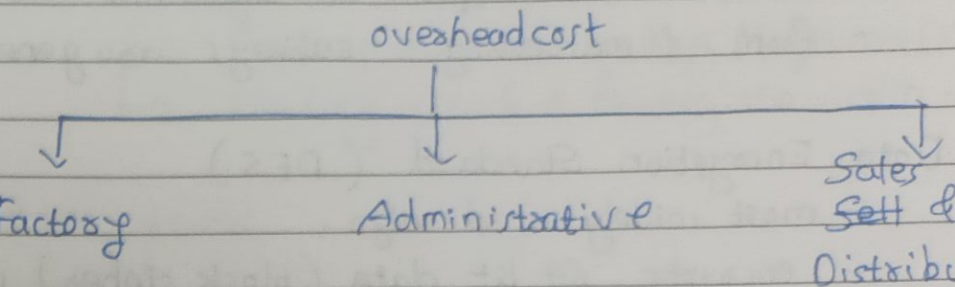
1) Involves recording, analyzing, reporting of company's cost (total cost, cost per unit, actual cost, production)

Significance of Cost Accounting

1) Cost Control
2) Analysis of Profit
3) Pricing Decision
4) Inventory Mgmt.
5) Decision Making
6) Process of Improvement

Elements of Cost





Further Overheadcosts:

i) Fixed Overhead Cost → eg. rent → regardless of volume of prodⁿ, this cost needs to be considered.

ii) Variable Overhead Cost → Change according to seasons & time periods. → Depends on prodⁿ volume

- Importance of understanding elements of cost.

1) Accurate costing
2) Pricing Decision
3) Profitability Analysis
4) Inventory Valuation
5) Performance Evaluation.

CNS

- Feistel Cipher
  - based on concept of invertible product cipher.

Partitions input block into 2 halves. Process through multiple rounds which perform a substitution on left data half based on round function of right half & subkey then

- no. of rounds depend on algorithm.
- from 1 masterkey, subkeys are generated.

• Data Encryption Standard (DES)
- most widely used algo.
- encrypts 64 bit data (block cipher) using 56 bit key.
- Developed by IBM as Lucifer cipher
- after revisions, Lucifer cipher evolved as DES.
- Symmetric Key block cipher algorithm.

HCI (MOD 3)
- Cognitive models
- Cognitive Complexity Theory (CCT)
- Keystroke Level Model (KLM)
  - key bounce time

20/08/24 Tuesday

~~CBPTS~~ DMPG [MOD 3]

Data Threats & Data center Security

1) Denial of Service (DoS)
2) Man in the middle (MITM)
3) Unintentional data loss
4) Repudiation
5) Malicious attack.

Types of DoS
- Teardrop attack → sending illegitimate data
- Flooding attack → flooding the victim with data

MITM attack

Interception
- IP spoofing
- ARP -"-
- DNS -"-

Decryption
- HTTPS spoofing
- SSL Beast
- SSL Hijacking
- SSL Stripping

- Threat Modeling
  - identify & enumerate potential threats & prioritize security mitigations.

Elements:
1) Assets → what valuable data & equipment should be security?
2) Threats → what attacker can do to the system?
3) Vulnerabilities → what are the flaws in system?

Steps to threat modeling
i) Identify asrets
ii) Outline arch.
iii) Break down application
iv) Identify threats
v) Classify & structure threats
vi) Rate severity

21/08/24 Wednesday

HCI

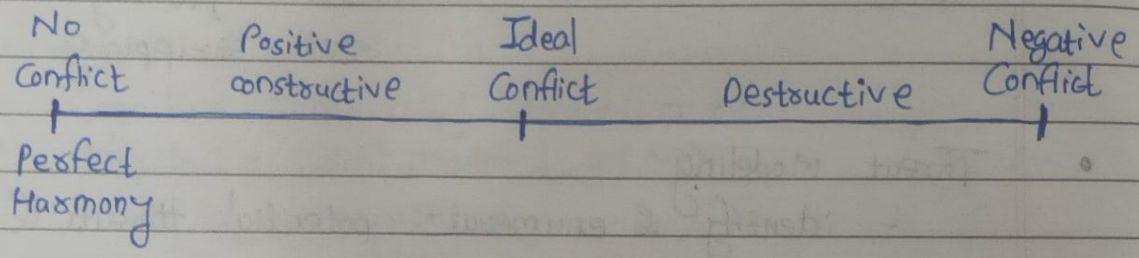
Ethnography : User behaviours.

HTA → Hierarchical Task Analysis

23/08/24 Friday

HRW

- conflict management.
  - → situational (based on situation)
  - → process conflicts (long lasting problems)



Constructive Conflicts	Destructive Conflicts
- supportive to goals	- performance decline
- helps in improvement of performance	- abusive language
- personal wellbeing	- gossips / rumors.
- respect for other's opinion	- personal comments
- communication in +ve way	- silence
- problem solving	- stress
- increased awareness	

HPC

Exploratory Decomposition
- tile puzzle

1	2	3	4
5	6	●	8
9	10	11	12
13	14	15	16

empty tile

1) Data Decomposition
2) Recursive -11-
3) Exploratory -11-
4) Speculatory -11-

- Anomalous Computations

- Speculative Decomposition
  - dependencies are not known a-priori.
- Hybrid Decomposition.

Task Generation

Static Task Generation
↓
we know how many task would be there
↓
data & recursive decomp^n

Dynamic Task Generation.
↓
we don't know how many tasks would be there a-priori
↓
exploratory & speculation decomp^n.

26/08/24
Monday

A & F (Mod 2)

- Preparation of Financial Statements.

At a specific point of time shows financial snapshot
- Performance

1) Income statement (Profit/loss statement)
2) Balance Sheet (assets/ liabilities / equity profit)
3) Cashflow Statement (inflow/ outflow of cash)
4) Statement of changes in equity

- Steps for preparing financial statements
1) Gather financial data
2) Record Transactions (book keeping)
3) General ledger entry (collective transaction writing)
4) Adjusting entries
5) Trial Balance
6) Financial Stmt (final stmt)
7) Analysis Stmt (summary)

- Importance of financial statements
1) Decision making
2) Investor Relations
3) Creditor
4) Tax purpose

- Sole Proprietary
- one single person owner of the firm & operator of the firm.

Characteristics

1) Single ownership
2) Unlimited liabilities
3) Easy setup
4) Taxation (Personal vr Business tax)
5) Control

Balance Sheet: Snapshot of company's financial health & performance

i) Assets (owns) ii) Liabilities (owes)
iii) Investment (equity)

Fundamental Equation

Assets = Liabilities + equity

Assets

- Current → Immediate liquidity
- Non Current → Have long term value → Not easily convertible to cash.

Liabilities

- Current → debts must be paid every year → Short term loans
- Non-Current → Long term loans

Equity → Owner's investment.

Left Side → Assets = Right side → Liabilities + Equity

Current assets	= 10,000	Accounts Payable	= 8,000
Amount Receivable	= 5,000	Salary	= 2,000
Inventory	= 8,000		
Prepared Exp	= 2,000	Total Current liabilities	= 10,000
Total assets (current)	= 25,000	Note payment	= 10,000
Equipment	= 20,000	Total liability	= 20,000
Depreciation	= 5,000		
Net Equipment	= 15,000	Owner's Equity	= 20,000
Total Assets	= 40,000	Total	= 40,000

always equal

1) Objective ques (mcq) (5M)
-11- (mcq) (1M)
2) Answer in short (6 to 7 M)
3) Descriptive (6 to 7)
4) Descriptive (6 to 7)

KDC → Key Distribution Center.

D D M M Y Y Y Y

CNS (Mod 3: Public Key Cryptography & RSA)

Private key Cryptography (Symmetric keys)

- Sharing key is concern.

- Public Key Cryptography
  - coe use 2 keys
  - complements the private key

Public key can be used to encrypt msg & verify signature

Private key is used to decrypt the ~~key~~ msg at the receiver side.

- Infeasible to determine private key based on public key.

Algos: RSA, Elliptic Curve, Diffe Hellman, DSS.

RSA Algorithm

Rivest, Shamir, Adleman (MIT)

$P_U = \{e, n\}$, $P_R = \{d, n\}$

M = Plain text C = Cipher text

Encryption $C = m^e \bmod n$

Decryption $M = c^d \bmod n$

Key Generation

1) Select 2 large prime numbers p & q.
2) Calculate $n = p \times q$
3) Select int e such that $gcd(\phi(n), e) = 1$
   where, $\phi(n) = (p-1) \times (q-1)$
4) Calculate d
   $d \times e = 1 \bmod (\phi(n))$

HCI

Diff^n bet^n Dialogue & Forms

Dialogue → limited data
Forms → huge amount of info

State Transition Networks (STN)
- circles / states
- arcs - actions / events

JSD Diagrams (Jackson's Structured Design Diagram)

CNS

Diffie Hellman Key Exchange Algorithm
- used for key exchange
- public key algo.

① Select prime number p.
Select α, 'α' is primitive root of p.
(α & p → global public)

'α' is primitive root of p iff
$\alpha \bmod p$,
$\alpha^2 \bmod p$,
⋮
$\alpha^{p-1} \bmod p$
} Generates unique set of nos. from 1 to $p-1$.

eg. $\alpha = 3$, $p = 7$.

$3 \bmod 7 = 3$
$3^2 \bmod 7 = 2$ set = {1, 2, 3, 4, 5, 6}
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$

② User A key generation
Select private X_A ... $X_A < p$
Compute public $Y_A = \alpha^{X_A} \bmod p$.

③ User B key generation
Select private X_B ... $X_B < p$
Comput public $Y_B = \alpha^{X_B} \bmod p$

④ Calculate secret key by user A.

$$K = (Y_B)^{X_A} \bmod p.$$

(5) Calculate secret key by B.

$K = (Y_A)^{X_B} \bmod p$

Both K's are same.

DMPG

IMP
- What is meant by threats. what are its types?
- Elements of threat modelling.
- Steps to threat modeling
- What is authentication & authorization?

Access Control Models

i) Discretionary access control (DAC)
ii) Mandatory -r- (MAC)
iii) Role based access control (RBAC)
iv) Attribute-based access control (ABAC)

Mod 2

Cloud Storage (what is) & its types.
Data centers (def^n, eg, adv, disadv)
Disaster Recovery

Mod 1

What is data, give its sources
What is DLM?

RM

MOD 1 { What is Research, what are its types?
What is literature review?

MOD 2 { What do you mean by Research design & its importance & need (5 M)
Measurement & scaling techniques & types
Processing & analysis

MOD 3 Quantitative techniques