9

Dijkstra's Algo (single source shortest path)

10 – Google map, (work on both direct/undir)

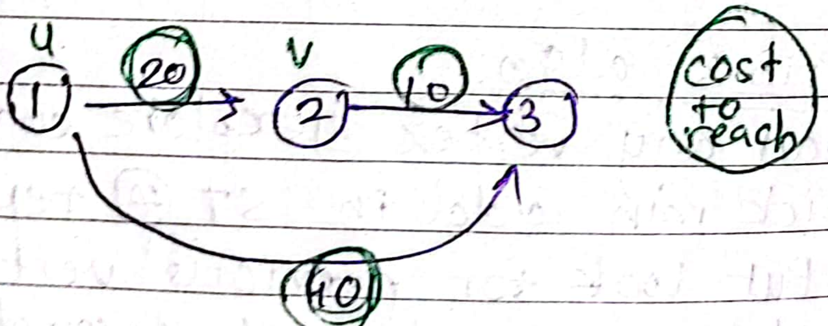
– from single source to all dest'

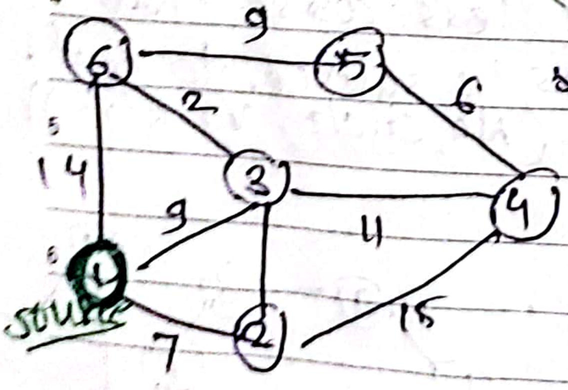
11 with minimum value.

– main :-

LUNCH if $d(u) + c(u,v) < d(v)$

1 then, $d(v) = d(u) + c(u,v)$





source 1	2	3	4	5	6
1	∞	∞	∞	∞	∞
1	7	9	∞	∞	14
1, 2	7	9	22	∞	14
1, 2, 3	7	9	20	∞	11
1, 2, 3, 6	7	9	20	20	11
1, 2, 3, 6, 4	7	9	20	20	11

... When walking through the "valley of shadows," remember, a shadow is cast by a Light.

* Kruskal's algorithm MST

- spanning tree - subgraph (connected) if, it should contains all vertices of 'G' & and (v - 1) edges & no cycle

complete graph K_4 = =

Possi. spanni T = $n^{n-2} = 4^{4-2} = 16$

- in KMST Algo - intermimideate stages may produce disconnected graph

- 2 approaches

(A) - Min heap - (sort)

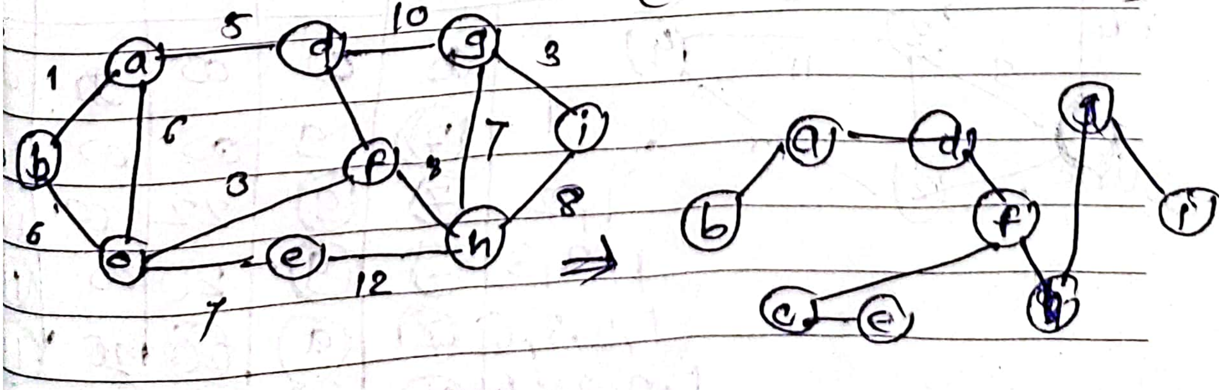
(B) pick min and add (consider Limitat'of ST)

* Prim's algo

(1) start any vertex (2) explore connect to that (3) pick min add in ST (4) repeat (2), (3)

(5) But look for previous vertex that it can also have less cost than current vertex as a source to dest.

(No cycle, V, E(V-1))



2018
WK 50 • 349-016

15
SAT
DEC

DECEMBER

M	T	W	T	F	S	S
31					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	
17	18	19	20	21	22	
24	25	26	27	28	2	

9 RSA algo - asymmetric(two key)

- p, q prime no

-10 $n = p \times q$

- $\phi(n) = (p-1) * (q-1)$

11

- $1 < e < \phi(n)$

LUNCH $e \Rightarrow$ coprime to $\phi(n)$
↳ $\gcd(e, \phi(n)) = 1$

1

- public key (n, e)

2

- $de \bmod \phi(n) = 1$

3 private key = d

$$\boxed{\begin{array}{l} de \cong 1 \bmod \phi(n) \\ d = \dfrac{1+K\cdot\phi(n)}{e} \rightarrow \text{whole no} \\ K = 0, 1, 2, \ldots \end{array}}$$

4 5

$p = 13$, $q = 17$

$n = p \times q = 13 \times 17 =$

$n = 221$

$\phi(n) = 12 \times 16 = 192$

$e = 35$

such that $\boxed{\gcd(35, 192) = 1}$

public key (221, 35)

Private key

$de \bmod \phi(n) = 1$

$d = \dfrac{1 + k\cdot\phi(n)}{e}$

for k=2, $\boxed{d = 11}$

whole no. (quotient) accept.

6

eg. HI   H = 8   I = 9

16 SUNDAY encryption:- $89^e \bmod n$
$= 1394$

decryption:- $c^d \bmod n =$ 89

Many individuals have, like uncut diamonds, shining qualities beneath a rough exterior.

Block Cipher

* DES algo (Data Encry Stand)

9 - total 16 rounds

- text size = 64 bit /plain/ cipher both

10 - key size = 48 bits

8-bits ~~removed~~ for parity (8th posi)

11 (Left circular shift) → 8-bit for rearrangement

- in each rounds ④ steps

LUNCH 1. Dividing bits ② parts - 32-32

2. Bit shuffling

1 3. Non linear substitution

4. Exclusive or operations

2 -

- left circular shift -

3 for round ① ② ⑨ 16 → shift ① bit

other shift → 2 bit

4

5

6

The whole world steps aside for the man who knows where he is going. • • •

Block Cipher

* AES algo (Adv. Encry. ~~St~~ Stand) :- (10 R

- It has input array, state Array & key arr

(1) Input array (4X4) 16 cells → 8 bits each
Total = 16 X 8 = 128 bits = 4 words
Plain text is represent in this

(2) state array → to store intermediate state
intermediate stages (4X4)
10 Rounds

(3) key array → 4 words → input
↳ expanded into 44 word
each round → 4 words
= 10 rounds X 4 words
= 40 + 4 (~~for~~ add. Round key)
= 44

COLUMNS REPRESENT a WORD

input for round → 128 bit plain text & 4 words

Round = 10 & 10
E D

1. substitute Byte
2. Shift Rows
3. mix column
4. Add round Key → XOR

*MD5:- produce 128 bits MD.

→ working:-

9 ① padding:- such that total length is 64 bit less than exact multiple of 512.

10 e.g. msg = 1000 bits + padding

11 = 1000 + $\boxed{472}$

$512 \times 3 - 64 = 1472 - 1000 = \boxed{472}$

LUNCH msg = 1472

1 ② appending :- Append original length before padding.

2 calculate length % 64 = 64

∴ append 64 bits

3 ③ Dividing msg - each 512 bits

4 ④ Initializing:- (4 chaining variables) 32 bit each

5 A, B, C, D, → predefined value.

6 ⑤ Processing: 512 bit blocks

1. copy chaining variables in corresp. variables

A = a, B = b, C = c, D = d

2. Divide 512 block into 16 - 32 bit blocks

2018

WK 50 • 345-020

11

TUE

DEC

DECEMBER

M	T	W	T	F	S	S
31					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	2
24	25	26	27	28	29	30

2

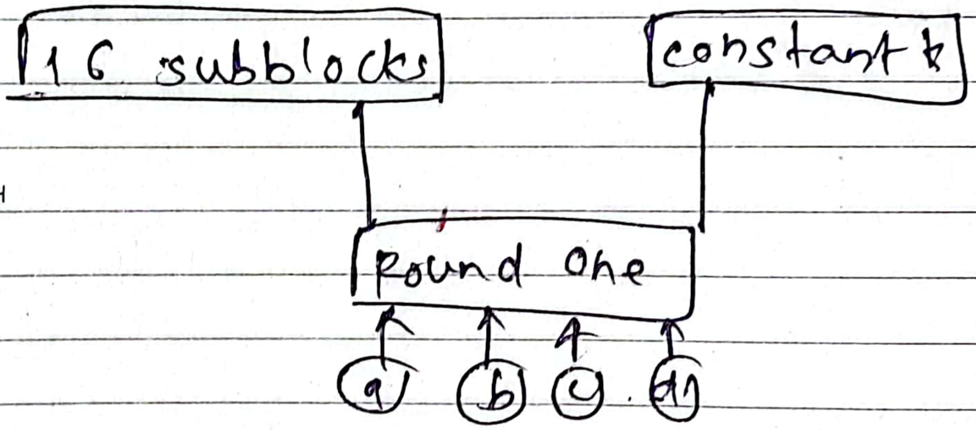
9 3. Four rounds:-

- 16 subblock of a block(512bits)

10 - a constand.

11

LUNCH



1

2

$$a = b + ((a + process, p(b,c,d) + m(i] + T[k)$$

3

4

5

6

Putting off an easy thing makes it hard, and putting off a hard one makes it impossible.