unit test -03

(1) Link State Algorithm:

The ~~net~~ network topology and all link costs are known that is available as a input to the LS algorithm. Each node broad cast link state packets to all other nodes in the network, with each LS packet containing the identities and costs of attached links.

Dijkstras algorithm computes the least-cost path from one node to all other nodes in the network.

~~D(v) is~~ D(v): cost of the least cost path from the source to destination.

p(v): previous node along the current least cost path.

N: subset of nodes.

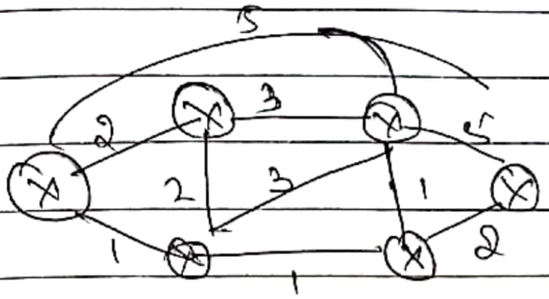
Initializations!

```
N' = {u}
for all nodes v
    if v is a neighbour of u
        then D(v) = c(u,v)
    Else
        D(v) = ∞

Loop
    find w not in N' such that D(w) is a minimum
    add w to N'
    update D(v) for each neighbour v of w & not in N':
        D(v) = min (D(v), D(w) + c(w,v))
```

until N' = N

Eg:-

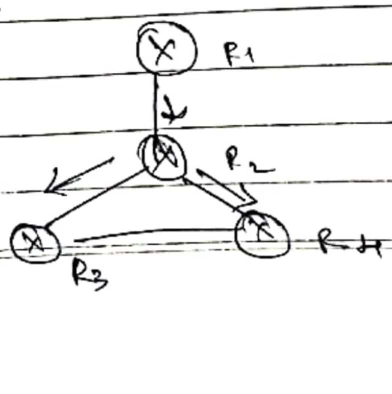


Step	N'	D(v), p(v)	D(w), p(w)	D(x), p(x)	D(y) p(y)	D(z), p(z)
0	u	2, u	5, u	1, u	∞	∞
1	ux	2. u	4. x		2. x	∞
2	uxy	2. u	3. y			4. y
3	uxyv		3. y			4. y
4	uxyvw					4. y
5	uxyvwz					

The currently known least cost paths from u to its directly attached neighbours, v, x & w are 2, 1 & 5. y & z has ∞ cause they are not directly attached. In Every iteration the least cost path for each variable is found.

② uncontrolled flooding:

when a node receives a broadcast packet, it duplicate the packet and forwards it to all of its neighbours. If graph is connected, this scheme will eventually deliver a copy of the broadcast packet to all nodes in the graph,



R_2 will flood to R_3, R_3 will flood to R_4, R_4 will flood to R_2 and R_2 will flood again to R_3 & so on. This creates endless cycling of two broadcast packets, one clockwise, and one counterclockwise.

controlled flooding:

① In sequence number controlled flooding:

Each node maintains a list of the source address and seq no. of each broadcast packet it has already received, duplicated. It first checks ~~with~~ whether the packet is in this list. If so, the packet is dropped. If not the packet is duplicated.

② RPF:

When a router receives a broadcast packet with a given source address, it transmits the packet on all of its going links only if the packet arrived on the link that is on it's own shortest path back to the source. Otherwise, the router simply discards the incoming packet without forwarding.

unit test -04

② RSA algorithm :

Assume that a plaintext m must be encrypted to a cipher text c

This has three phases.

① Key generation :

→ choose two plain numbers a & b & compute n = a . b

→ find n. Select Encryption key x, Such that x & (a-1)(b-1) are relatively prime.

→ find y. Calculate decryption key y

$$xy \bmod (a-1)(b-1) = 1$$

→ a & b Can be discarded.

→ public key = $\{x, n\}$

→ private key = $\{y, n\}$

② Encryption :

→ Both Sender & receiver must know the value of n

→ The sender knows the value of x & receiver knows y

→ ciphertext c is constructed by

$$c = m^x \bmod n$$

③ Decryption :

given the ciphertext c, the plain text m is extracted by

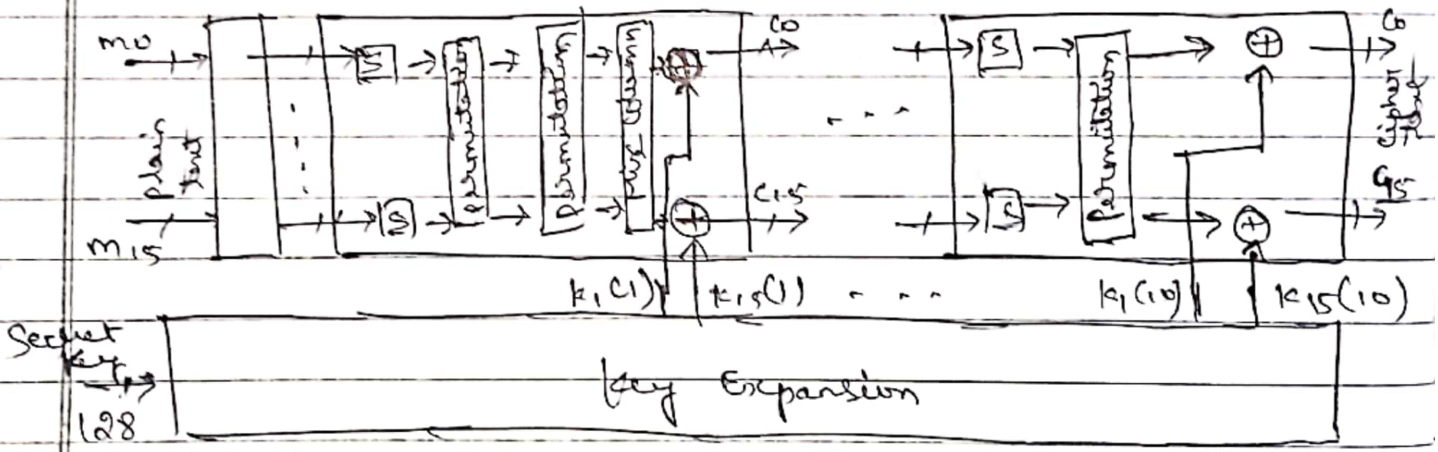
$$m = c^y \bmod n.$$

③ AES :

- AES has better security strength than DES.
- In AES message is divided into 128 bits blocks & it

uses 128 or 192 or 256 bit key.

- The plain text is formed as 16 bytes mo through m15 and is fed into round 1 after an initialization Stage.
- In this round, substitute - units (S) perform a byte by byte substitution of blocks.
- The ciphers move through a permutation - stage to Shift rows to mix columns.
- At the end of this round, all 16 blocks of ciphers are Exclusive OR. with the 16 bytes of round 1 key ko(1) to k15(1)



unit test-05

③ multi media applications are classified into three types.

(i) streaming stored audio / video

(ii) conversational voice / video -over-IP

(iii) streaming live audio / video.

Streaming live audio / video :-

- These applications allows a user to receive a live audio or video such as live sporting event, news event etc.
- Today, thousands of radio & television stations around the world are broadcasting content over the internet.
- Live, broad-cast like applications often have many users who receive the same audio / video program at the same time.
- Although the distribution of live audio / video to ~~many~~ many receivers can be efficiently accomplished by IP multicasting techniques, multicast distribution is more often accomplished today via application layer multicast.

② Dynamic adaptive streaming over HTTP, the video is encoded into several different versions, with each version having a different bit rate and correspondingly a different quality level.

- with DASH, each video version is stored in HTTP server, each with a different URL.
- The HTTP server also have a manifest file, which provides a URL for each version along with its

bit rate.

- while downloading chunks, the client also measures the received bandwidth and runs a rate determination algorithm to select the chunk to request next.
- If the client has a lot of video buffered and if the measured receive bandwidth is high, it will choose a chunk from a high-rate version.
- By dynamically monitoring the available bandwidth and client buffer level, & adjusting the transmission rate with version switching, DASH can often achieve continous playout at the best possible quality level without frame freezing or skipping.