VIT Vidyalankar Institute of Technology
(Accredited A+ by NAAC)
(Autonomous Institute Affiliated to University of Mumbai)

Mid Semester Examination

Branch	Date	Sem.	Roll No. / Exam Seat No.	Subject	Student's Signature	Junior Supervisor's Name and Sign
CMPN	8/4	6		CSS		

Question No.	A	B	C	D	E	F	G	H	Total	Total out of (20 /30 / 40)
1										
2										
3										
4										

Examiners Signature	Student's Sign (After receiving the assessed answer sheet)

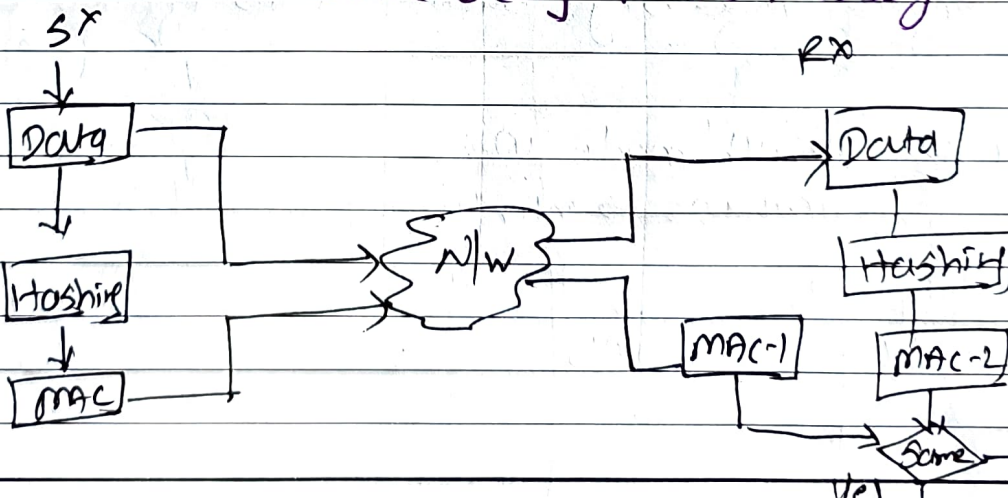
CSS Monday Test - 3
Paper solution
Amit K. Nerurkar

Q1

a.

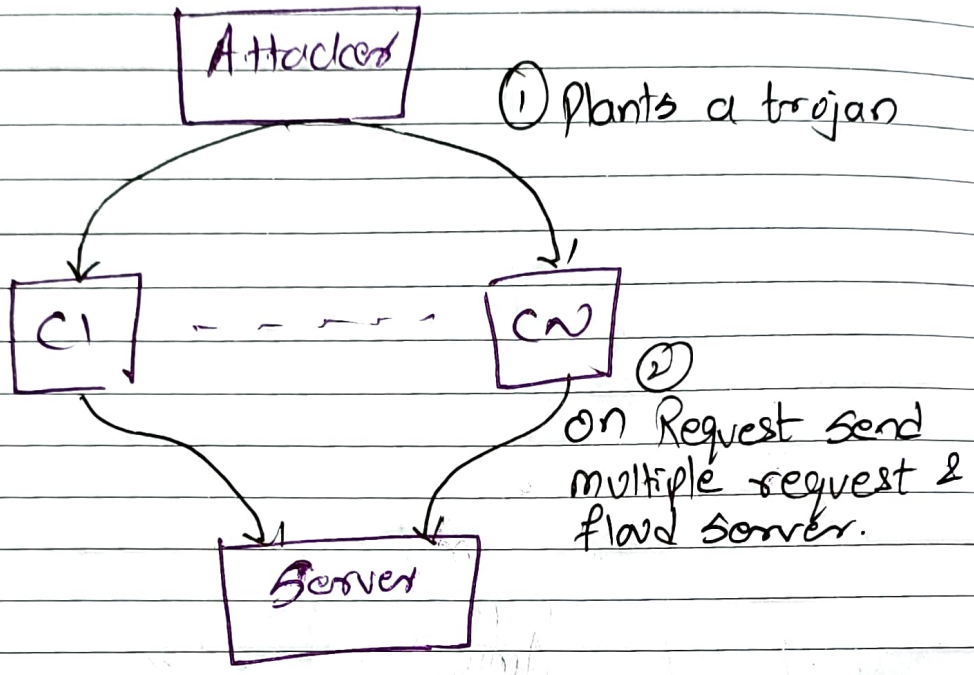
Parameter	~~MD~~5	SHA
Size	128 bits	160 bits

b. MAC [Message Authentication Code]: It checks authenticity of the message.



c. DDoS attack

Distributed Denial of Service:

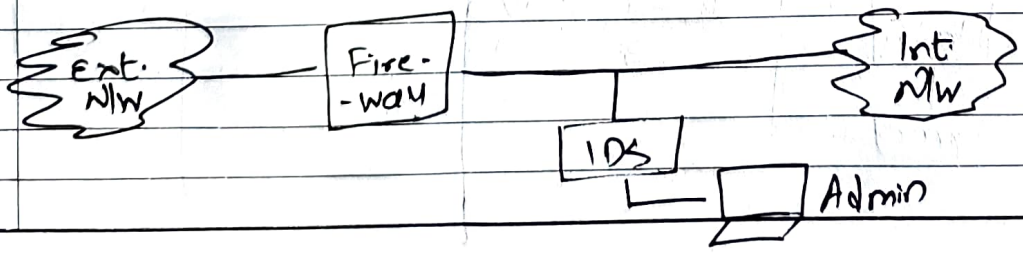


Attacker ~~have~~ plants a trojan in the clients (random) & when it gives signal, it will start flooding server with multiple request

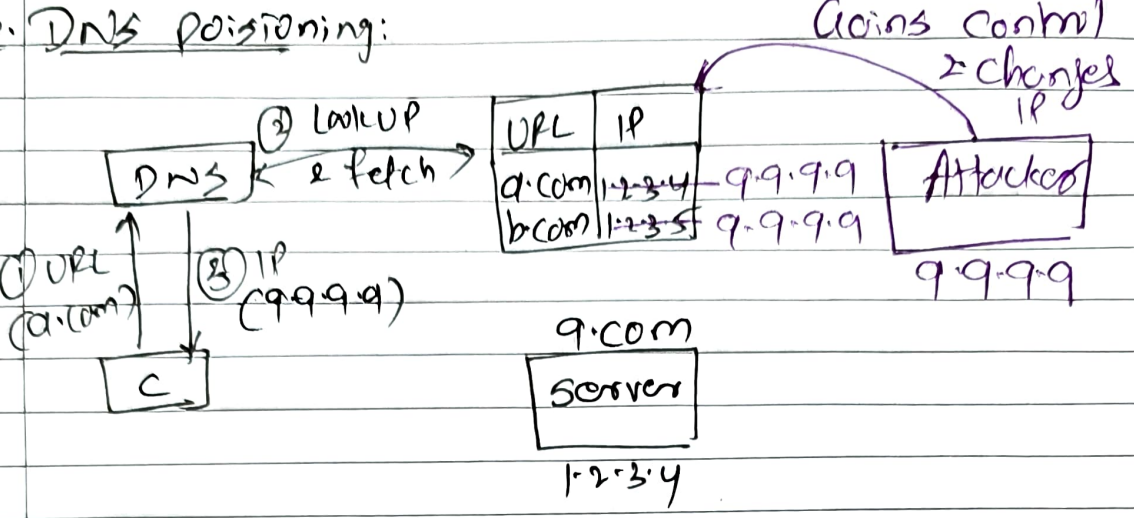
Since server is not able to identify ~~from~~ ~~where~~ ~~those~~ single source it is called as DDOS.

d. Use stealth mode IDS:

~~that~~ IDS is intentionally shifted to other n/w.

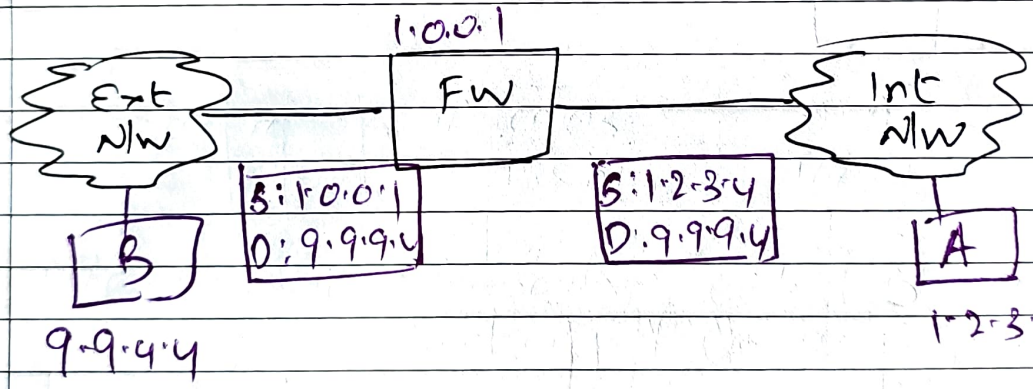


e. DNS poisoning:



As shown, Attacker gains control on DNS & modifies IP in DNS cache with its own IP, this makes DNS always giving IP of attacker.

f. It has to use NAT [Network Address Translation]



While packet going out ~~we~~ Firewall will change SIP with its own IP making outsider to be hidden of actually IP.

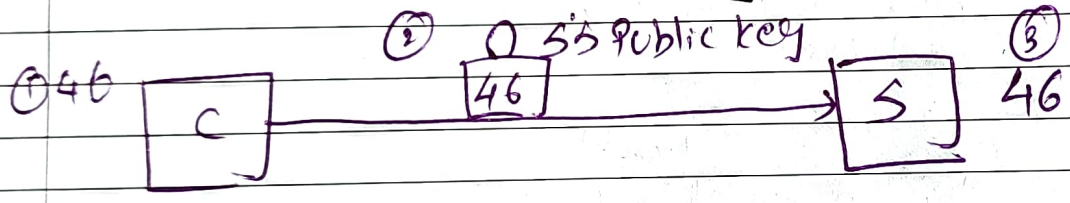
g SHA-1 needs 5 chaining variable of size ~~16 bits~~ 32 bits each.

A, B, C, D, E

h. SSL uses symmetric keys, when client verifies the Digital certificate of server, it creates random no. called session which is encrypted using server's public key.

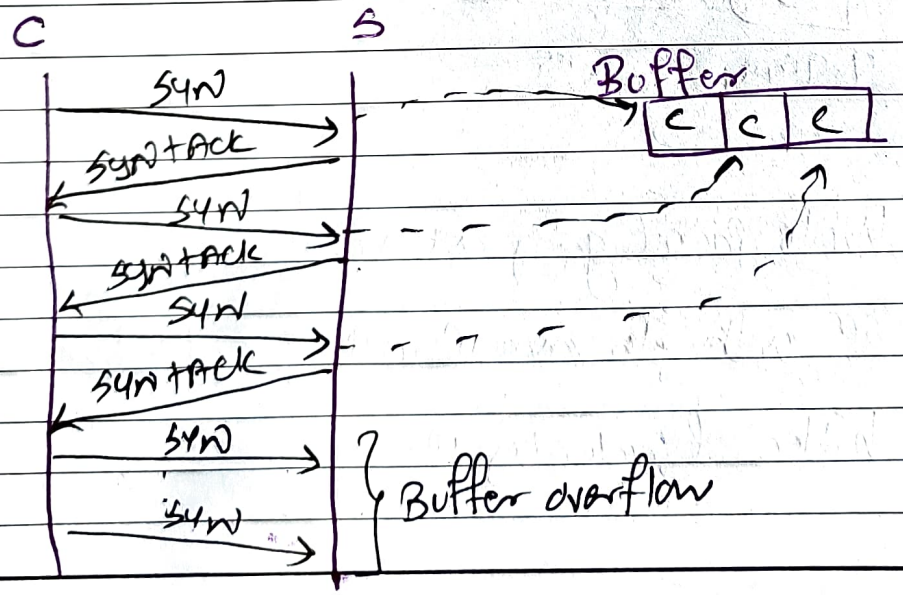
Server receives this decrypts using server's ~~public~~ private key & server gets session key.

Henceforth any data sent or received will be encrypted or decrypted using session keys.



Q2

a.

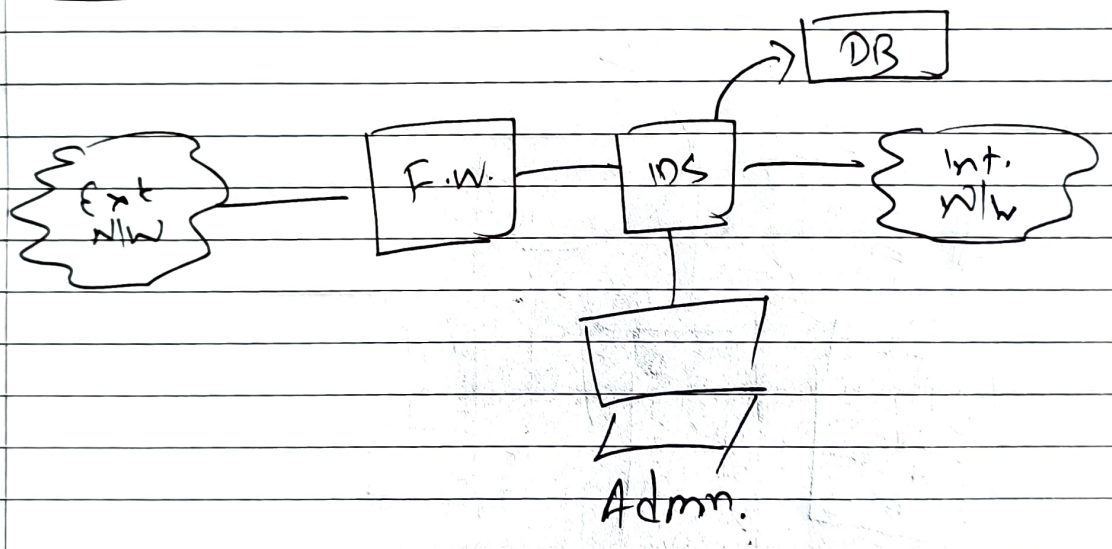


- Client sends SYN packet & Server enqueues client's information in Buffer & sends SYN + ACK.

- Client should send SY ACK but intentionally keeps sending SYN & finally it floods the server ultimately causing DoS attack.

- Server's buffer is now full, causing overflow attacks & finally it is making Server unavailable for giving any service.

Identification of ~~Do~~ SYN flooding:



- Intrusion Detection System is used for analysing the packets ~~with~~ which are bypassed by Firewall.

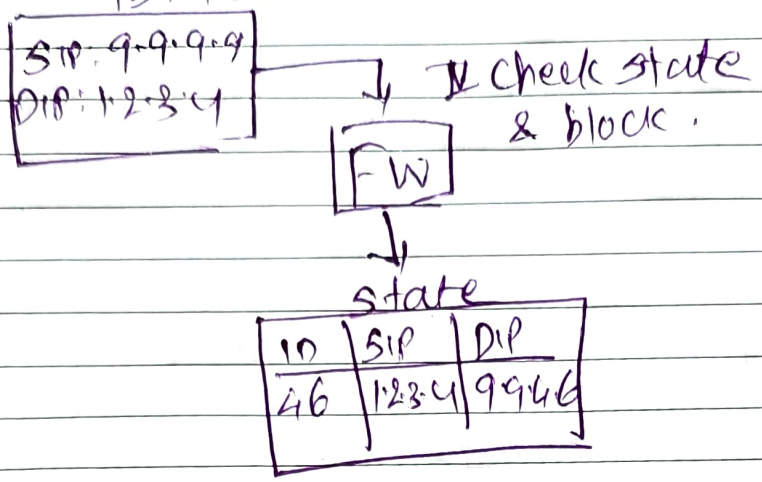
- Packets of SYN (multiple) coming inside is referred by by Database for signature, it imm. notifies admin about the same.

Q2

b: Stateful Inspection Firewall:

As shown when the packet goes out, firewall checks the Rulebase & if packet is allowed to go out it enters packet details in state. When reply comes back the firewall checks data & decides to accept or block the packet

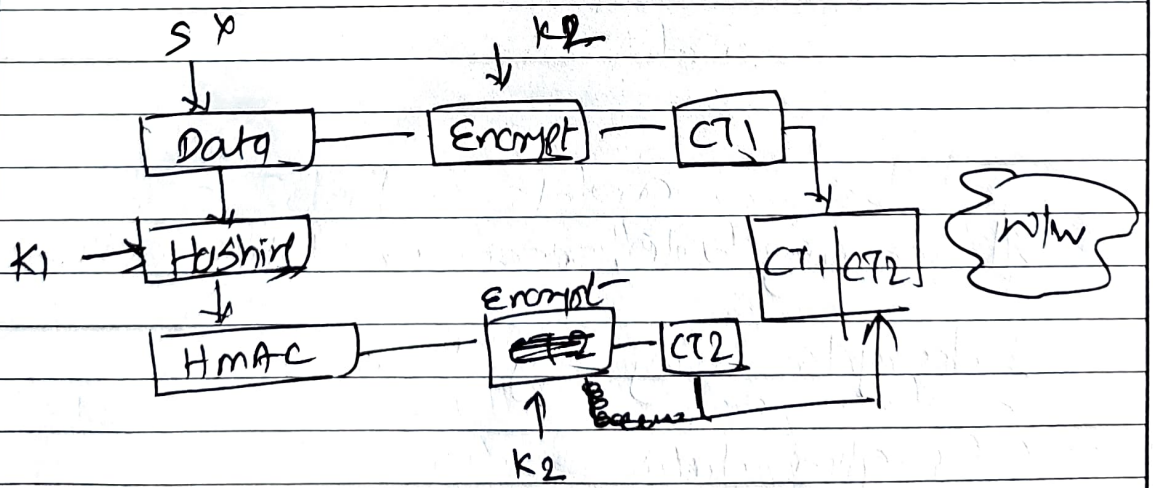
III ID=46



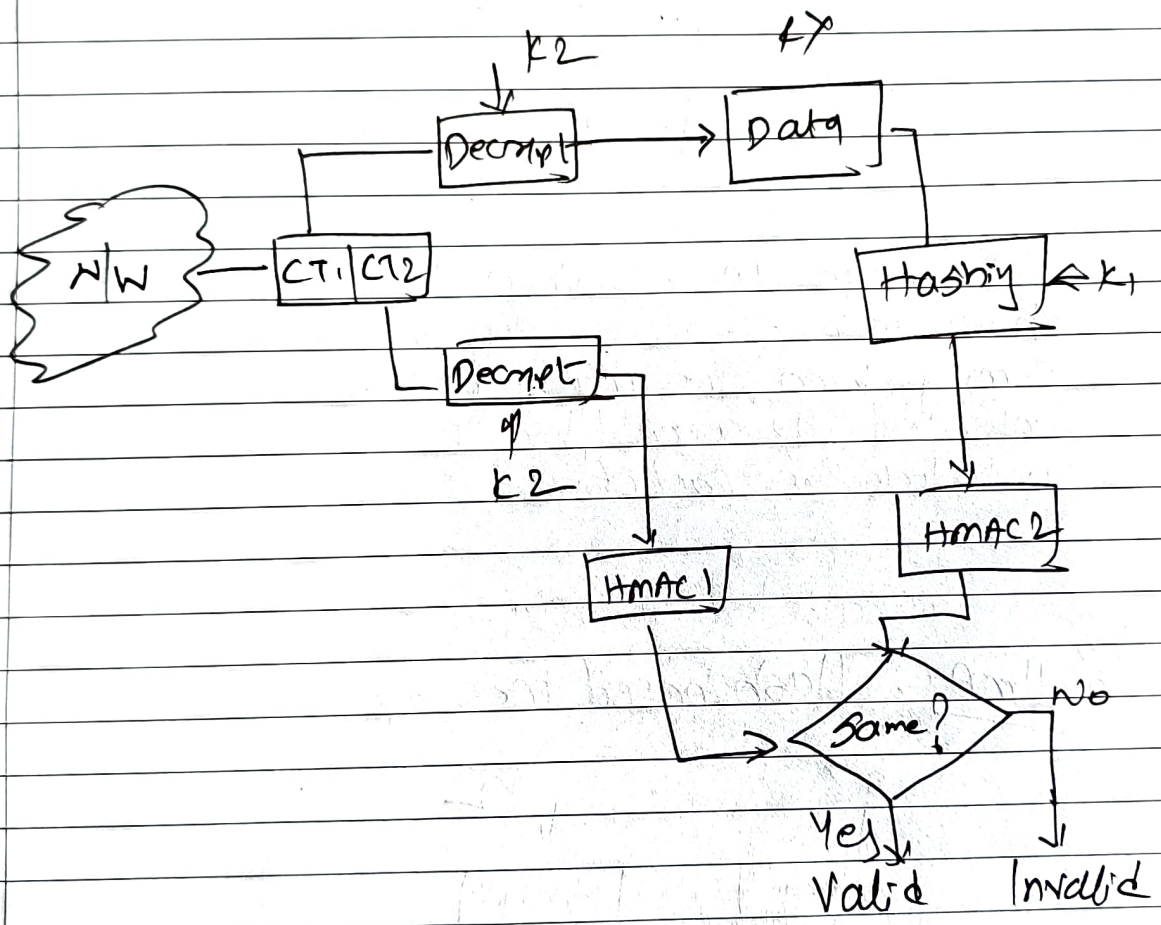
As shown above, when the packet is coming back ~~with SO~~ as reply with 2 if it is not coming from the machine from where it is intended to come then Firewall checking state will block the packet.

Q3

a. HMAC: Hash based message Authentication Code



- As shown above, the message is hashed using key K1.
- HMAC & message is encrypted using key K2 which gives two parts of cipher text (CT1 & CT2)
- CT1 & CT2 is sent on a network.



At receiving side, receiver takes CT1 & CT2 & decrypts using key K2.

CT1 gives data

CT2 gives HMAC called as HMAC 1.

On data again apply hashing using Key K1 & this will give HMAC called as HMAC 2.

If HMAC 1 & HMAC 2 are ~~there~~ same then message is correct.

Q3

b Message Digest:

I Perform padding to make message multiple of 512 less 64.

eg. Message = 1000 bits

∴ use 3 blocks of 512 ie 512 x 3 = 1536

II Padding length calculation

Padding = 1536 - 64 - 1000 = 472 bits.

Salt Message padding.

III Divide above message into blocks of 512 bits.

① B1

② B2

③ B3

IV Initialize 4 chaining variables each of 32 bits

A, B, C, D

∴ A = a

B = b

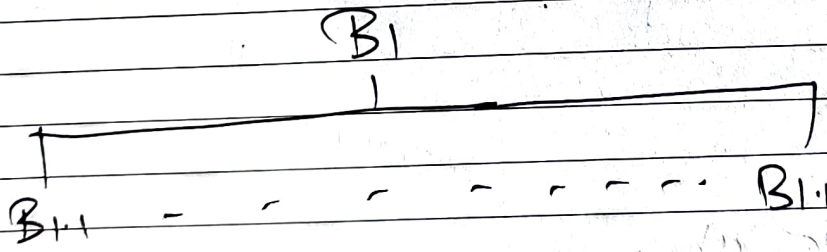
C = c

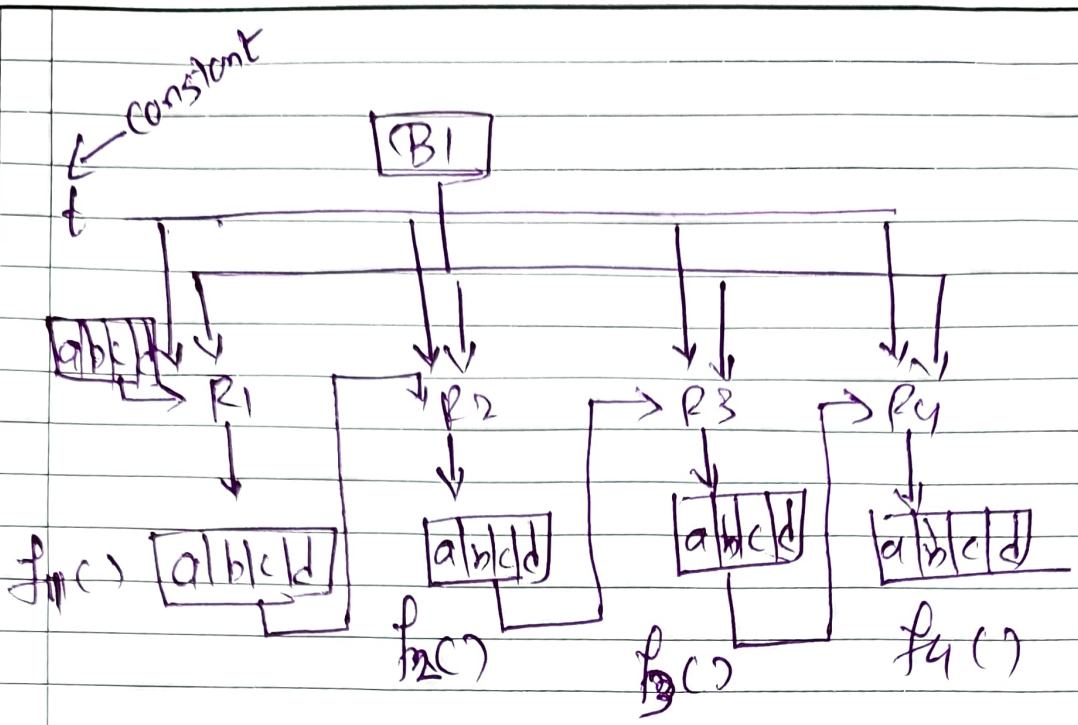
D = d

Total Buffer / Chaining variables = 4 × 32 = 128 bits.

V Each block of 512 bits will go for 4 rounds & every round has total 16 operations.

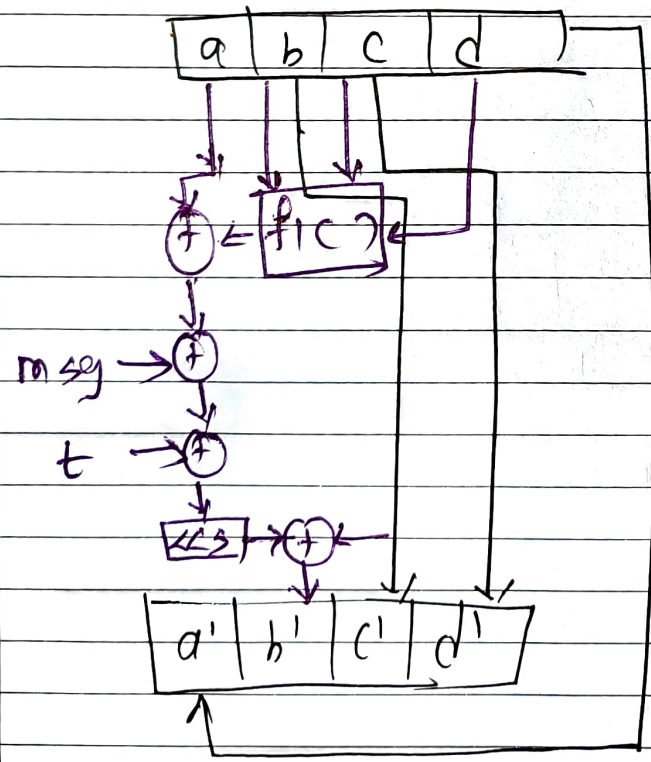
VI 512 bits block is further divided into 16 blocks each of 32 bits.





As shown above diagram shows how 4 rounds of operations are performed.

VI Every round in detailed working:



$a' = d$

$c' = b$

$d' = c$

$b' = b + [\{[a \oplus f_1(c)] \oplus msg \oplus t\} <<< 5]$