b) Definition – 1M

Requirement – 1M
(Nonrepudiation)

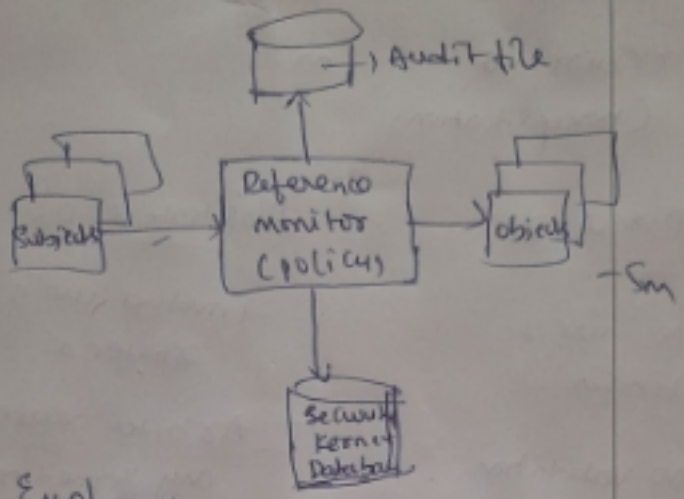
Direct DS	Arbitrated DS
No use of Arbiter	Involves use of Arbiter
No validation in b/w.	Arbiter validates any signed message – 3M
Can be implemented by private key algorithm	Can be implemented with either private or public key algorithms

7) Definition of Firewall – 01

(1) Screened host firewall, single homed bation Configuration – 3

(2) Screened host firewall, dual homed bation Configuration – 3 — 10 M

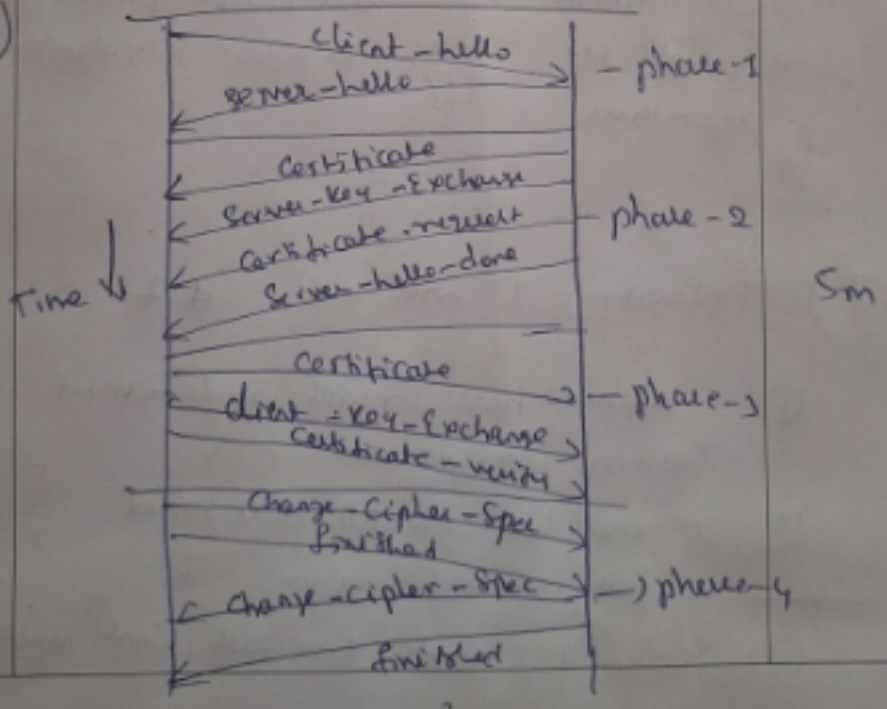
(3) Screened Subnet firewall Configuration – 3



5m

Explanation – 2m

6)



5m

4) Types of Intruders

① Masquerader

② Misfeator

③ Clandestine-user

— 4m

Types of intrusion detection systems

① Statistical anomaly detection

(1) Threshold detection

(2) profile based

② Rule-Based detection

(1) Anomaly detection

(2) penetration identification

— 6m

10M

5) Security rules — 3m

① Complete mediation

② Isolation

③ verifiability

$F(B,C,D) = (B \wedge C) \vee (\bar{B} \wedge D)$

$G(B,C,D) = (B \wedge D) \vee (C \wedge \bar{D})$

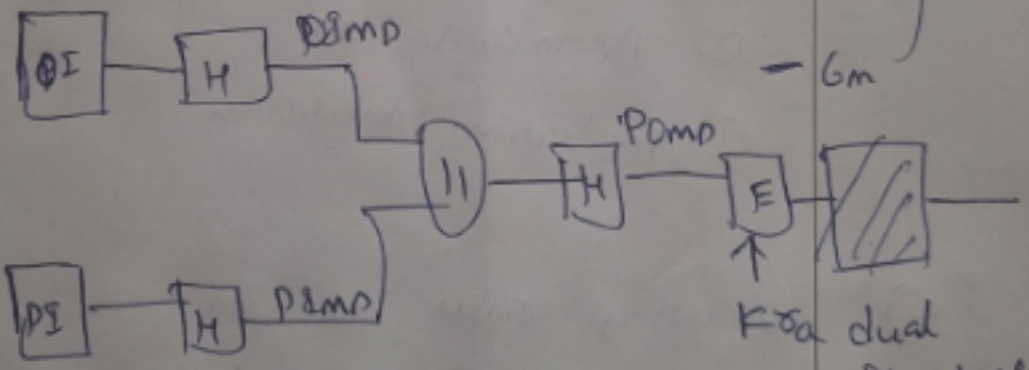
$H(B,C,D) = B \oplus C \oplus D$ — 2m

$I(B,C,D) = C \oplus (B \vee \bar{D})$

3) Dual Signatures are used to send both order information & payment information to merchant & Issuer. At the receiving end order information can only decrypted by merchant & Payment information can decrypt by Issuer — 3m

— 6m

10m



Explanation — 2m

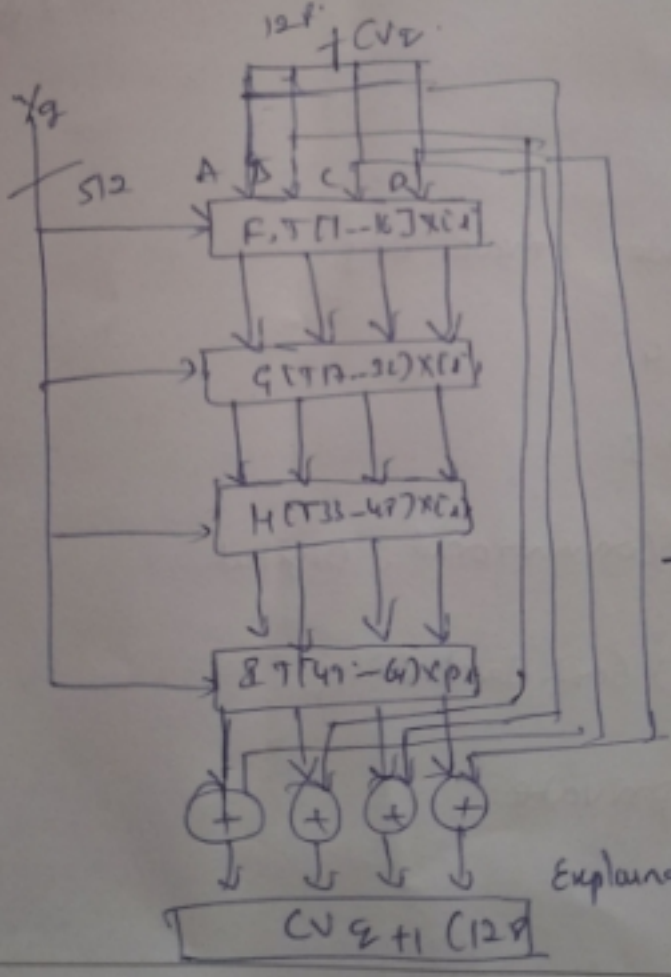
g) iv) All the above — 1

h) iv) 4 — 1

i) iv) All the above — 1

j) iv) All the above — 1

2)



6m

Explanation - 3m

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Approved by AICTE & ISO 9001:2008 Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

Accredited by National Board of Accreditation Council (NBA)

SCHEME & SOLUTION: CONTINUOUS INTERNAL ASSESSMENT- 3

Date:

Course: CNS Course Code: 17TE7DECNS

Semester& Section: VII 'A & 'B' Total no of Pages:

Scheme & Solution prepared by: VIVEK RH-VI

Signature

Q. No.	Description	Marks Distribution
a)	i) Sender private key	1
b)	iv) 4	1
c)	iii) 3	1
d)	i) Conventional, Digital	1
e)	iii) Confidentiality	1
f)	i) private	1

USN

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute Affiliated to VTU, Belagavi)

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Telecommunication Engineering

Continuous Internal Assessment Test - III

Course: **Cryptography and Network security** — **Date: 06/01/2021**

Course Code: **17TE7DECNS** — Maximum marks: **50**

Semester: **VII** — Duration: **90 Min**

	Note: Answer 5 full questions.	Marks
(a)	Hashed message is signed by sender using. i) Sender Private key iii) sender public key ii) Receiver Private key iv) Receiver public key	1x10
(b)	How many protocols make SSL i) 1 ii) 2 iii) 3 iv) 4	
(c)	Hash function must meet _____ criteria i) 5 ii) 2 iii) 3 iv) 4	
(d)	A ____ signature is included in the document, A ____signature is separate entity i) Conventional , Digital iii) Digital , Digital ii) Conventional , Conventional iv) Digital , Conventional	
(e)	A digital signature cannot provide _____ to message i) Integrity iii) Confidentiality ii) Non repudiation iv) Authentication	
(f)	A _____ network is used inside an organization. i) Private ii) public iii) Semi private iv) Semi public	
(g)	SSL provides? Integrity ii) Confidentiality iii) Compression iv) All the above	
(h)	How many phases will virus undergo? i) 2 ii) 3 iii) 5 iv) 4	
(i)	Which of these are an intrusion detection technique i) Threshold detection iii) Profile Based ii) Penetration identification iv) All the above	
(j)	A packet filter router uses i) Source address iii) Destination address ii) port number iv) All the above	
2	With all necessary equations and figures discuss the MD5 processing of single 512 bit block.	10
3	What is the need for dual signature in SET? How are they constructed?	10
4	Briefly describe the three classes of intruder and different approaches to intrusion detection system?	10
	OR	
5	List security rules of reference monitor, with a neat diagram discuss the concept of reference monitor.	10
6	a) Discuss about 4 phases in SSL handshake protocol b) Define Digital signature? Discuss its requirements? Distinguish between direct digital signature and arbitrated signature	5 5
	OR	
7	What is firewall? With a neat diagram explain different types of firewall configurations	10