B-030 Bhatt Pranjal Deepak
FU3F2223089
TE-B
Pranjal | comps

CSS

Date: / /

Page No.:

14.3/15

7-2-25

Assignment No. 1

Q.) Explain the following system security terms in detail with examples:

a) Security Mechanism:

→ i) Security mechanism are various techniques recommended to provide security services at the various OSI layers.

ii) The various ~~seriousty~~ security mechanism that can be applied are as follows:

1) Encipherment (Encryption)
- Symmetric
- Asymmetric

2) Digital signature
- signing a data unit
- verifying a data unit

3) Access control
- Password
- Time of access
- Duration of access
- Access route

4) Data integrity
- Sent quality of data
- Received quantity of data
- Sequencing of data unit
- Time stamping

5) Authentication
- Handshaking
- Cryptographic techniques

6) Traffic Padding

7) Routing control

8) Pervasive ~~seq~~ security

9) Security lobels

10) Security audit

11) Security Recovery

12) Event detection.

Supervisor's Sign. : ____________

Bhatt Pranjal
TE-B Comps
B030 Pranjal

Date : / /
Page No. :

iv]

	HMAC	CBC-MAC	CMAC
Type:	Hash based MAC	block cipher based MAC	-''-
underlying Algo.	Hash function	block cipher	-''-
key length	128, 256 bit	AES : 128	Same as CBC-MAC
Efficiency	Fast	faster HMAC	Slightly Slow
Application	Used TLS, SSL	banking	Sequre ~~commun~~ communication

14.3/15

7.2 .35

Supervisor's Sign. ____________