

Total No. of Questions : 8]

SEAT No. :

PD-4305

[Total No. of Pages : 2

[6403]-103

T.E. (E &TC)

NETWORKS SECURITY

(2019 Pattern) (Semester - VI) (Elective- II) (304195)

Time : 2½ Hours]

[Max. Marks : 70

Instructions to the candidates :

- 1) Answer Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8.
- 2) Neat diagrams must be drawn wherever necessary.
- 3) Figures to the right side indicate full marks.
- 4) Use of Calculator is allowed.
- 5) Assume suitable data, if necessary.

Q1) a) Discuss the block cipher modes of operation and stream cipher mode of operation. [9]

b) Explain the subkey generation in the Blowfish algorithm. [8]

OR

Q2) a) What is an Initialization Vector (IV)? What is its significance? [4]

b) Which basic steps are performed in one round of operation in DES? Explain in detail. [8]

c) Discuss the difference between differential and linear cryptanalysis. [5]

Q3) a) Elaborate the working of hash based Message Authentication codes (HMAC). [6]

b) Discuss X.509 Authentication services [7]

c) Write a short note on: Digital signatures [4]

OR

Q4) a) What are biometric authentication techniques? Explain its importance in today's digital world. [6]

b) How the Authentication Applications such as Kerberos work? Explain in detail. [7]

c) Write a short note on: Knapsack algorithm. [4]

P.T.O.

- Q5) a)** Explain in detail PGP Pretty Good Privacy concept and services provided by PGP. [6]
b) Explain in brief S/MIME protocol. [6]
c) Describe in brief IP security applications, IP Security architecture. [6]

OR

- Q6) a)** Describe Key management use in email security. [6]
b) How confidentiality is obtained using Encapsulating, Security payload [6]
c) Describe in brief security associations. [6]

- Q7) a)** Discuss how secure socket layer and transport layer security can be obtained. [6]
b) Which are the key participants in SET? [6]
c) Discuss the web security considerations. [6]

OR

- Q8) a)** Elaborate different types of firewalls. What are limitations of firewalls? [6]
b) What are the types of intruders and what are intrusion techniques? [6]
c) What is need of SSL? Explain all Phases of SSL handshake protocol in detail. [6]

