**B.Tech. SEM -VII ( Computer) 2014 Course (CBCS) : WINTER - 2018**

**SUBJECT: NETWORK SECURITY AND CRYPTOGRAPHY**

Day: Monday | **W-2018-2537** | Time: 02.30 PM TO 05.30 PM

Date: 26/11/2018 | Max Marks. 60

---

**N.B. :**

1) All questions are **COMPULSORY**.
2) Neat diagrams must be drawn **WHEREVER** necessary.
3) Figures to the right indicate **FULL** marks.
4) Assume suitable data, if necessary.

---

| | | | |
|---|---|---|---|
| **Q.1** | **a)** | Define security, explain its basic components. | **(05)** |
| | **b)** | Differentiate between threats and attacks. | **(05)** |
| | | **OR** | |
| **Q.1** | **a)** | What is denial of service attack? How it affects the network performance. | **(05)** |
| | **b)** | Explain the following w.r.t. security:<br>**i)** Non-Repudiation<br>**ii)** Spoofing | **(05)** |
| **Q.2** | **a)** | Define the terms:<br>**i)** Cryptography<br>**ii)** Cryptosystem | **(05)** |
| | **b)** | Explain the working of single round of DES. | **(05)** |
| | | **OR** | |
| **Q.2** | **a)** | Write a short note on Transpositions cipher. | **(05)** |
| | **b)** | What are different types of attack possible on RSA? Explain in brief. | **(05)** |
| **Q.3** | **a)** | What is Deffie-Hellman key exchange protocol? | **(05)** |
| | **b)** | Write a short note on Digital certificates. | **(05)** |
| | | **OR** | |
| **Q.3** | **a)** | What is the purpose of digital signature? | **(05)** |
| | **b)** | Explain in detail Distributed Denial of Service authentication. | **(05)** |
| **Q.4** | **a)** | Discuss the use of Secure Electronic Transaction w.r.t security. | **(05)** |
| | **b)** | Write a short note on Privacy Enhanced Mail Protocol. | **(05)** |
| | | **OR** | |
| **Q.4** | **a)** | Explain in brief x.509 certificates. | **(05)** |
| | **b)** | Explain the security in GSM and 3G. | **(05)** |
| **Q.5** | **a)** | Explain TCP/IP protocol suit. | **(05)** |
| | **b)** | With the help of suitable diagram explain IPV4. | **(05)** |
| | | **OR** | |
| **Q.5** | **a)** | What is Encapsulating security payload (ESP)? Explain. | **(05)** |
| | **b)** | Write a short note on data compression using zip. | **(05)** |
| **Q.6** | **a)** | What are firewalls? Why do they need? | **(05)** |
| | **b)** | Explain Network Address Translation in detail. | **(05)** |
| | | **OR** | |
| **Q.6** | **a)** | What are benefits of firewall? What problems can arise with firewall? | **(05)** |
| | **b)** | What are goals and objectives of Intrusion Detection System? | **(05)** |

* * * * *