

Con. 9376-13.

GS-5752

**(REVISED COURSE)**

(3 Hours)

[ Total Marks : 100

- N.B.** (1) Question No. 1 is compulsory.  
(2) Attempt any **four** questions from remaining **six** questions.  
(3) Assume suitable **data** if **required**.

1. (a) Explain different Birthday problems. 5  
(b) What are the key principles of security ? 5  
(c) Compare and contrast SHA-T and MD-5 5  
(d) Explain the Honey Pots. 5
  2. (a) How flaw in TCP/IP can cause operating systems to become Vulnerable ? Also Explain how Kerberos are used for user authentication in windows. 10  
(b) For the given values  $p = 19$ ,  $q = 23$  and  $e = 3$  find  $n$ ,  $\phi(n)$  and  $d$  using RSA algorithm. 10
  3. (a) What is Buffer overflow and Incomplete mediation in Software Security ? 10  
(b) Explain one-time initialization process and processes in each round of Advanced Encryption Standard. 10
  4. (a) What is a denial of service attack ? What are the way in which an attacker can mount a DOS attack on the system ? 10  
(b) Compare Packet Sniffing and Packet Spoofing. Explain the session hijacking attack. 10
  5. (a) Explain Multiple level Security Model. Also explain Multilateral Security. 10  
(b) What is Malware ? Explain Salami and Linearization attacks. 10
  6. (a) Explain software Reverse Engineering. Also Explain Digital Rights Management. 10  
(b) Describe the different types of IDS and their limitations. 10
  7. Write short notes on (any **four**) :— 20
    - (a) CAPTCHA
    - (b) Access Control Matrix
    - (c) Covert Channel
    - (d) Firewall
    - (e) RC4.
-