

Con. 4511-12.

(REVISED COURSE)

GN-8492

(3 Hours)

[Total Marks : 100

- N.B.:
1. Question No. 1 is compulsory.
 2. Attempt any **four** questions from out of **six** questions remaining.
 3. Assume data if required and state it clearly.

- Q.1:
- a) What are eight security mechanisms to implement security? (5)
 - b) Distinguish between attack, vulnerability and access control (5)
 - c) What is Feistel Cipher? (5)
 - d) What is CAPTCHA? (5)
- Q.2:
- a) What is race condition? Describe an example of a race conditions. (10)
 - b) What is distinction between a polymorphic and a metamorphic worm? (5)
 - c) What is a double transposition cipher? Describe it with example. (5)
- Q.3:
- a) What are block cipher algorithmic modes? Describe any two modes. (10)
 - b) What are firewall design principles? (10)
- Q.4:
- a) What is the principle behind One-Time-Pads (OTP)? Why they are highly secure? (10)
 - b) What is biometric authentication? What are two parameters defined for biometric measurement? (10)
- Q.5:
- a) Describe the different vulnerabilities in enterprise network with real examples. (10)
 - b) What is Digital Rights Management (DRM)? Describe DRM for P2P application. (10)
- Q.6:
- a) What are strengths and limitations Intrusion Detection System? (10)
 - b) Using the RSA algorithm, encrypt the following: (10)
 - i. $p=3, q=11, e=7, M=12$
 - ii. $p=7, q=11, e=17, M=25$
 - iii. Find the corresponding d_s for (i) and (ii) and decrypt the ciphertexts.
- Q.7: Solve the following: (any three): (20)
- a) AES
 - b) SSL/TLS
 - c) Honeypots
 - d) MD5