BT-8/J-22 **48249**

CYBER SECURITY

Paper–OE-CS-402A

ne Allowed : 3 Hours] [Maximum Marks : 75

te : Attempt any **five** questions in all, selecting at least **one** question from each Unit. All questions carry equal marks.

UNIT–I

What is cybercrime? Discuss the scope of cybercrime. Explain different types of cybercrime against individual, property and government. 15

(a) Discuss the principles of block cipher. How des cipher achieves the Shannon's goal of confusion and diffusion? 8

(b) Explain the strength and weakness of Data Encryption Standard (DES). Differentiate between differential and linear cryptanalysis. 7

UNIT–II

a) What is Secure Hash Algorithm (SHA)? Why SHA algorithm is used for? Distinguish between MD5 and SHA1. 8

) What is Digital Signature Standard (DSS) in cryptography discuss proof of DSS algorithm? 7

4. (a) Differentiate between Kerberos and X.509. Discuss the main components of Kerberos. How does it work? 8

(b) Discuss in brief the various enhancements to electronic mail security. How PGP operations are authenticated? 7

UNIT–III

5. (a) Differentiate between active and passive attacks. Discuss the different ways to prevent cybercrime. 8

(b) Elaborate different data security considerations that must be considered before data disposal and data storage. 7

6. (a) Define firewall? Describe firewall technology and the various approaches to firewall implementation. 8

(b) Write a detailed note on Secure Electronic Transaction (SET). 7

UNIT–IV

7. What is digital forensic? Explore the types of digital forensic. Discuss the challenges faced by digital forensic. 15

8. (a) Why do we need cyber laws? Discuss legal perspective of cybercrimes and cyber security. 8

(b) Explore the use and components of IP security. List the services provided by encapsulating security payload. 7