COURSE: B.COM(H)

SEMESTER: IV

PAPER: CYBER CRIMES AND LAWS

ASSIGNMENT QUESTIONS

Assignment 1

20 Marks

1Explain the meaning and uses of digital signature.

2 What constitutes damage to computer, computer system or computer network? State the penalties provided under the IT Act, 2000 for such an offence.

Q3 Write notes on the following:

(1) WIPO

(ii) Copyright as a tool of security

(ii) Adjudicating Officer

Assignment 2

20 Marks

1. Write notes on the following:

   (1) Internet Governance
   (2) Penalties and Compensation
   (3) Copyright Infringement Officer

2. Define the term 'Cyber Space'. What are the different types of jurisdiction in cyber space?

3. What is domain name? Explain the different types of domain name.

CLASS TEST QUESTIONS

10*2= 20 Marks

Q1. (a) What is Internet? Explain the basic applications of Internet.

(b) What is Cyber Security? What are the different initiatives taken the Government for promotion of cyber security.

Q2. (a) Write a short note on 'Cryptography'.

(b) What is domain name? Explain the different types of domain name.

Multiple Choice questions (MCQ's)

1. Many Cyber Crimes comes under Indian Penal Code Which one of the following is an example?

A. Sending Threatening message by Email

B. Forgery of Electronic Record

C. Bogus Website

D. All of above

Answer D

2. The Information Technology Act 2000 is an Act of Indian Parliament notified on

A. 27th October 2000

B. 15th December 2000

C. 17th November 2000

D. 17th October 2000
Answer D

3. Digital Signature Certificate is ____________ requirement under various applications

A. Statutory

B. Legislative

C. Govenmental

D. Voluntary

Answer A

4. Assessing Computer without prior authorization is a cyber crime that comes under____

A. Section 65

B. Section 66

C. Section 68

D. Section 70

Answer B

5. ____________ means a person who has been granted a licence to issue a electronic signature certificate.

A. Certifying Authority

B. Certifying Private Key Authority

‘C. Certifying system controller

D. Appropriate Authority

Answer A

6. ________ is a data that has been organized or presented in a meaningful manner.

A. A process

B. Software

C. Storage

D. Information

Answer D

7. _______ is an application of information and communication technology (ICT) for delivering Government Service.

A. Governance

B. Electronic Governance

C. Governance and Ethics

D. Risk and Governance.

Answer B

8. The Altering of data so that it is not usable unless the changes are undone is

A. Biometrics

B. Encryption

C. Ergonomics

D. Compression

Answer B

9. Authentication is _________

A. To assure identity of user on a remote system

B. Insertion

C. Modification

D. Integration

Answer A

10. The following cannot be exploited by assigning or by licensing the rights of others

A. Patent

B. Design

C. Trademark

D. All of the above

Answer C

11. Which of the following is not a type of cyber crime?

a) Data theft

b) Forgery

c) Damage to data and systems

d) Installing antivirus for protection

Answer D

Explanation: Cyber crimes are one of the most threatening terms that is an evolving phase. It is said that major percentage of the World War III will be based on cyber-attacks by cyber armies of different countries.

12. Which of the following is not a type of peer-to-peer cyber-crime?

a) Phishing

b) Injecting Trojans to a target victim

c) MiTM

d) Credit card details leak in deep web

Answer: d

Explanation: Phishing, injecting Trojans and worms to individuals comes under peer-to-peer cyber crime. Whereas, leakage of credit card data of a large number of people in deep web comes under computer as weapon cyber-crime.

13. Which of the following is not done by cyber criminals?

a) Unauthorized account access

b) Mass attack using Trojans as botnets

c) Email spoofing and spamming

d) Report vulnerability in any system

Answer: d

Explanation: Cyber-criminals are involved in activities like accessing online accounts in unauthorized manner; use Trojans to attack large systems, sending spoofed emails. But cyber-criminals do not report any bug is found in a system, rather they exploit the bug for their profit.

14. What is the name of the IT law that India is having in the Indian legislature?

a) India’s Technology (IT) Act, 2000

b) India’s Digital Information Technology (DIT) Act, 2000

c) India’s Information Technology (IT) Act, 2000

d) The Technology Act, 2008

Answer: c

Explanation: The Indian legislature thought of adding a chapter that is dedicated to cyber law. This finally brought India’s Information Technology (IT) Act, 2000 which deals with the different cyber-crimes and their associated laws.

15. What is the punishment in India for stealing computer documents, assets or any software’s source code from any organization, individual, or from any other means?

a) 6 months of imprisonment and a fine of Rs. 50,000

b) 1 year of imprisonment and a fine of Rs. 100,000

c) 2 years of imprisonment and a fine of Rs. 250,000

d) 3 years of imprisonment and a fine of Rs. 500,000

Answer:D

Explanation: The punishment in India for stealing computer documents, assets or any software’s source code from any organization, individual, or from any other means is 3 years of imprisonment and a fine of Rs. 500,000.

16. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?

a) Cracking or illegally hack into any system

b) Putting antivirus into the victim

c) Stealing data

d) Stealing hardware components

Answer: a

Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law says that cracking or illegally hacking into any victim's computer is a crime. It covers a wide range of cyber-crimes under this section of the IT Act

17. VIRUS stands for

A. Very Intelligent Result Until Source

B. Very Interchanged Resource Under Search

C. Vital Information Resource Under Siege

D. Viral Important Record User Searched

Answer B

18. Which of the following is/are threats for electronic payment systems?

A. Computer worms

B. Computer virus

C. Trojan horse

D. All of the above

Answer D

19. Which of the following virus overtake computer system, when it boots and destroy information?

A. System infectors

B. Trojan

C. Boot infectors

D. **Stealth virus**

Answer D

20. Firewalls are used to protect against

A**.** data driven attacks

B. fire attacks

C. virus attacks

D. unauthorised access

Answer D

21. ________ software are programs that are installed onto your computer and can scan and remove known viruses which may have been contracted.

A. Firmmware

B. Adware

C. Keylogger

D. Antivirus

Answer D