Total No. of Questions: 25 **Enrollment No :** ____________________

MEDICAPS UNIVERSITY

Faculty of Engineering / Science

End Semester Examination May 2025

OE00073 Cyber Security Fundamentals

Programme	:	B.Tech. / B. Sc.	**Branch/Specialisation**	:	All
Duration	:	3 hours	**Maximum Marks**	:	60

Note: *All questions are compulsory. Internal choices, if any, are indicated. Assume suitable data if necessary. Notations and symbols have their usual meaning.*

Section 1 (Answer all question(s))

Marks CO BL

Q1. Which of the following is not a fundamental component of a symmetric cipher model? **1 2 2**

○ Plaintext ● Public key

○ Encryption algorithm ○ Ciphertext

Q2. Choose among the following techniques, which are used to hide information inside a picture- **1 1 1**

○ Image rendering ● Steganography

○ Rootkits ○ Bitmapping

Q3. Which of these methods is used to check the validity of a message? **1 1 1**

○ Digital signature ○ Protocol

● Message digest ○ Decryption algorithm

Q4. During the Diffie-Hellman key exchange, each party generates a_______. **1 2 2**

○ A public key and a shared secret key ○ An encryption key and a decryption key

● A private key and a public key ○ Session key and a master key

Q5. They are malicious hackers whose primary goal is to commit cybercrimes to make money. Who are "they" in this context? **1 1 1**

○ White Hat Hackers ○ Hacktivists

○ Gray Hat Hackers ● Black Hat Hackers

Q6. The most important step in system hacking is- **1 2 2**

○ Covering tracks ○ Information gathering

● Cracking passwords ○ None of the above

Q7. Choose the one that is autonomous and does not require a host program from the list below- **1 2 2**

○ Trap door ○ Trojan horse

○ Virus ● Worm

Q8. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network? **1 3 3**

○ Digital crime ● Cyber Attack

○ System hijacking ○ Threats

Q9. Which section deals with cyberterrorism? **1 1 1**

○ 66 C ○ 66 B

○ 66 D ● 66 F

Q10. The Information Technology Act 2000 is an Act of Indian Parliament notified on- **1 1 1**

○ 17th November 2000 ○ 27th October 2000

● 17th October 2000 ○ 15th December 2000

Section 2 (Answer all question(s))

Marks CO BL

Q11. Introduce any one symmetric cipher substitution technique with an example. **2 2 3**

Rubric	Marks
Substitution Technique	2

Q12. Differentiate the terms confusion and diffusion in block cipher. **2 4 4**

Rubric	Marks
2 differences	2

Q13. **(a)** Differentiate cipher feedback mode (CFB) & output feedback mode with a diagram. **6 4 4**

Rubric	Marks
2 difference	6

(OR)

(b) Suppose key = 'hello' and plaintext = 'medicaps'; then write a Playfair matrix (table) and encrypt a message using Playfair cipher.

Rubric	Marks
Playfair matrix (table) Cipher Text= KL BM GE MU	6

Section 3 (Answer all question(s))

Marks CO BL

Q14. Describe a brute force attack. **2 1 1**

Rubric	Marks
Brute Force attack with example	2

Q15. Explain message authentication code with its basic weakness. **3 3 3**

Rubric	Marks
Message Authentication Code with diagram	3

Q16. (a) Users A & B exchange the key using the Diffie-Hellman algorithm. Assume a=5, q=11, XA=2, and XB=3. Find YA, YB, and K. **5 5 5**

Rubric	Marks

value of YA=3
YB=4
K=5
	5

(OR)

(b) Perform encryption and decryption using the RSA algorithm for the following: P=7; q=11; e=17; M=8.

Rubric	Marks

Encryption with right process, calculate all values
n=77
Φ(n) =60
d=53 (may be very as per the selection)
encryption = 57
decryption=8
	5

Section 4 (Answer any 2 question(s))

Marks CO BL

Q17. Analyze and explain the differences between passive and active cyberattacks, providing examples of each. **5 4 4**

Rubric	Marks
2 differences between Passive and Active Cyberattacks	5

Q18. Create a classification framework for cvbercrimes, detailing their types and examples, and evaluate their potential impact on individuals and organizations. **5 6 6**

Rubric	Marks
Create a classification framework for Cybercrimes, detailing their types and examples	5

Q19. Evaluate the role of different types of hackers (white hat, black hat, and gray hat) in improving or damaging cybersecurity. **5 6 5**

Rubric	Marks
White Hat, Black Hat, Gray Hat definition	5

Section 5 (Answer all question(s))

Marks CO BL

Q20. Define phishing and mention one common phishing technique. **2 2 2**

Rubric	Marks
Phishing definition	2

Q21. Explain the role of registry settings in mobile device security. **3 3 3**

Rubric	Marks
role of registry settings in mobile device security	3

Q22. (a) Analyze the impact of credit card fraud on individuals and businesses with examples. **5 4 4**

Rubric	Marks
The impact of credit card fraud on individuals and businesses with examples.	5

(OR)

(b) How can organizations enhance mobile security against cyber threats?

Rubric	Marks
Give points to enhance mobile security.	5

Section 6 (Answer all question(s))

Marks CO BL

Q23. Name any two sections of the Indian IT Act-2000. **2 1 1**

Rubric	Marks
Give any two sections of the Indian IT Act-2000.	2

Q24. Describe the importance of a digital signature in online transactions. **3 3 3**

Rubric	Marks
importance of a digital signature in online transactions	3

Q25. (a) How can digital forensics help in tracking cybercriminals? Explain with an example. **5 5 5**

Rubric	Marks
digital forensics help in tracking cybercriminals	5

(OR)

(b) Design a simple strategy to enhance digital evidence management in forensic cases.

Rubric	Marks
simple strategy to enhance digital evidence management in forensic cases.	5

******