Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No......................................

Faculty of Engineering

End Sem Examination Dec-2023

OE00073 Cyber Security Fundamentals

Programme: B.Tech. Branch/Specialisation: All

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Which encryption method ensures that only the intended recipient can decrypt the data? **1**

(a) Link encryption (b) End-to-end encryption

(c) Symmetric encryption (d) Asymmetric encryption

ii. Which of the following is not a common use case for symmetric ciphers? **1**

(a) Securing email communication

(b) Protecting stored passwords

(c) Securely transmitting credit card data

(d) Establishing secure SSL/TLS connections

iii. Block chaining techniques are commonly used in- **1**

(a) Symmetric key encryption (b) Public key encryption

(c) Digital signatures (d) Hash functions

iv. A Public key encryption system- **1**

(a) Allows anyone to decode the transmission

(b) Allows only the correct sender to decode the data

(c) Allows only the correct receiver to decode the data

(d) None of these

v. Which of the following is a type of vulnerability in cybersecurity related to improper system configurations? **1**

(a) Technology weakness

(b) Configuration weakness

(c) Security policy weakness

(d) Structured threat

vi. What is the primary motive of a phreaker in the realm of cybercrimes? **1**

(a) Financial gain (b) Stealing sensitive data

(c) Manipulating phone systems (d) Distributing malware

P.T.O.

vii. What is the primary goal of a phishing attack? **1**

(a) Stealing confidential data or login credentials
(b) Planting a hidden virus on the target system
(c) Launching a distributed denial-of-service (DDoS) attack
(d) Encrypting the victim's files for ransom

viii. What is "card-not-present" (CNP) fraud? **1**

(a) A type of online shopping discount
(b) A method of making in-store payments
(c) A fraudulent transaction where the physical card is not required
(d) A payment method using mobile devices

ix. In digital forensics, what is the chain of custody? **1**

(a) A secure method of encrypting data
(b) The process of investigating cybercrimes
(c) The chronological documentation of who has handled evidence and when
(d) A type of cyberattack

x. Which Indian legislation serves as the foundation for cyber laws in the country? **1**

(a) Indian Penal Code
(b) Indian Copyright Act
(c) Information Technology Act, 2000
(d) Indian Cybersecurity Act

Q.2 i. What are the key advantages and disadvantages of symmetric ciphers in the context of information security? **2**

ii. How key management is handled in substitution ciphers? **3**

iii. Compare and contrast the different types of substitution techniques, such as Caesar cipher, Playfair cipher, and the use of substitution tables. **5**

OR iv. Describe with example DES Algorithm. **5**

Q.3 i. How does the Diffie-Hellman key exchange algorithm enable two parties to securely exchange secret keys over a public channel? **4**

ii. Perform encryption and decryption using RSA algorithm for p=3, q=11, e=7, m=5. **6**

OR iii. What are some countermeasures and strategies to defend against brute-force attacks? **6**

Q.4 i. Explain the concept of a zero-day vulnerability and its significance in the world of cybersecurity. **2**

ii. Explain the differences between passive attacks and active attacks in the context of cybersecurity. **3**

iii. Discuss the potential legal consequences for individuals engaged in cybercrimes, such as hacking, phishing, or other malicious activities. **5**

OR iv. How can organizations mitigate the risks associated with technology weaknesses as a type of vulnerability? **5**

Q.5 i. What are the techniques and motivations behind password cracking in cybercrimes? **4**

ii. Explain the characteristics and risks associated with viruses, worms, Trojan Horses, and backdoors in cyberattacks. **6**

OR iii. What are the legal and financial implications for victims of credit card fraud? What steps should they take when they suspect fraudulent activity? **6**

Q.6 Attempt any two:

i. How can digital evidence be effectively managed to maintain its integrity and chain of custody throughout an investigation? **5**

ii. What are the main sections of the Indian IT Act-2000? How do they regulate electronic transactions and data security? **5**

iii. Describe the significance of public key certificates in the context of digital security and encryption. **5**

******

Marking Scheme
Cyber Security Fundamentals-OE00073(T)

Q.1	i)	Ans: b) End-to-end encryption		**1**
	ii)	Ans: d) Establishing secure SSL/TLS connections		**1**
	iii)	Ans: a) Symmetric key encryption		**1**
	iv)	Ans: c).		**1**
	v)	Ans: b) Configuration weakness		**1**
	vi)	Ans: c) Manipulating phone systems		**1**
	vii)	Ans: a) Stealing confidential data or login credentials		**1**
	viii)	Ans: c) A fraudulent transaction where the physical card is not required		**1**
	ix)	Ans: c) The chronological documentation of who has handled evidence and when		**1**
	x)	Ans: c) Information Technology Act, 2000		**1**
Q.2	i.	Key advantages	1 Mark	**2**
		disadvantages	1 Mark	
	ii.	Key management…….. ciphers	(As per explanation)	**3**
	iii.	Compare and contrast …….tables.	(As per explanation)	**5**
OR	iv.	DES Algorithm.	(As per explanation)	**5**
Q.3	i.	Diffie-Hellman………..channel	(As per explanation)	**4**
	ii.	Perform …… for p=3, q=11, e=7, m=5.	(As per explanation)	**6**
OR	iii.	Some …. …. Attacks	(As per explanation)	**6**
Q.4	i.	Differences …. Cybersecurity	(As per explanation)	**3**
	ii.	Concept of … cybersecurity.	(As per explanation)	**2**
	iii.	Potential ………. activities.	(As per explanation)	**5**
OR	iv.	Organizations .. …. Vulnerability	(As per explanation)	**5**
Q.5	i.	Techniques …….. .. cybercrimes	(As per explanation)	**4**
	ii.	Characteristics …..….. cyberattacks	(As per explanation)	**6**
OR	iii.	Legal …… activity	(As per explanation)	**6**
Q.6		Attempt any two:		
	i.	Digital evidence …… investigation	(As per explanation)	**5**
	ii.	Main sections ……….. security	(As per explanation)	**5**
	iii.	Significance ……encryption.	(As per explanation)	**5**

******

P.T.O.