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

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2022

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.

Q.1 i. In the DES algorithm the round key is ____ bit and the round input is ____ bits. **1**

(a) 48,32 (b) 64,32 (c) 56,24 (d) 32,32

ii. Which of the following slows the cryptographic algorithm – **1**

I. Increase in Number of rounds

II. Decrease in Block size

III. Decrease in Key Size

IV. Increase in Sub key Generation

(a) I and III (b) III and IV (c) II and III (d) II and IV

iii. The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other. **1**

(a) Man-in-the-middle (b) Ciphertext attack

(c) Plaintext attack (d) None of these

iv. Message authentication code is also known as **1**

(a) Key code (b) Hash code

(c) Keyed hash function (d) Message key hash function

v. Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____. **1**

(a) State sponsored hackers (b) Blue hat hackers

(c) Cyber terrorists (d) Red hat hackers

vi. Which of the following is an example of active reconnaissance? **1**

(a) Searching public records

(b) Telephone calls as a help desk or fake customer care person

(c) Looking for the target's details in the database

(d) Searching the target's details in paper files

vii. If you think someone has misused your personal or financial information, the first thing you should do is- **1**
(a) Cut up all of your credit cards and shred your bank statements.
(b) Call one of the three major credit reporting companies and ask them to put an initial fraud alert on your credit report.
(c) Call your friends and family and put them on the lookout for someone pretending to be you.
(d) None of these

viii. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium. **1**
(a) Malware (b) Remote access trojans
(c) Keyloggers (d) Spyware

ix. A valid definition of digital evidence is- **1**
(a) Data stored or transmitted using a computer
(b) Information of probative value
(c) Digital data of probative value
(d) Any digital evidence on a computer

x. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds? **1**
(a) Cracking or illegally hack into any system
(b) Putting antivirus into the victim
(c) Stealing data
(d) Stealing hardware components

Q.2 i. Define block cipher and stream cipher. **2**
ii. Explain symmetric encryption of confusion and diffusion. **3**
iii. Describe with example DES Algorithm. **5**
OR iv. Write short note on: **5**
(a) End to end encryption.
(b) Potential locations on confidentiality attacks.

Q.3 Attempt any two.
i. Explain message authentication code and hash function. **5**
ii. Describe Diffie Helman key exchange with example. **5**
iii. Perform encryption and decryption using RSA algorithm for p=3, q=11, e=7, m=5. **5**

Q. 4 i. Define cyber-attack. What are its types? Explain. **3**
ii. Write and explain the classification of vulnerability and threats. **7**
OR iii. Differentiate between: **7**
(a) Hacker, cracker, phreaker
(b) White hat hacker and black hat hacker

Q.5 Attempt any two:
i. Describe registry setting and RAS security for mobile devices. **5**
ii. Explain various tools and methods used in cybercrimes. **5**
iii. Elaborate Proliferation of mobile and wireless devices. Also tell different attacks on mobile phone. **5**

Q.6 Attempt any two:
i. Explain Basic Indian IT Act-2000 and its various sections. **5**
ii. What is digital signature? What are three uses for digital signatures? **5**
iii. Describe digital forensics investigation methods, reporting and management of evidence. **5**

******

Marking Scheme
OE00073 Cyber Security Fundamentals

Q.1	i)	In the DES algorithm the round key is _____ bit and the Round Input is _____bits. **a)48,32**	**1**
	ii)	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation **c)2 and 3**	**1**
	iii)	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other. **a) man-in-the-middle**	**1**
	iv)	Message authentication code is also known as **c)keyed hash function**	**1**
	v)	Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____ **c) Cyber Terrorists**	**1**
	vi)	Which of the following is an example of active reconnaissance? **b) Telephone calls as a help desk or fake customer care person**	**1**
	vii)	If you think someone has misused your personal or financial information, the first thing you should do is: **b) Call one of the three major credit reporting companies and ask them to put an initial fraud alert on your credit report.**	**1**
	viii)	These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium. **d)Spyware**	**1**
	ix)	A valid definition of digital evidence is: **c) Digital data of probative value**	**1**
	x)	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**	**1**
Q.2	i.	Define Block cipher and stream cipher. **(1 mark each)**	**2**
	ii.	Explain Shannon's Theory of Confusion and Diffiusion. **(1.5 mark each)**	**3**
	iii.	Describe with example DES Algorithm. **(Algorithm 2.5 mark, Example 2.5 mark)**	**5**
OR	iv.	Write short note on: **(2.5 mark each)** a)End to end encryption. b)Potential locations on confidentiality attacks.	**5**
Q.3		**Attempt any two.**	
	i.	Explain Message authentication code and hash function. **(2.5 mark each)**	**5**
	ii.	Describe Diffie Helman key exchange with example. **(Algorithm 2.5 mark, Example 2.5 mark)**	**5**
	iii.	Perform encryption and decryption using RSA algorithm for p=3, q=11, e=7, m=5. **(Stepwise marking 5 marks)**	**5**
Q. 4	i.	Define Cyber attack. What are its types, explain. **(Definition 1 mark, types 2 marks)**	**3**
	ii.	Write and explain the Classification of Vulnerability and threats. **(3.5 marks each)**	**7**
	iii.	Differentiate between: **(3.5 marks each)** a) Hacker, Cracker, Phreaker b) White hat hacker and black hat hacker	**7**
Q.5		**Attempt any two.**	
	i.	Describe Registry setting and RAS security for Mobile devices. **(2.5 mark each)**	**5**
	ii.	Explain various Tools and Methods used in cybercrimes. **(2.5 mark each)**	**5**
	iii.	Elaborate Proliferation of mobile and wireless devices. Also tell different attacks on mobile phone. **(2.5 mark each)**	**5**
Q.6		**Attempt any two.**	
	i.	Explain Basic Indian IT Act-2000 and its various sections. **(2.5 mark each)**	**5**
	ii.	What is digital signature? What are three uses for Digital Signatures? **(2.5 mark each)**	**5**
	iii.	Describe Digital forensics investigation methods, reporting and management of evidence. **(2.5 mark each)**	**5**

******