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

Faculty of Engineering
End Sem (Even) Examination May-2019
CA5EL12 Cyber Security
Programme: MCA   Branch/Specialisation: Computer Application

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.   Who disguised as legitimate software   1
          (a) Root Kit   (b) Spyware   (c) Trojan   (d) Worms
     ii.   _____ encrypts all the data on your computer and then asks for a   1
          large payment
          (a) Botnet   (b) Worm   (c) Adware   (d) Ransomeware
     iii. _____ compromise the confidentiality, integrity or availability   1
          of data or a system
          (a) Threats   (b) Worms   (c) Virus   (d) Agobot
     iv.   The method used to activate the threat is called _____.   1
          (a) Supply Chain   (b) Threat Vector
          (c) SDBot   (d) DDoS
     v.   Front-end validation checks for the software is part of _____   1
          controls.
          (a) Applications   (b) Hardware
          (c) Logical   (d) None of these
     vi.   Trying to steal the information of other computer system is called 1
          _____.
          (a) Cracking   (b) Hacking   (c) Blackhat   (d) Back-end Access
     vii. What is the most significant issue in computer forensics?   1
          (a) Preserving evidence   (b) Seizing evidence
          (c) Admissibility of evidence (d) Discovery of evidence
     viii. Digital Forensic Laboratory of the Government of India is located in   1
          _____.
          (a) Hyderabad (b) Kolkata   (c) Delhi   (d) Mumbai
     ix.   The IT Amendment Act was made effective from   1
          (a) 27 Oct 2009   (b) 07 Oct 2009
          (c) 02 Oct 2009   (d) 05 Oct 2009

P.T.O.

     x.   The word 'Cyber Crime" has been define under _____.   1
          (a) 66A   (b) 66F
          (c) 66D   (d) Not Define in the Act

Q.2 i.   What is Cyber Security? Explain.   2
     ii.   Explain Malware attacks with their functions.   3
     iii. What is DDoS? Explain its types in detail.   5
OR   iv.   What is Botnets? How Botnet Grows? Explain the properties of   5
          AgoBot.

Q.3 i.   Define Threat vector and Threat landscape.   3
     ii.   Define Cyber Crime Channel. Classify in detail.   7
OR   iii. What is hacking? Explain various cybercrime methods with   7
          suitable examples.

Q.4 i.   Why we need Computer Fraud protection? Explain.   3
     ii.   What is fraud? Explain various types of fraud control methods in   7
          details.
OR   iii. Describe Cyber Crime Incidents. Explain the Cyber Crime   7
          Incident management procedure with the help of flow chart.

Q.5 i.   Is there a difference between Computer Security and Computer   3
          forensics? Explain.
     ii.   What is Digital forensics? Explain how the "Chain of Conduct"   7
          concept applies in Computer/ Digital Forensics.
OR   iii. What are the various phases and activities involved in the life cycle   7
          of a forensics investigations process? Explain with relevant
          example.

Q.6   Attempt any two:
     i.   What is the meaning of the term "Cyberlaw"? Explain the salient   5
          features of the Indian IT Act.
     ii.   Quote the Indian IT Act 2000 chapters that are relevant in   5
          cybercrime and information security.
     iii. Under the Indian IT Act, is there a legal protection available for   5
          "Personal data" and "Sensitive data"? Explain.

*****

Marking Scheme
CA5EL12 Cyber Security

Q.1	i.	Who disguised as legitimate software	**1**	
		(c) Trojan		
	ii.	_____ encrypts all the data on your computer and then asks for a large payment	**1**	
		(d) Ransomeware		
	iii.	_____ compromise the confidentiality, integrity or availability of data or a system	**1**	
		(a) Threats		
	iv.	The method used to activate the threat is called _____.	**1**	
		(b) Threat Vector		
	v.	Front-end validation checks for the software is part of _____ controls.	**1**	
		(a) Applications		
	vi.	Trying to steal the information of other computer system is called _____.	**1**	
		(b) Hacking		
	vii.	What is the most significant issue in computer forensics?	**1**	
		(c) Admissibility of evidence		
	viii.	Digital Forensic Laboratory of the Government of India is located in _____.	**1**	
		(a) Hyderabad		
	ix.	The IT Amendment Act was made effective from	**1**	
		(a) 27 Oct 2009		
	x.	The word 'Cyber Crime" has been define under _____.	**1**	
		(d) Not Define in the Act		

Q.2	i.	Cyber Security		**2**
	ii.	Malware attacks with their functions.		**3**
	iii.	DDoS	1 mark	**5**
		Its types	4 marks	
OR	iv.	Botnets	1 mark	**5**
		Botnet Grows	2 marks	
		Properties of AgoBot.	2 marks	

Q.3	i.	Define Threat vector and Threat landscape.		**3**
	ii.	Define Cyber Crime Channel	2 marks	**7**
		Classification	5 marks	

OR	iii.	Hacking	2 marks	**7**
		Cybercrime methods	5 marks	

Q.4	i.	Need of Computer Fraud protection		**3**
	ii.	Fraud	2 marks	**7**
		Types of fraud control methods	5 marks	
OR	iii.	Cyber Crime Incidents	2 marks	**7**
		Cyber Crime Incident management procedure with flow chart	5 marks	

Q.5	i.	Difference between Computer Security and Computer forensics		**3**
	ii.	Digital forensics	2 marks	**7**
		Chain of Conduct	5 marks	
OR	iii.	Phases and activities involved in the life cycle of a forensics investigations process	2 marks	**7**
		Relevant example.	5 marks	

Q.6		Attempt any two:		
	i.	Meaning of the term Cyberlaw	2 marks	**5**
		Salient features of the Indian IT Act	3 marks	
	ii.	Indian IT Act 2000 chapters relevant in cybercrime and information security.		**5**
	iii.	Legal protection available for "Personal data" and "Sensitive data"		**5**

*****