(3 Hours) [Total Marks: 80]

N.B.: (1) Question No. 1 is **Compulsory**.
(2) Attempt any **three** questions out of the remaining **five**.
(3) Each question carries 20 marks and sub-question carry equal marks.
(4) Assume suitable data if required.

1.		**Solve any four.**	(20)
	(a)	Illustrate the Botnets structures used in cyber crimes	(5)
	(b)	Demonstrate with example the difference between weak passwords, strong passwords and Random passwords.	(5)
	(c)	Recommend any five steps for creating Cyber security Awareness.	(5)
	(d)	Summarize Notable features of the ITAA	(5)
	(e)	Differentiate between Steganography and cryptography.	(5)
2.	(a)	Discuss traditional techniques to prevent attacks on WIFI.	(10)
	(b)	Examine the PCI DSS compliance 'levels' and discuss how are they determined.	(10)
3.	(a)	Predict high-Level Threats and Vulnerabilities for mobile use at organizational level.	(10)
	(b)	Draw and explain DDoS attacks. How to prevent Dos/DDos attacks?	(10)
4.	(a)	Determine Security Considerations for top Web Security Threats.	(10)
	(b)	Examine the common HIPAA violations Causes and what are its categories?	(10)
5	(a)	Illustrate factors to be considered in the security of: a) Debit and Credit Card b) Mobile Banking c) UPI d) Online banking	(10)
	(b)	How does a VPN work? What should a good VPN do? How to surf securely with a VPN?	(10)
6.	(a)	Judge the role of AI/ML in Cyber Security.	(10)
	(b)	What are the FISMA Compliance Requirements? Demonstrate Penalties for FISMA Compliance Violations	(10)

****