SET-II

Roll No. | | | | | | | | | | |

COER University

END SEMESTER EXAMINATION, EVEN SEMESTER, 2023-24

Time : 3 hour **Semester** : VI **Total Marks : 100**
Program Name : B.Tech **Branch/Specialization** : Cyber Security
Course Code : SOC310 **Course Name** : Cryptography & Network Security

Note: All questions are compulsory. No student is allowed to leave the examination hall before the completion of the time.

Q. No 1	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Illustrate the following equation using Chinese Remainder Theorem. X = 2(Mod 3) X = 3(Mod 5) X = 2(Mod 7)	CO 1	3
(b)	Define groups, rings, and fields in the context of number theory. How are these structures used in modern cryptography?	CO 1	3
(c)	Explain Euler's Totient function and Euler's Theorem with suitable example. Also, enlist the applications.	CO 1	2
(d)	Prove that Fermat's theorem hold for the following or not? I. P=5, a=2 II. P=6, a=2	CO 1	3
(e)	Describe Euclid's algorithm for finding the greatest common divisor (GCD) of two integers. Provide an example illustrating its usage.	CO 1	2

Q. No 2	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Discuss why AES eventually replaced 3DES as the preferred symmetric encryption standard despite 3DES being more widely used initially.	CO 2	2
(b)	Illustrate encryption and decryption using the RSA algorithm for the following: p=17; q=31; e=7; M=2	CO 2	3
(c)	Discuss a real-world application scenario where public key cryptography is more suitable than symmetric key cryptography.	CO 2	2
(d)	Explain the process of key generation, distribution, and storage in a cryptographic system.	CO 2	2
(e)	Illustrate Diffie-Hellman Key Exchange algorithm and How does Diffie-Hellman contribute to secure communication over an insecure channel?	CO 2	2

Q. No 3	Attempt Any Four Parts. Each Question Carries 5 Marks.	CO	BL
(a)	Discuss the principles of digital signatures and their role in ensuring message authenticity and integrity.	CO 3	2
(b)	Describe the purpose and functionality of a Message Authentication Code (MAC) in cryptographic systems.	CO 3	2
(c)	Compare MD5 and SHA algorithms.	CO 3	3
(d)	Describe the Digital Signature Algorithm (DSS). How does it ensure the authenticity and integrity of a digital message?	CO 3	3
(e)	Define HMAC (Hash-based Message Authentication Code). How does HMAC enhance the security of traditional MAC algorithms.	CO 3	2

Q. No 4	Attempt Any Two Parts. Each Question Carries 10 Marks.	CO	BL
(a)	Explain the concept of firewall designs and the principles that should guide the construction of a firewall for it to be effective.	CO 4	3
(b)	Discuss various threats encountered in computer systems. Differentiate among viruses, worms and Trojans.	CO 4	2
(c)	Define an intruder in the context of network security. Also define the motivations and techniques commonly employed by intruders to compromise system security?	CO 4	2

Q. No 5	Attempt Any Two Parts. Each Question Carries 10 Marks.	CO	BL
(a)	Discuss email authentication of the source prevent email spoofing and identity fraud? Discuss techniques used for email sender authentication, such as SPF, DKIM, and DMARC.	CO 5	2
(b)	Differentiate between IP and IPv6 in terms of their security features and capabilities. Discuss how IPv6 addresses security concerns present in IPv4.	CO 5	3
(c)	Explain the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol. How does S/MIME enhance email security.	CO 5	2

----------**End of Paper**----------