QP Code: SN22BTECH585 Reg. No | | | | | | | | | | | AR 21

Gandhi Institute of Engineering and Technology University, Odisha, Gunupur
(GIET University)

B. Tech (Seventh Semester - Regular) Examinations, November – 2025

22BCSPC47002 – Cryptography and Network Security

(CSE)

Time: 3 hrs Maximum: 70 Marks

PART – A **(2 x 5 = 10 Marks)**

Q.1. Answer ***ALL*** questions

		CO #	Blooms Level
a.	Find the result of 7^{10} mod 11 and 6^9mod 10.	CO4	K1
b.	Define Fermat and Euler's theorem.	CO2	K2
c.	Differentiates between Hash Function and MAC	CO3	K4
d.	Define Authentication and Confidentiality	CO2	K2
e.	Define the concept of Double DES and Triple DES.	CO2	K3

PART – B **(15 x 4 = 60 Marks)**

Answer ***all*** the questions

		Marks	CO #	Blooms Level
2. a.	Define cryptography. Briefly describe OSI security architecture with appropriate block diagram	8	CO1	K1
b.	Prove that R=<Z_6, +,x> is a commutative ring.	7	CO1	K2
	(OR)			
c.	Describe the classical encryption techniques in details.	10	CO1	K2
d.	Find GCD of 1070 and 1066 using Euclid algorithm.	5	CO1	K3
3.a.	Discuss the key scheduling and encryption process of the Blowfish algorithm with suitable diagrams and examples.	8	CO2	K2
b.	Evaluate encryption and decryption using RSA algorithm for the following. p=7,q=11;e=17;m=8	7	CO2	K3
	(OR)			
c.	Explain the AES with block diagram.	8	CO2	K2
d.	How is discrete logarithm evaluated for a number? Summarize the role of discrete log in the Diffie-Hellman key exchange in exchanging the secret key among two users? Find the discrete logarithm for log2 (9) mod 11.	7	CO2	K3
4.a.	How does screened host architecture for firewalls differ from screened subnet firewall architecture? Which offer more security for the information.	8	CO3	K2
b.	Formulate what are the requirements of Kerberos? Explain about Kerberos version.	7	CO3	K4
	(OR)			
c.	Describe Secure Electronic Transaction for E-Commerce transaction. Explain X.509 with neat diagram.	8	CO3	K2
d.	Differentiate between statistical anomaly detection and rule based intrusion detection system?	7	CO3	K1
5.a.	How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.	8	CO4	K3
b.	Analyze the MD5 message digest algorithm with necessary block diagram.	7	CO4	K4
	(OR)			
c.	Describe Digital signature algorithm & show how signing & verification is done using DSS.	8	CO4	K2
d.	Why it is important for secure email transaction. Briefly describe about the S/MIME certification processing.	7	CO4	K3

--- End of Paper ---