23HNIA0508

Code: 23A05601T

R23

B.Tech III Year II Semester (R23) Regular Examinations March/April 2026

CRYPTOGRAPHY & NETWORK SECURITY

(Common to CSE and CSE (CS))

Time: 3 hours | Max. Marks: 70

PART – A

(Compulsory Question)

*****

1		Answer the following: (10 X 02 = 20 Marks)	
	(a)	List and explain any one AES transformation functions.	2M
	(b)	Define the Feistel structure used in traditional block ciphers.	2M
	(c)	Given RSA parameters: p = 11, q = 13, and e = 7: Compute n and φ(n)	2M
	(d)	Define the principle of public key cryptography.	2M
	(e)	List any two major applications of cryptographic hash functions.	2M
	(f)	State the principle of the Secure hash algorithm (SHA).	2M
	(g)	What is Encapsulating Security Payload (ESP) in IPSec?	2M
	(h)	List the main phases in IKE and state what is established in any one phase.	2M
	(i)	What is the cryptographic parameters are established during the handshake phase?	2M
	(j)	Define the TLS and SSH based on layer of operation.	2M

PART – B

(Answer all the questions: 05 X 10 = 50 Marks)

2	(a)	Compare and contrast Data encryption standard (DES) and Advanced encryption standard (AES).	5M
	(b)	The plaintext "HELLO" is encrypted using the following monoalphabetic substitution mapping: A → Q, B → W, C → E, D → R, E → T, F → Y, G → U, H → I, … Encrypt the plaintext and show the ciphertext.	5M
		OR	
3	(a)	Define the Traditional block cipher structure. Explain how it provides confusion and diffusion in encryption.	5M
	(b)	Explain the OSI Security architecture and it's the role of security services and mechanisms.	5M
4	(a)	Differentiate between RSA and Elliptic curve cryptography (ECC).	5M
	(b)	User A and B use the Diffie-Hellman key exchange technique, a common prime q = 11 and a primitive root alpha = 7. If user A has private key XA= 5, What is A's public key YA?	5M
		OR	
5	(a)	Find 3^21 mod 11 using Fermat's little theorem.	5M
	(b)	Define finite fields GF (p) and GF (2^n). Explain their use in public key cryptography.	5M
6	(a)	Explain the role of X.509 certificates in Public Key Infrastructure (PKI) and list the main fields of the certificate.	5M
	(b)	What is a HMAC? Given a message M = "HELLO", explain how an HMAC is computed using a secret key K.	5M
		OR	

Contd. in Page 2

7	(a)	Explain in detail Message authentication function and its requirements.	5M
	(b)	Explain how public and private keys are used to secure internal emails with digital signatures, including signing and verification steps.	5M
8	(a)	What is an IP Security Policy (IPSP)? How does it determine the handling of incoming and outgoing IP packets?	5M
	(b)	Compare the security implications of using ESP with and without authentication.	5M
		OR	
9	(a)	Explain how the Security Parameter Index (SPI), sequence numbers, and cryptographic algorithms are used to enforce the policy.	5M
	(b)	Explain the Kerberos message exchanges between a client, Authentication Server (AS), and Ticket Granting Server (TGS), including tickets and authenticators.	5M
10	(a)	Explain the Transport Layer Security (TLS).	5M
	(b)	Illustrate the TLS handshake between a client and a web server, including the certificate exchange steps.	5M
		OR	
11	(a)	List the types of firewalls and explain its any two in detail.	5M
	(b)	Explain the placement and configuration of firewalls in a network. Why is firewall location critical for security?	5M

*****