Code No.: EC851PE	R20	H.T.No.			8	R						

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
IV–B.TECH–II–Semester End Examinations (Regular) – April - 2025
NETWORK SECURITY AND CRYPTOGRAPHY
(ECE)

[Time: 3 Hours] **[Max. Marks: 70]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 20 marks. Answer all questions in Part A.
Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART-A **(20 Marks)**

1.	a)	What is the role of padding in block cipher encryption?	[2M]
	b)	What is traffic confidentiality, and how does encryption help achieve it?	[2M]
	c)	What is the significance of modular multiplication in IDEA?	[2M]
	d)	Define the block size of Blowfish.	[2M]
	e)	What is the primary purpose of the Diffie-Hellman key exchange?	[2M]
	f)	Name two real-world applications of Elliptic Curve Cryptography.	[2M]
	g)	What is HMAC, and how is it different from a hash function?	[2M]
	h)	List three security properties of hash functions.	[2M]
	i)	Define Encapsulating Security Payload (ESP).	[2M]
	j)	What is a Denial of Service (DoS) attack?	[2M]

PART-B **(50 Marks)**

2.	a.	A Caesar cipher shifts "HELLO" to "KHOOR". Find the shift value and decrypt "OLSSV".	[5M]
	b.	Demonstrate how ECB and CBC modes handle a given plaintext with an example.	[5M]
		OR	
3.	a.	Encrypt "AB" using Affine Cipher: E(x)=(5x+8) mod 26.	[5M]
	b.	Describe the process of substitution-permutation network (SPN) in modern encryption.	[5M]
4.	a.	Encrypt "1234ABCD" using 3DES (EDE mode) with keys: K1=0x0123456789ABCDEF, K2=0xFEDCBA9876543210	[5M]
	b.	Compare the block sizes and key lengths of Blowfish, IDEA, and RC5.	[5M]
		OR	
5.	a.	Compute the first subkey of IDEA using a 128-bit key: K=0x0123456789ABCDEFFEDCBA9876543210.	[5M]
	b.	Explain the role of random number generation in encryption security.	[5M]
6.	a.	Compute 7^29mod 13 using Fermat's theorem.	[5M]
	b.	How does the RSA algorithm ensure secure communication?	[5M]
		OR	
7.	a.	Given Diffie-Hellman parameters: Prime p=23, base g=5, Alice's secret key = 6, Bob's secret key = 15, Compute the shared secret key.	[5M]
	b.	Why is randomness important in cryptographic key generation?	[5M]

8.a.	A system hashes passwords using SHA-512 instead of SHA-256. What security advantage does this provide?	[5M]
b.	Evaluate the security features of PGP vs. S/MIME.	[5M]
	OR	
9.a.	If a sender's private key is stolen, how does it impact the authenticity of signed documents?	[5M]
b.	Why is hashing used for password storage instead of encryption?	[5M]
10.a.	A company wants to secure email communication. Explain how S/MIME can be configured and used.	[5M]
b.	Analyze the potential vulnerabilities in VPN implementations and how they can be mitigated.	[5M]
	OR	
11.a.	You are securing a VoIP communication system. How can IPSec protocols enhance its security?	[5M]
b.	Evaluate the role of sandboxing in malware detection and prevention.	[5M]

****