Code No.: (R22CY401PC)	R22	H.T.No.			8	R						

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
II–B.TECH–II–Semester End Examinations (Supply) -December- 2025
CRYPTOGRAPHY AND NETWORK SECURITY
(CSC)

[Time: 3 Hours] **[Max. Marks: 60]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 10 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 **(10 Marks)**

1. a)	Classify the security attacks.	[1M]
b)	List out the security mechanisms.	[1M]
c)	State the principles of block cipher.	[1M]
d)	Name the four transformations used in AES.	[1M]
e)	Summarize the applications of cryptographic hash functions.	[1M]
f)	Show the requirements for digital signatures.	[1M]
g)	Which elements are encrypted when HTTPS is used?	[1M]
h)	What are the key factors contributing to the higher security risk of wireless networks compared to wired networks?	[1M]
i)	Why has PGP grown explosively and widely used?	[1M]
j)	Mention the benefits of IPSec.	[1M]

PART-B **(50 Marks)**

2.	Demonstrate the model for network security with a neat diagram.	[10M]
	OR	
3.	Examine the approach of substitution techniques with suitable examples.	[10M]
4.	Label the general depiction of the DES encryption algorithm and explain with suitable example.	[10M]
	OR	
5.	Perform encryption and decryption using the RSA algorithm, for the following: i. p = 3; q = 11, e = 7; M = 5 ii. p = 5; q = 11, e = 3; M = 9 iii. p = 7; q = 11, e = 17; M = 8 iv. p = 11; q = 13, e = 11; M = 7 v. p = 17; q = 31, e = 7; M = 2	[10M]
6.	Analyze the Message Digest generation using SHA-512 and describe the SHA-512 processing of single 1024-Bit block with a neat sketch.	[10M]
	OR	
7.	Show the general format of a X.509 certificate and discuss the purpose of each element in the certificate.	[10M]
8.	Inspect the role of secure sockets layer in providing the security services.	[10M]
	OR	
9.	Provide an overview of IEEE 802.11 wireless LAN.	[10M]
10.	Illustrate the IPsec architecture and describe the relationship among the elements in the architecture.	[10M]
	OR	
11.	Assess the mechanism for implementation of internet key exchange.	[10M]

****