Question Paper Code	13056

M.E. / M.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2024
Third Semester

M.E. - Computer Science and Engineering (with Specialization in Networks)
20PCNEL309 - CRYPTOGRAPHY AND WIRELESS NETWORK SECURITY
Regulations - 2020

Duration: 3 Hours   Max. Marks: 100

PART - A (10 × 2 = 20 Marks)
Answer ALL Questions

		Marks	K-Level	CO
1.	Mention the different aspects of security levels.	2	K2	CO1
2.	Illustrate meet in the middle attack done in 2-DES.	2	K2	CO1
3.	Justify the Diffie Hellman key exchange protocol is vulnerable.	2	K2	CO2
4.	Mention the signature function in DSS.	2	K2	CO2
5.	List the Steps involved in SSL required protocol.	2	K2	CO3
6.	Name any cryptographic keys used in PGP.	2	K2	CO3
7.	List any two applications of X.509 Certificate.	2	K2	CO4
8.	Discuss firewalls architecture.	2	K2	CO4
9.	Summarize the Limitations of Mobile Network Environment.	2	K2	CO5
10.	Illustrate Risk Mitigation with suitable scenario.	2	K2	CO5

PART - B (5 × 13 = 65 Marks)
Answer ALL Questions

			Marks	K-Level	CO
11.	a)	Convert "MEET ME" using Hill cipher with the key matrix Convert the cipher text back to plaintext.	13	K2	CO1

```
17  17  5
21  18  21
2   2   19
```

OR

			Marks	K-Level	CO
	b)	Explain the DES algorithm with a detailed diagram.	13	K2	CO1
12.	a)	Perform encryption and decryption using RSA algorithms for the following. P=17; q=11; e=7; M=88.	13	K2	CO2

OR

			Marks	K-Level	CO
	b) i)	Draw the general structure of DES and explain how encryption and decryption are carried out.	7	K2	CO2

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create   **13056**

| | ii) | Mention the strength of the DES algorithm. | *6* | *K2* | *CO2* |

| 13. | a) | Explain kerberos authentication mechanism with suitable diagram? | *13* | *K2* | *CO3* |

<div align="center">OR</div>

| | b) | Explain in detail about architecture of IP Security. | *13* | *K2* | *CO3* |

| 14. | a) | Explain in detail about the different types of Intrusion Detection Systems. | *13* | *K2* | *CO4* |

<div align="center">OR</div>

| | b) | Discuss in detail about the firewalls architecture and its purpose. | *13* | *K2* | *CO4* |

| 15. | a) | Explain in detail about IEEE 802.11 with suitable application. | *13* | *K2* | *CO5* |

<div align="center">OR</div>

| | b) | Describe in detail about Bluetooth Architecture and its components. | *13* | *K2* | *CO5* |

<div align="center">

PART - C (1 × 15 = 15 Marks)

</div>

| 16. | a) | Describe about the 3G Communication systems and Explain how authentication is established in 3GPP. | *15* | *K2* | *CO6* |

<div align="center">OR</div>

| | b) | Explain about the 3G Security Architecture and its Authentication and Key Agreement. | *15* | *K2* | *CO6* |