Guru Nanak Dev Engineering College, Ludhiana			
Department of Information Technology			
Program	B.Tech. (IT)	**Semester**	6th
Subject Code	PEIT-113	**Subject Title**	Network Security
Mid Semester Test (MST) No.	I	**Course Coordinator**	Dr. Randeep Kaur
Max. Marks	24	**Time Duration**	1:30 HRS
Date of MST	21-3-2025	**University Roll Number**	

Note: Attempt all questions

Q. No.	Question	COs, RBT level	Marks
			MM: 24
Q1	Explain the one-time pad scheme.	CO1, L2	2
Q2	Draft and organize the model of Network Security.	CO1, L4	2
Q3	Write the various security mechanisms.	CO1, L6	4
Q4	Construct a Playfair matrix with the key "engineering". And encrypt the message "test this process",	CO1, L6	4
Q5	Write the purpose of S-boxes in DES? Explain the avalanche effect.	CO1, L3	4
Q6	Discuss the Principles of Public Key Cryptosystems. Explain the RSA algorithm and explain the RSA with p=7, q=11, e=17, M=8. Discuss its merit.	CO2, L6, L2	8

Course Outcomes (CO)

Students will be able

1	Understand Symmetric Ciphers, Classical Encryption Techniques, Block Cipher and Data Encryption Standard.
2	Analyze Public Key Cryptography and RSA
3	Compare different authentication protocols
4	Evaluate Network Security requirements and Applications
5	Recognize and prevent system security threats

RBT Classification	Lower Order Thinking Levels (LOTS)			Higher Order Thinking Levels (HOTS)		
RBT Level Number	L1	L2	L3	L4	L5	L6
RBT Level Name	Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

GuruNanakDevEngineeringCollege, Ludhiana

DepartmentofInformationTechnology

Program	B.Tech.(IT)	**Semester**	6th
SubjectCode	PEIT-113	**SubjectTitle**	NetworkSecurity
MidSemesterTest (MST) No.	I	**Course Coordinator**	Dr.Randeep Kaur
Max.Marks	24	**Time Duration**	1:30 HRS
DateofMST		**UniversityRoll Number**	

Note: Attemptallquestions

Q.No.	Question	COs, RBT level	MM: 24 Marks
Q1	Identify the security services provided by digital signature.	CO3,L2	2
Q2	Design the role of Ticket Granting Server in inters realm operations of Kerberos.	CO4,L6	2
Q3	Explain in detail about X.509 authentication services.	CO3,L2	4
Q4	Differentiate transport and tunnel mode in IPsec.	CO5,L4	4
Q5	Discuss the working principle of the SET protocol and relate it to the concept of EST in the context of secure online transactions for e-commerce applications.	CO4, L6	4
Q6	With the help of a real-world example, explain the concept of forward secrecy. How does TLS 1.3 enforce forward secrecy by default, and why is it an essential security feature in modern encrypted communication?	CO5,L6	8

CourseOutcomes(CO)

Studentswillbeable

1	UnderstandSymmetricCiphers,ClassicalEncryptionTechniques,BlockCipherandData Encryption Standard.
2	AnalyzePubiicKeyCryptographyand RSA
3	Comparedifferentauthenticationprotocols
4	EvaluateNetworkSecurityrequirementsandApplications
5	Recognizeandpreventsystemsecuritythreats

RBT Classification	**LowerOrderThinkingLevels (LOTS)**			**HigherOrderThinkingLevels (HOTS)**		
RBTLevel Number	L1	L2	L3	L4	L5	L6
RBTLevelName	Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

[Total No. of Pages: 02]

[Total No. of Questions: 09]
Uni. Roll No. .....

Program: B.Tech. (Batch 2018 onward)
Semester: 6th
Name of Subject: **Network Security**
Subject Code: **PEIT-113**
Paper ID: **17213**
Scientific calculator is Not Allowed

Max. Marks: 60

Time Allowed: **03 Hours**

32 - 35

NOTE:

1. Parts A and B are compulsory
2. Part-C has Two Questions **Q8** and **Q9**. Both are compulsory, but with internal choice
3. Any missing data may be assumed appropriately

Part – A [Marks: 02 each]

Q1.

a. Discuss Eulers Theorem.
b. Classify attacks and their types. 1
c. Define digital signatures. 1
d. List the advantages of stenography. 1
e. Differentiate viruses and threats. 1
f. Analyze the importance of public and private keys. 1

Part – B [Marks: 04 each]

Q2. Solve RSA Algorithm by taking the prime number value p=3 and q=11. 2

Q3. Discuss in detail how the Network intrusion detection method SNORT can be used to counter intruders.

Q4. Classify the working of firewalls in network security. Discuss malicious software's and their types. 2

Q5. Justify the role of Kerberos in Network Security also explain Kerberos authentication mechanism with suitable example. 3

Q6. Distinguish between symmetric and asymmetric key cryptography in terms of security and performance with suitable examples. Analyze its advantages and limitations in real world applications. 2

Q7. Examine the role of Transport Layer Security in data transmission and how does it ensure confidentiality and integrity in data transmission. Compare with Secure socket layer also. 1

Part – C

[Marks: 12 each]

Q8. Illustrate in detail architectural components of IP Security and OSI security architecture? Also Explain Authentication Header and Encapsulation Security Payload. 8

OR

Explain AES and DES in detail? Comment "Triple DES is better than DES" if yes than why?

Q9. Analyze how public key and private keys contribute to the security of Digital Signatures. Evaluate the significance of key exchange in Diffie Hellman and how keys work in Diffie Hellman Algorithm. 6

OR

Compare and contrast the roles of MD5 and SHA algorithms in authentication protocols. Highlight their similarities and differences in terms of security and usage, also Identify the need and importance of Authentication Protocols.

****