



CRYPTOGRAPHY AND NETWORK SECURITY (CS701PC)

COURSE PLANNER

I. Course Overview:

The course covers fundamental aspects of security in a modern networked environment with the focus on system design aspects and cryptography in the specific context of network / internetwork security. It also dwells into basics of cryptographic techniques, algorithms and protocols required to achieve these properties; computational issues in implementing cryptographic protocols and algorithms; and system/application design issues in building secure networked systems.

II. Prerequisites:

- Computer networks.
- Design and analysis of algorithm.
- Engineering Mathematics

III. Scope of Course:

At the end of the course the student would:

- be in a position to understand Security concepts
- be able to write fluently Cryptography.
- be able to perform Security Related real world problems
- .

IV. Course Objectives:

COURSE OBJECTIVES:	
<i>At the end of the course, the students will be able to:</i>	
I	<i>Explain the importance and application of each of confidentiality, integrity, Authentication and availability.</i>
II	<i>Understand the various cryptographic algorithms.</i>
III	<i>Understand the basic categories of threats to computers and networks</i>
IV	<i>Describe the enhancements made to IPv4 by IPSec.</i>
V	<i>Discuss Web security and Firewalls.</i>



V. Course Outcomes:

S.No.	Course Outcomes (CO)	Knowledge Level (Blooms Level)
CO1	<i>Understand</i> basic cryptographic algorithms, message and web authentication and security issues.	L2: Understand
CO2	<i>Identify</i> information system requirements for both of them such as client and server	L1: REMEMBER
CO3	<i>Understand</i> the current legal issues towards information	L2: Understand
CO4	<i>Distinguish</i> and explain different protocol like SSL, TLS Vis-à-vis their applications	L4: ANALYZE
CO5	<i>Comprehend</i> and explain security services and mechanisms	L5: EVALUATE

VI. How Program Outcomes are Assessed:

Program Outcomes (PO)		Level	Proficiency assessed by
PO1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.	3	Assignment Mock test Quiz
PO2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	2	Assignment Mock test Quiz
PO3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	3	Assignment Mock test Quiz



Program Outcomes (PO)		Level	Proficiency assessed by
PO4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	3	Assignment Mock test Quiz
PO5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.	3	Mini Project
PO6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.	-	
PO7	Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	-	
PO8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.	2	
PO9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	2	Quiz
PO10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	2	Seminar
PO11	Project management and finance: Demonstrate knowledge and understanding of the engineering and	3	Hands On



Program Outcomes (PO)		Level	Proficiency assessed by
	management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.		Training
PO12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	2	Competitive Examinations

VII. How Program Specific Outcomes are Assessed:

Program Specific Outcomes (PSO)		Level	Proficiency assessed by
PSO1	Foundation of mathematical concepts: To use mathematical methodologies to crack problem using suitable mathematical analysis, data structure and suitable algorithm.	2	Technical Paper Writing
PSO2	Foundation of Computer System: The ability to interpret the fundamental concepts and methodology of computer systems. Students can understand the functionality of hardware and software aspects of computer systems.	2	Slip Test
PSO3	Foundations of Software development: The ability to grasp the software development lifecycle and methodologies of software systems. Possess competent skills and knowledge of software design process. Familiarity and practical proficiency with a broad area of programming concepts and provide new ideas and innovations towards research.	2	Research oriented Studies

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High) - : None



VIII. Course Content:

UNIT – I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security
Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

UNIT – II

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4. Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal All Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

UNIT – III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme. Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure

UNIT – IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH) Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security

UNIT – V

E-Mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

Books and References:

Text Books

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson



Education, 6th Edition

2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition

REFERENCE BOOKS:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition. 2. Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition

3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.

4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH 5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning 6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

IX. NPTEL Web Course:

https://onlinecourses.nptel.ac.in/noc19_cs28/preview

https://www.youtube.com/watch?v=1plMO7ChXMU&list=PLJ5C_6qdAvBFAuGoLC2wFGruYE2gYtev

NPTEL Video Course:

https://www.youtube.com/watch?v=VJelZrYc49c&list=PLLOxZwkBK52Ch0y2lLtfepy4Lt_SVkw03

<https://www.youtube.com/watch?v=vZ7YQ67CbtC>

<https://nptel.ac.in/courses/106105031/>

Relevant syllabus for GATE:

Authentication, Basis for public key cryptography, Digital signature and certificates , firewalls

Relevant syllabus for IES: Not Applicable



X. Course Plan

S.No	Week	Topics To be Covered	Link for PPT	Link for PDF	Course Learning Outcome	Teaching Aids	Text Book
1	1	UNIT - 1 Introduction	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define CNS	BB / PPT	T1
2		The need of Security, Security approaches	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Need of Security in Networks	BB / PPT	T1
3		Principles of security	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Security Principles	BB / PPT	T1
4		Types of Security Attacks, Security services, mechanisms	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Security attacks, security services and mechanisms	BB / PPT	T1
			https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
5	2	A model for Network Security	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Analyse the Network security models	BB / PPT	T1



			usp=sharing				
6		Cryptography concepts	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Cryptography concepts with the Cryptography mechanisms like, Encryption, Decryption, Transposition, Symmetric and Asymmetric methods	BB / PPT	T1
7		Introduction, Plain text, cipher text	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
8		Substitution Techniques	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
9	3	Transposition Techniques	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
10		Encryption and Decryption, Steganography	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
11			https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1



12		Symmetric Algorithm	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
13		Symmetric and Asymmetric Cryptography	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
14	4	Key Range and Key Size	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
15		Possible Types of Attacks	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
16		MOCK TEST - I					
17		Bridge Class - I					
18	5	UNIT-II Symmetric key ciphers, Block Cipher Principles	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define Symmetric Key Ciphers and Block Cipher Principles	BB / PPT	T1
19		DES	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Cryptography concepts with the Cryptography mechanisms like, Encryption, Decryption, Transposition,	BB / PPT	T1



20		AES	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Symmetric and Asymmetric methods	BB / PPT	T1
21		Blow Fish	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
22		RC5,RC4	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
23		IDEA	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
24	6	Block Cipher Operations	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Block Cipher Operation and Stream Cipher Concepts	BB / PPT	T1
25		Stream Cipher	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Analyse the Public Key Cryptosystems	BB / PPT	T1
26		Principles of Public Key Cryptosystems	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Analyse the RSA Algorithm	BB / PPT	T1



			3ChzVewzJKew? usp=sharing				
27	7	RSA Algorithm	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand the Elgamal Cryptography, Diffie - Hellman Exchange and Knapsack Algorithm related to Cryptography	BB / PPT	T1
28		Elgamal cryptography	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
29		Diffie-Hellman Key Exchange	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
30		Knapsack Algorithm	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
31		** Introdcuton To Network Simulators	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
32	8	UNIT-III Cryptographic Hash Functions	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define Hash Function realted to Cryptography	BB / PPT	T1
33		Message Authentication	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1



			2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	3ChzVewzJKew?usp=sharing			
34		Secure Hash Algorithm (SHA512),	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Analyse Secure Hash Algorithm and Authentication Requirement	BB / PPT	T1
35		Secure Hash Algorithm (SHA512), Authentication Requirement	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
37	9	MID TERM-I					
38							
39							
40	9	HMAC	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand HMAC and CMAC	BB / PPT	T1
41		CMAC	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
42			Digital signatures	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Digital Signature	BB / PPT
43	10	Elgamal Digital Signature Scheme	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Algamal Digital Signature Scheme	BB / PPT	T1



			3ChzVewzJKew?usp=sharing	ing			
44		Bridge Class - II					T1
45		Key Management and Distribution:	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define Key Management and Distribution	BB / PPT	T1
46		Symmetric Key Distribution Using	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Analyse Key Distribution using Symmetric & Asymmetric Encryption	BB / PPT	T1
47		Distribution of Public Keys	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Distribution of Public Keys	BB / PPT	T1
48		Kerberos	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Aquire a knowledge about Kerberos	BB / PPT	T1
49	11	X.509 Authentication Service,	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Undesratnd X.509 Authentication Service	BB / PPT	T1
			https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1



			https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
50		X.509 Authentication Service,	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
51		** NS2 Simulator Introduction and Applications	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Gather the knowledge about Network Simulator Application	BB / PPT	T1
52	12	Public – Key Infrastructure	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Public - Key Infrastructure	BB / PPT	T1
53		UNIT-IV Transport-level Security:	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define Transport Level Security	BB / PPT	T2
54		Web security considerations	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Gather the Knowledge about Web Security Considerations and Transport Layer	BB / PPT	T2
55	13	Secure Socket Layer	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Information & Transport Layer Responsibilities	BB / PPT	T2



			3ChzVewzJKew?usp=sharing	ing		
56		Transport Layer Security	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	BB / PPT	T2
57		HTTPS, Secure Shell (SSH)	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	BB / PPT	T2
58		Wireless Network Security:	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	BB / PPT	T2
59	14	Mobile Device Security	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	BB / PPT	T2
60		IEEE 802.11, Wireless LAN	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	BB / PPT	T2
61		IEEE 802.11i Wireless LAN Security			BB / PPT	T2
62		MOCK Test-II				
63		Bridge Class - III				



64	15	UNIT-V E-Mail Security: Pretty Good Privacy	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define Email Security	BB / PPT	T1
65		SMIME IP Security: IP Security overview	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand SMIME IP Security	BB / PPT	T1
66		IP Security architecture, Authentication Header	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand IP Security and Architecture	BB / PPT	T1
67		Encapsulating security payload	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
68	16	Combining security associations	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Understand Authentication Header, Encapsulation of Security Payload, Security Associations and Internet Exchange	BB / PPT	T1
69		Internet Key Exchange	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
70		Case Studies on Cryptography and security:	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1



			3ChzVewzJKew?usp=sharing				
71		Secure Multiparty Calculation	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
72		Virtual Elections, Single sign On	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing		BB / PPT	T1
73	17	Secure Inter-branch Payment Transactions	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	https://drive.google.com/drive/folders/1pN1W6_2vQ_qcwWF5SN3-3ChzVewzJKew?usp=sharing	Define the Case Study of Network Security, the Virtual Elections, Single Sign on Network Security	BB / PPT	T2
74		Cross site Scripting Vulnerability			Analyse the Secure Multiparty Calculation	BB / PPT	T2
77	18	MID TERM-II					

XI. Mapping Course Outcomes Leading to the Achievement of Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes (PO)												Program Specific Outcomes (PSO)		
	PO 1	PO 2	PO3	PO4	PO 5	PO6	PO 7	PO8	PO9	PO1 0	PO1 1	PO1 2	PS O1	PS O2	PSO 3
CO1	2	2	2	3	3	-	-	2	2	-	-	2	2	2	2
CO2	2	2	3	2	2	-	-	2	2	-	-	2	2	2	2
CO3	3	3	2	3	3	-	-	2	2	2	2	2	2	2	2
CO4	3	3	3	3	3	-	-	2	2	2	3	2	2	2	2



CO5	3	2	3	3	3	-	-	2	2	2	2	2	2	2	2
AVG	2.6	2.4	2.6	2.8	2.8			2	2	2	2.33	2	2	2	2

**1: Slight
(Low)**

**2: Moderate
(Medium)**

**3: Substantial
(High)**

- : None

XII. Question Bank

Descriptive Questions

Unit I

Short answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Define the terms security attacks?	[L1:REMEMBER]	CO1
2	Define the terms traffic analysis?	[L1:REMEMBER]	CO1
3	Define active attacks?	[L1:REMEMBER]	CO1
4	What is passive attacks? List the types of passive attacks?	[L1:REMEMBER]	CO1
5	Discuss about security mechanisms?	[L2;UNDERSTAND]	CO1
6	Discuss about Principles of Security?	[L2;UNDERSTAND]	CO1
7	What is Symmetric and Asymmetric Cryptography?	[L1:REMEMBER]	CO1
8	Define Steganography?	[L1:REMEMBER]	CO1
9	Difference between Passive and Active Security Threats?	[L4: ANALYZE]	CO1
10	Explain the model of network security?	[L2;UNDERSTAND]	CO1

Long answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Compare active and passive attacks?	[L4: ANALYZE]	CO1
2	Define security attack? Explain in detail about the various types of attacks for which internet work is vulnerable to?	[L1:REMEMBER]	CO1
3	Discuss about different types of various security services?	[L2: UNDERSTAND]	CO1
4	Describe network security model in detail?	[L2: UNDERSTAND]	CO1
5	Explain about transpose and substitution techniques?	[L2: UNDERSTAND]	CO1
6	Explain about different types of integrity constraints?	[L2: UNDERSTAND]	CO1
7	Discuss about the logical database Design?	[L2: UNDERSTAND]	CO1
8	Distinguish strong Symmetric and Asymmetric Cryptography?	[L4: ANALYZE]	CO1
9	Define the essential ingredients of the symmetric cipher?	[L1:REMEMBER]	CO1
10	List and briefly define categories of security mechanisms	[L1:REMEMBER]	CO1

Unit-II

Short answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	What are the differences between public-key	[L1:REMEMBER]	CO2



	and private-key encryption?		
2	Explain various modes of operations about block ciphers	[L2: UNDERSTAND]	CO2
3	Write a short note on location of encryption devices?	[L2: UNDERSTAND]	CO2
4	What is the purpose of S-Boxes in DES? `Explain the avalanche effect.	[L1:REMEMBER]	CO2
5	List four general categories of schemes for the distribution of public keys.	[L1:REMEMBER]	CO2
6	Difference between Differential Cryptanalysis and Linear Cryptanalysis?	[L4: ANALYZE]	CO2
7	Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?	[L1:REMEMBER]	CO2
8	Differentiate between block cipher and stream cipher?	[L4: ANALYZE]	CO2
9	List important design considerations for a stream ciphers	[L1:REMEMBER]	CO2
10	What are the essential ingredients of a public-key directory? What is a public-key certificate?	[L1:REMEMBER]	CO2

Long answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Define stream and block ciphers with examples?	[L1:REMEMBER]	CO2
2	Explain block cipher modes of operation?	[L2: UNDERSTAND]	CO2
3	Explain about AES?	[L2: UNDERSTAND]	CO2



4	Explain DES algorithm?	[L2: UNDERSTAND]	CO2
5	Explain about Blowfish?	[L2: UNDERSTAND]	CO2
6	Explain about Domain relational calculus?	[L2: UNDERSTAND]	CO2
7	Discuss RSA algorithms?,	[L2: UNDERSTAND]	CO2
8	Discuss Diffie – Hellman key exchange algorithms,?	[L2: UNDERSTAND]	CO2
9	Discuss about Knapsack Algorithm?	[L2: UNDERSTAND]	CO2
10	What are the principal elements of a public-key Cryptosystem? What are the roles of public and private key?	[L1:REMEMBER]	CO2

Unit-III

Short answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Define HMAC?	[L1:REMEMBER]	CO3
2	Define Kerberos	[L1:REMEMBER]	CO3
3	Define Hash function?	[L1:REMEMBER]	CO3
4	Discuss about SHA Algorithm	[L2: UNDERSTAND]	CO3
5	Differentiate between Symmetric and Asymmetric key	[L4: ANALYZE]	CO3
6	Compare and contrast Kerberos version 5 and version 4?	[L4: ANALYZE]	CO3
7	List out Services of X.509 Authentication	[L1:REMEMBER]	CO3
8	List out the Properties of Public Key	[L1:REMEMBER]	CO3
9	Define digital signature? Explain its role in	[L1:REMEMBER]	CO3



	network security		
10	Define Elgamal Digital Signature	[L1:REMEMBERING]	CO3

Long answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Define a message authentication code? List the difference between a message authentication code and a one-way hash function? In what ways can a hash value be secured so as to provide message authentication?	[L1:REMEMBER]	CO3
2	Discuss Symmetric key Distribution	[L2: UNDERSTAND]	CO3
3	Explain About Secure hash Algorithm(SHA-512)	[L2: UNDERSTAND]	CO3
4	Explain about Authentication Requirements	[L2: UNDERSTAND]	CO3
5	What requirements should a digital signature scheme satisfy? What is the difference between direct and arbitrated digital signature?	[L1:REMEMBER]	CO3
6	Explain About HMAC	[L2: UNDERSTAND]	CO3
7	Define Public Key? What are the three broad categories of public-key Cryptosystems? What requirements must a public-key cryptosystems fulfill to be a secure algorithm?	[L1:REMEMBER]	CO3
8	What four requirements were defined for Kerberos? What entities constitute a full-service Kerberos environment?	[L1:REMEMBER]	CO3
9	List the requirements for the use of a	[L1:REMEMBER]	CO3



	public-key certificate scheme?		
10	Demonstrate the purpose of the X.509 standard? What is a chain of certificates?	[L3: APPLY]	CO3

UNIT IV:

Short answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	List Out Web Security Considerations	[L1:REMEMBER]	CO4
2	Describe SSH	[L2: UNDERSTAND]	CO4
3	Define Transport Layer Security?	[L1:REMEMBER]	CO4
4	List notations used in HTTPS?	[L1:REMEMBER]	CO4
5	Define IEEE 802.11	[L1:REMEMBER]	CO4
6	Define Wireless Security	[L1:REMEMBER]	CO4
7	Differentiate between IEEE 802.11&802.11i	[L4: ANALYZE]	CO4
8	DiscussIEEE 802.11 Wireless LAN	[L2: UNDERSTAND]	CO4
9	Explain about e-mail compatibility?	[L2: UNDERSTAND]	CO4
10	Describe about Mobile Device Security?	[L2: UNDERSTAND]	CO4

Long answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Discuss about SSL in detail	[L2: UNDERSTAND]	CO4
2	Define the steps are involved in the SSL Record Protocol transmission?	[L1:REMEMBER]	CO4



3	List and briefly define the parameters that define an SSL session connection, Session State	[L1:REMEMBER]	CO4
4	What services are provided by the SSL Record Protocol?	[L1:REMEMBER]	CO4
5	Explain SSH in detail	[L2: UNDERSTAND]	CO4
6	Explain TLS in detail	[L2: UNDERSTAND]	CO4
7	Explain in detail about IEEE 802.11i Wireless LAN	[L2: UNDERSTAND]	CO4
8	Discuss in detail about HTTPS	[L2: UNDERSTAND]	CO4

Unit-V

Short answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Why is the segmentation and reassembly function in PGP needed?	[L1:REMEMBER]	CO5
2	Define Authentication	[L1:REMEMBER]	CO5
3	Describe the Security Combining Associations	[L2: UNDERSTAND]	CO5
4	Define IP	[L1:REMEMBER]	CO5
5	Define MIME	[L1:REMEMBER]	CO5
6	Discuss about Internet Key Exchange?	[L2: UNDERSTAND]	CO5
7	What is Encapsulating security payload?	[L1:REMEMBER]	CO5
8	Explain about Virtual Elections?	[L2: UNDERSTAND]	CO5
9	Differentiate between MIME & S/MIME	[L4: ANALYZE]	CO5
10	Discuss about Cross Site Scripting	[L2: UNDERSTAND]	CO5

Long answer Questions

S.NO	Questions	Bloom's Taxonomy	Course Outcome
1	Write about Case Studies on Cryptography and security	[L2: UNDERSTAND]	CO5
2	Compare I/O costs for all file organizations	[L4: ANALYZE]	CO5
3	Explain about Pretty Good Privacy, how does PGP use the concept of trust	[L2: UNDERSTAND]	CO5
4	Discuss about Secure Multi Party Calculation ,Secure Single Sign ON	[L2: UNDERSTAND]	CO5
5	Discuss in detail about IP Security	[L2: UNDERSTAND]	CO5
6	Explain about Secure Inter branch Transitions	[L2: UNDERSTAND]	CO5
7	Give examples of applications of IPSec. What services are provided by IPSec?	[L1:REMEMBER]	CO5
8	Explain about IP Security Architecture	[L2: UNDERSTAND]	CO5
9	Explain about Authentication Header?	[L2: UNDERSTAND]	CO5
10	Write in detail about S/MIME IP Security	[L2: UNDERSTAND]	CO5

Objective-Type Questions

UNIT-1

- 1) The protection of transmitted data from passive attack is_____
a) Authentication b) Access control c) Confidentiality d) Non-REpudation
- 2) Fabrication is attack on _____
a) Confidentiality b) Non-REpudation c) Authentication d) Availability
- 3) A hijacker can create a new session using the stolen data in _____
a) Network Layer b) Application Layer c) Transport Layer d) Data link Layer
- 4) _____ Responsible for publishing the RFCs, with approval of the IESG
a) IAB b) IESG c) IBA d) IETF
- 5) Modification of data is an attack on _____
a) Integrity b) Confidentiality c) Authenticity d) Availability
- 6) Expansion of B2B is _____



- 7) Denying of message by destination is called_____
- 8) In network security model the secret-key is distributed to the principles by_____
- 9) Releasing of message to an unauthorized person is called as_____
- Security service_____requires that neither the sender nor the receiver of a message be able to deny the transmission
- 10)_____is used by the participants to exchange keys without contacting public-key authority.

UNIT-2

- 1) Size of a single buffer register in MDS is_____
- 2) DES is a_____algorithm
- 3) AES requires_____number of bits for plaintext
- 4) In DES the term E/P stands for_____
- 5) Maximum allowable padding length in MDS is upto_____
- 6) Number of rounds in DES
 - a) 8
 - b) 16
 - c) 32
 - d) 4
- 7) One of the best application that use DES is
 - a) ATM
 - b) digital significance
 - c) Digital equipment
 - d) none of these
- 8) Which algorithm doesn't use feistel cipher technique
 - a) DES
 - b) IDEA
 - c) RSA
 - d) RC5
- 9) Initialization vector is not used in
 - a) CBC
 - b) CFB
 - c) OFB
 - d) none of these
- 10) RSA algorithm is not based on
 - a) exponentials
 - b) modules numbers
 - c) prime numbers
 - d) ring numbers

UNIT-3

- 1) MLA in S/MIME represents_____
- 2) S/MIME uses_____algorithm for encrypting signature
- 3) In PGP service for E-Mail compatibility _____algorithm is used.
- 4) RFC_____defines a format for text messages that are sent using electronic mail.
- 5) Absolute requirement of the specification is called _____.
- 6) MIME version of parameter value is
 - a) 4.0
 - b) 2.0
 - c) 3.0
 - d) 1.0
- 7) S/MIME uses which algorithm for encrypting session keys
 - a) DES
 - b) RSA
 - c) Diffie –helmen
 - d) IDEA
- 8) For message encryption and decryption algorithm in S/MIME is
 - a) DES
 - b) IDEA
 - c) 3DES
 - d) Blowfish
- 9) Fragmentation of large message in to number of part is called as
 - a) message/partial sub type
 - b) Message/external body
 - c) message/application type
 - d) All the above
- 10) Which MIME content type indicates that the body contains multiple independent parts
 - a) More Type
 - b) Application Type
 - c) Multipart type
 - d) Application subtype

UNIT-4

- 1) IP Security is provided in _____ layer.
- 2) The size of the initiator cookie in ISAKMP header is _____



- 3) IPv6 header has a fixed size of _____ objects.
- 4) The number of fields in the IPv4 and IPv6 headers respectively are _____
- 5) The size of the security parameters index fields is ESP format is _____
- 6) SSL provides security at _____ layer
- 7) _____ provides secured communication between client and server.
- 8) The protocol that is used to change the secure channel to new speed is _____
- 9) In the construction of dual signature, the encryption algorithm is _____
- 10) Alert protocol uses _____ bytes

UNIT-5

- 1) The protocol used for the management of TCP/IP networks is the _____
- 2) An _____ is a data variable that represents one aspect of the managed agent
- 3) A person who is not authorized to use the system but penetrates it is called _____
- 4) Virus places an identical copy of itself into other program in _____ phase
- 5) SNMP V1 operates on _____ protocol
- 6) _____ database lists the access privileges of each subject and protection attributes of each subject
- 7) An example of _____ gateway implementation is the socks package
- 8) _____ is a non negative integer that may be incremented but not decremented until it is reset by management action
- 9) The socks service is located on TCP port number _____
- 10) Failures resource exhaust counter measure _____ activity

GATE

- 1) A sender S sends a message m to receiver R, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place.
 - (I) S can launch a birthday attack to replace m with a fraudulent message.
 - (II) A third party attacker can launch a birthday attack to replace m with a fraudulent message.
 - (III) R can launch a birthday attack to replace m with a fraudulent message.

1. Which of the following are possible security violations? []

(A) (I) and (II) only (B) (I) only (C) (II) only (D) (II) and (III) only

2. Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires []

(A) Anarkali's public key (B) Salim's public key (C) Salim's private key

(D) Anarkali's private key.

3. Which of the following are used to generate a message digest by the network security



protocols? []

(P) RSA (Q) SHA-1 (R) DES (S) MD5

(A) P and R only (B) Q and R only (C) Q and S only (D) R and S only

4. What is the number of possible 3 x 3 affine cipher transformations ?

a.168 b. 840 c. 1024 d. 1344

5. Super-Encipherment using two affine transformations results in another affine transformation.

a. True b. False c. May be d. Can't say

6. Confusion hides the relationship between the ciphertext and the plaintext.

a. True b. False c. May be d. Can't say

7. The S-Box is used to provide confusion, as it is dependent on the unknown key.

a. True b. False c. May be d. Can't say

8. DES follows

a. Hash Algorithm b. Caesars Cipher c. Feistel Cipher Structure d. SP Networks

9. The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key

a.12 b.18 c.9 d.16

10. The DES algorithm has a key length of

a. 128 Bits b. 32 Bits c. 64 Bits d. 16 Bits

Websites addresses:

- <http://nptel.iitm.ac.in/video.php?subjectId=106106093>
- <http://www.sqlcourse.com/index.html>
- <http://www.tutorialspoint.com/sql/>

Expert details:

1) Prof. **Sourav Mukhopadhyay** ,IIT Khargpur

Journals (National & International):

1) International Journal of Intelligent Information and Database Systems



(<http://www.inderscience.com/jhome.php?jcode=ijjids>)

2) The Journal of Biological Databases and Curation
(<http://database.oxfordjournals.org/content/current>)

List of topics for students seminar s:

- 1) Electrical curve Cryptography
- 2) RSA Algorithm
- 3) Kerberos
- 4) PGP
- 5) SMIME

Case Studies / Small Projects:

- 1) Virtual Elections
- 2) Single sign On