BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, Pilani
Hyderabad Campus

Academic – Graduate Studies and Research Division
SECOND SEMESTER 2021-2022
(COURSE HANDOUT PART II)

17.01.2022

In addition to Part-I (General handout for all courses appended to the timetable) this portion gives further specific details regarding the course:

Course No.	:	**CS G513**
Course Title	:	**Network Security**
Instructor-In-Charge	:	**Dr. Rajib Ranjan Maiti**

Description : This course examines issues related to network and information security. Topics include security concepts, security attacks and risks, security architectures, security policy management, security mechanisms, cryptography algorithms, security standards, security system interoperation and case studies of the current major security systems

1. Scope

Though this course is self-contained, a basic understanding of computer network and cryptography can help greatly to grasp the course content. This course will provide a basic understanding of the policies and practices adopted to monitor and prevent unauthorized access, misuse, modification, or denial of a availability of resources over computer network. It will provide an understanding of the algorithms and protocols to ensure the security of networked resources. We have divided the complete course into three different sections.

The first section of the course covers some of the important **topics in cryptography**. This will help to gain a level of understanding of cryptographic techniques that are used to develop security protocols to protect networking resources. In addition, it covers some basics of **Number Theory,** without going into much details**,** to develop a mathematical background used in various cryptographic techniques.

The second section of the course covers the protocols, which use cryptographic primitives to solve various security problems such as key management and distribution, user authentication etc. Basically, this section will demonstrate how cryptographic techniques are used to solve the problems related to network security.

Finally, the **third section** covers application of cryptographic protocols in real world communication. This includes application layer security (https and email security), transport layer security (TLS or SSL) and IP layer security (IPSec). This section will also explore the recent topics in cyber-attacks.

2. Objectives

On successful completion of the course, the students should be able to:

a. understand basic principles and results of the theory of secure communication;
b. know principles and problems of basic cryptosystems for encryption (both secret and public key), digital signing and authentication;
c. know methods to create core cryptographic protocols primitives;
d. practically use simple cryptosystems;
e. know how the real protocols enabling secure communication over internet, various tools and techniques to protect as well as attack a computer network.

3. Text Books

(T1) William Stallings, “Cryptography and Network Security: Principles and Practice,” 7th Edition, Pearson, 2017

4. Reference Books:

(R1) D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), 3e, CRC Press.

(R2) B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, 2e, John Wiley & Sons.

(R3) Bernard Menezes: Network Security & Cryptography, 1st Edition, Cengage Learning, Delhi, 2011.

(R4) B. A. Forouzan, D. Mukhopdhyay, “Cryptography and Network Security”, McGraw Hill, 3rd Edition. 2017

Note: In this course, we will follow (T1) as textbook. However, the students are suggested to consult with the books (R4) and research papers for **Modern Cryptography and Network Security**.

5. Lecture Plan

Lecture #	Learning Objectives	Topics to be covered	Reading
Section A: Cryptographic Techniques and Algorithms			
1	Course overview	Course Introduction, evaluation plan, OSI model and Network Security	Lecture Slides, Ch 1
2, 3	To learn mathematics for Cryptography and symmetric encryption	Integer arithmetic, GCD, Euclid's Algorithm, Modulo, congruence, matrices, group, ring, field, GF(2^n), prime numbers, primality testing	Ch. 2, 5
4, 5	To learn symmetric	**Classical Encryption Techniques:** Symmetric Cipher	Ch. 3

	encryption and stream ciphering	Model, Cryptanalysis, Substitution, affine cipher, One-Time Pad (OTP), Transposition (Permutation) Ciphers, Steganography, playfair cipher, Vigenere cipher, hill cipher, attacks on classical encryption	
6, 7	To learn modern encryption	**DES:** Feistel Cipher Structure, Data Encryption Standard (DES), Avalanche in DES, Strength of DES, Differential Cryptanalysis, Linear Cryptanalysis, Block Cipher Design Principles	Ch. 4
8, 9	To apply number theoretic principles	**Basic Concepts in Number Theory and Finite Fields :** Algebraic Structures, Polynomial Arithmetic, Fermat's Little Theorem, Euler Totient Function, Euler's Theorem, Chinese Remainder Theorem, SIS and LWE Assumptions.	Ch2, Ch5
10, 11	To learn modern encryption	**AES:** Basic Structure of AES, Substitute Bytes, Shift Rows, Mix Columns, AES Arithmetic, Add Round Key, AES Key Expansion, AES Example Key Expansion, AES Example Encryption, AES Example, Avalanche AES Decryption	Ch6
12	To learn Key Stream basics	**Pseudo Random Number Generation and Stream Ciphers**: Pseudo Random Numbers, Linear-Congruential Generators, Blum Blum Shub Generator, Using Block Ciphers as PRNGs, RC4 Stream Ciphers, A5/1	Ch 8
13	To learn operation using DES and AES	Double-DES, Triple-DES, DES-X, Electronic Codebook Book (ECB), Cipher Block Chaining (CBC), Message Padding, Cipher Text Stealing (CTS), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR).	Ch7
14, 15	To learn asymmetric encryptions basics	**Public Key Cryptography:** Public Key Encryption, RSA Encryption, ElGamal, D-H, ECC, Robin cryptosystem	Ch. 9, Ch10
16, 17	To learn basic attacks on asymmetric crypto systems	**Attacks on each of cryptosystems:** factorization attack**,** chosen cipher attack**,** broadcast attack, related message attack, short pad attack, revealed exponentiation attack, low exponent attack, plaintext attack, short message attack, cycling attack, unconcealed message attack, common modulus attack, timing attack, power attack, known plaintext attack, security of ECC	Ch. 9
18, 19	To understand differences cryptographic hashes	**Cryptographic Hash Functions:** Hash Function, Cryptographic Hash Functions, Birthday Problem, Block Ciphers as Hash Functions, Secure Hash Algorithm	Ch. 11

		(SHA), MD5, Trapdoor	
20, 21	To ensure message integrity	**Message Authentication Codes:** Message Security Requirements, MAC, HMAC, Using Symmetric Ciphers for MACs. Cipher-based Message Authentication Code (CMAC), Authenticated Encryption, CCM	Ch. 12
Section B: Cryptographic Protocols			
22, 23	To learn to generate user authentication codes	**Digital Signatures:** Digital Signature Model and requirements, Attacks, Forgeries, Digital Signature Standard (DSS), Digital Signature Algorithm, Key Generation, Signature Creation and verification, Forking Lemma	Ch. 13
24, 25	To learn challenges in key management	**Key Management and Distribution:** Key Distribution Using KDC, Key Distribution Using Public Keys, Secret Key Distribution with Confidentiality and Authentication, Distribution of Public Keys, Public-Key Certificates PKI, PKIX, and X.509, CA Hierarchy	Ch. 14
26, 27	To learn to allow access to users	**User Authentication Protocols:** User Authentication, Needham Schroeder Protocol, One-Way Authentication for Email, Kerberos, Remote User Authentication Using Public Keys	Ch. 15
Section C: Network Security			
28, 29	To learn applications of cryptosystems	**Advanced Protocols:** Zero knowledge Proofs, Identity based public key, Secure elections, Secure multi-party computation	R2. Ch. 5, Lec. notes
30, 31	To learn network traffic and the security	**Secure Socket Layer:** SSL Architecture, SSL Handshake Protocol, Handshake Messages, SSL Change Cipher Spec Protocol **Transport Level Security (TLS):** HTTPS **Secure Shell** (SSH), SSH Protocol Stack, SSH Transport Layer Protocol, SSH User Authentication Protocol, SSH Connection Protocol, **Port Forwarding**	Lecture Slides, Ch 17
32	To learn email security	**Electronic Mail Security:** Email Security Enhancements, Pretty Good Privacy (PGP), S/MIME	Ch. 19
33,34	To understand traffic security at routers	**IPSec:** overview, ESP, AH, IKE, VPN	Ch. 20

35, 36	To learn data link layer security	**Wireless Network Security**: Wireless Network Threats, Countermeasures Mobile Device Security Wi-Fi Operation IEEE 802.11 Architecture IEEE 802.11 Services Wired Equivalent Privacy (WEP), 802.11i Wireless LAN Security.	Ch. 18
37,38	To learn additional security mechanisms	**Intrusion Detection**: Concepts, Intrusion vs. Extrusion Detection Examples of Intrusion Categories of Intruders Hacker Behavior, Insider Behavior, Intrusion Techniques, Password Guessing and Capture Notification Alarms, Types of IDS	Lecture Slides
39,40	To understand Nnature of malicious codes	**Malicious Software:** Malicious Software, Backdoor or Trapdoor, Logic Bomb, Trojan Horse, Mobile Code Multiple-Threat Malware, Viruses, Behavior-Blocking Software, Worms, Distributed Denial of Service Attacks (DDoS)	(online) Ch21

6. Evaluation Plan:

Sl. No.	**Component & Nature**	**Weightage**	**Duration**	**Date & Time**
1.	Mid-Sem. Exam. **(Open Book)**	30%	90 min	As announced by TimeTable
2.	Other Components: Weekly Lab Assignments (**Open Book**)	10%	Details will be announced in the class	
3.	Other Components: Lab Test -1 & Lab Test – 2 (**Open Book**)	20%	Details will be announced in the class	
3.	End-Sem. Exam **(Open Book)**	40%	120 min.	As announced by TimeTable

Note: 40% of the evaluation to be completed by midsem grading.

"For Comprehensive exam and Mid-semester Test, the mode (offline/online) and the duration are subject to changes as decided by the AUGSD/Timetable division in future."

Note: All course related announcements will be made over **CMS**.

7. Make-up Policy: **No makeup will be given to Project/Assignment/Quiz.** For Mid-Sem and End-Sem examinations, however, Make-up will be granted strictly on prior permission and on justifiable grounds only. Students applying for make-up on medical grounds need to submit a certificate from a doctor.

8. Chamber Consultation Hour: Would be announced in the class.

9. Academic Honesty and Integrity Policy: Academic honesty and integrity are to be maintained by all the students throughout the semester and any type of academic dishonesty will be handled strictly.

Instructor-In-Charge
CS G513