BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, Pilani
Hyderabad Campus

SECOND SEMESTER 2019-2020,
COURSE HANDOUT (PART-II) **Date: 1/1/2020**

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 (BITS-Pilani, Hyderabad)**

Course 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. Objective

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.

2. Text Books

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

3. 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, I 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**.

Lecture Plan

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

		cipher, One-Time Pad (OTP), Transposition (Permutation) Ciphers, Product Ciphers, Rotor Machines, Rotor Machine Principle, Steganography, playfair cipher, Vigenere cipher, hill cipher, attacks on classical encryyption	
5, 6, 7	Symmetric encryption and block ciphering	**DES:** Feistel Cipher Structure, Data Encryption Standard (DES), Avalanche Effect, Avalanche in DES, Strength of DES, Differential Cryptanalysis, Linear Cryptanalysis, Block Cipher Design Principles **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 **Extensions of 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).	Ch. 4, 6,7
8	Generate Key Stream	**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
9,10	Apply number theoretic principles	**Basic Concepts in Number Theory and Finite Fields :** Euclid's Algorithm, Modular Arithmetic, Algebraic Structures, Galois Fields, Polynomial Arithmetic, Fermat's Little Theorem, Euler Totient Function $\phi(n)$, Euler's Theorem, Chinese Remainder Theorem etc	Ch. 2
11,12,13	Asymmetric encryptions	**Public Key Cryptography:** Public Key Encryption, RSA Encryption, ElGamal, D-H, ECC, Robin cryptosystem **Attacks on each of cryptosystems:** factorization	Ch. 9,10

		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	
14	Differentiate cryptographic hashes	**Cryptographic Hash Functions:** Hash Function, Cryptographic Hash Functions, Birthday Problem, Block Ciphers as Hash Functions, Secure Hash Algorithm (SHA), MD5	Ch. 11
15,16	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
17, 18	Recent cyber-attacks	**Recent attacks** on smart grid, smart city, smart home, CPS, blockchain, etc. and students presentations, botnets	Research papers
Section B: Cryptographic Protocols			
19,20	Generate user authentication codes	**Digital Signatures:** Digital Signature Model, Attacks, Forgeries, Digital Signature Requirements, Digital Signature Standard (DSS), DSS vs. RSA Signatures, Digital Signature Algorithm (DSA), DSA Key Generation, DSA Signature Creation, DSA Signature Verification	Ch. 13
21, 22	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
23,24	Allow access to users	**User Authentication Protocols:** User Authentication, Replay Attacks, Needham Schroeder Protocol Denning's Modification, One-Way Authentication for Email, Kerberos,	Ch. 15

		Remote User Authentication Using Public Keys	
Section C: Network Security			
25,26,27	Some applications of cryptosystems	**Advanced Protocols:** Zero knowledge Proofs, Identity based public key, Secure elections, Secure multi-party computation, Digital cash, Bitcoin	R2. Ch. 5, Lec. notes
28,29,30	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 and its Use, **Secure Shell** (SSH), SSH Protocol Stack, SSH Transport Layer Protocol, SSH User Authentication Protocol, SSH Connection Protocol, **Port Forwarding**	Lecture Slides, Ch 17
31,32	Securing emails	**Electronic Mail Security:** Email Security Enhancements, Pretty Good Privacy (PGP), S/MIME	Ch. 19
33,34	Securing traffic at routers	**IPSec:** overview, ESP, AH, IKE, VPN	Ch. 20
35, 36	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	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	Nature 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)	Lecture Slides
41,42	Advanced topics in cyber	Security challenges in IoT, CPS and Blockchain,	Lecture

	security	SQL injection, Biometric, Security and privacy in smart phone	slides

Evaluation Plan:

Sl. No.	Component & Nature	Weightage	Duration	Date & Time
1.	Mid-Sem. Exam. **(Closed Book)**	20%	1 Hrs. 30 Mins.	4/3 , 9.00 - 10.30AM
2.	Project **(Open Book)**	20%	Details will be announced in the class	
3.	Programming Assignments **(Open Book)**	10%	Perform cryptanalysis (breaking an encryption scheme without the key)	
4.	Quiz (**Open Book**)	10%	Based on the use of Wireshark to capture packets, simulate attacks and diagnose them.	
5	Reading assignments (**Open book**)	5%	Find recent cyber-attacks and Demonstrate	
3.	End-Sem. Exam **(Closed Book)**	35%	3 Hrs.	**06/05 AN**

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

Make-up Policy: No makeup will be given to Project/Assignment/Quiz. For tests, 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 confirmation letter from the concerned warden as well as from a doctor.

Chamber Consultation Hour: Would be announced in the class.

Malpractice Regulations: The following regulations are supplementary to BITS-wide policies regarding malpractices:

1. Any student or team of students involved/found involved in malpractices in working out assignments / projects will be awarded a zero for that assignment / project and will be blacklisted.

2. Any student or team of students found repeatedly – more than once across all courses – involved in malpractices will be reported to the Disciplinary Committee for further action. This will be in addition to the sanction mentioned above.
3. A malpractice - in this context - will include, but not be limited to:
   - Submitting some other student's / team's solution(s) as one's own;
   - Copying some other student's / team's data or code or other forms of a solution;
   - Seeing some other student's / team's data or code or other forms of a solution;
   - Permitting some other student / team to see or copy or submit one's own solution;
   - or other equivalent forms of plagiarism wherein the student or team does not work out the solution and use some other solution or part thereof (such as downloading it from the LAN or the Web).

- The degree of malpractice (the size of the solution involved or the number of students involved) will not be considered toward mitigating evidence. Failure on the part of instructor(s) to detect malpractice at or before the time of evaluation may not prevent sanctions based on later evidence.
- In this context, a malpractice does NOT include the following:
  a. Asking help from a third person doubts, as long as there is no overt or covert intend/attempt to positively contribute towards the solution of Assignment/Project.
  b. Pointing out compilation errors. (As long as there is no active contribution to the semantics of the code.)

  Either case, the fact that help was sought must be acknowledged while submitting the work

Academic Honesty and Integrity Policy: Academic honesty and integrity are to be maintained by all the students throughout the semester and no type of academic dishonesty is acceptable.

Instructor-In-Charge
CS G513