



Date: 04/01/2016

Instruction Division
Second Semester (2015-2016)
Course Handout (Part II)

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

Course No. : CS G513 & SS G513
Course Title : Network Security
Instructor-In-Charge : SK Hafizul Islam (Pilani)

Scope and Objectives

This course will give you the brief ideas about cryptographic techniques and their applications in Cryptography and Network Security. In addition, we will also learn some basics of number theory, which is required in order to understand the mathematical background of various cryptographic techniques.

Note: In this course, I will follow two books [T1] & [R1]. However, the students are suggested to consult with the books [R2] - [R5] for **Modern Cryptography and Network Security**.

Text Book

[T1] W. Stallings: Cryptography and Network Security, 5e, Pearson.

References

- [R1] B. A. Forouzan & D. Mukhopadhyay: Cryptography and Network Security, 2e, McGraw-Hill.
- [R2] D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), 3e, CRC Press.
- [R3] B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, 2e, John Wiley & Sons.
- [R4] Bernard Menezes: Network Security & Cryptography, 1st Edition, Cengage Learning, Delhi, 2011.
- [R5] A. Kahate: Cryptography and Network Security, 2nd Edition, TMH Education Private Limited, New Delhi.



Please Consider Your Environmental Responsibilities
Do Not Print Unless Necessary



Lecture Plan:

Topics	References	No. of Class
PART – I		
Introduction to Network Security, Trends, Architecture, Levels, Attacks, Services, Mechanism, Response Teams, Network Security model and Standards.	T1, R1-R4	1
PART – II		
<p><u>Classical Encryption Techniques:</u> Basics of Cryptography, Simple Symmetric Ciphers, General thought on breaking cryptosystems, Modular Arithmetic, Substitution and, Transposition Ciphers, Stream Cipher, RC4, Random Numbers, Cryptographically Secure Random Number Generators, One Time Pad</p> <p><u>Block Ciphers and the Data Encryption Standard:</u> Block Cipher Principles, Data Encryption Standard (DES), Block Cipher Design Principles,</p> <p><u>Advanced Encryption Standard</u> The Extended Euclidean Algorithm, Galois Fields, AES Structure, AES Round Functions, AES Key Expansion, AES Implementation</p> <p><u>Block Cipher Operation</u> Multiple Encryption, 3DES, DESX, Modes of Operations: Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode.</p> <p><u>Cryptographic Hash Functions and MAC:</u> Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm, MAC from hash functions and block ciphers.</p>	T1, R1-R4	5
PART – III		
<p><u>Number Theory:</u> Relevant Number Theory for public-key algorithms, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality.</p> <p><u>Public-Key Cryptography:</u> Principles of Public-Key Cryptosystems, RSA, ElGamal Cryptosystem, Diffie-Hellman Key Exchange, Attacks in RSA, RSAES-OAEP.</p>	T1, R1-R4	4
PART – IV		
<p><u>Digital Signatures</u> Digital Signatures, RSA Digital Signature, ElGamal Digital Signature Scheme, Schnorr Digital Signature Scheme, Digital Signature Standard (DSS)</p>	T1, R1-R4	3





PART – V		
User Authentication Protocols Remote User Authentication Principles, Remote User Authentication Using Symmetric Encryption, Kerberos, Remote User Authentication Using Asymmetric Encryption Key Management and Distribution Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure	T1, R1-R4	6
PART – VI		
Transport Layer Security Secure Sockets Layer (SSL), Transport Layer Security (TLS) Electronic Mail Security Pretty Good Privacy (PGP), S/MIME Secure Electronic Transaction (SET) Protocol IP Security IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, IKE, Virtual Private Network (VPN), Wireless Security, Intruders, Firewall and Malwares.	T1, R1-R4	7

Evaluation Plan:

Sl. No.	Component & Nature	Weightage	Duration	Date & Time
1.	Mid-Sem. Exam. (Closed Book)	25%	1 Hrs. 30 Mins.	14/3 11:00 - 12:30 PM
2.	Quiz	5%	Details will be announced in the class	
3.	Project/Assignment	40%	Details will be announced in the class	
3.	End-Sem. Exam (Closed Book)	30%	3 Hrs.	3/5 AN

Note: All course notices will be displayed on the CSIS Notice Board only.

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:





Please Consider Your Environmental Responsibilities
Do Not Print Unless Necessary



BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, Pilani Pilani Campus

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

Instructor-In-Charge
CS G513 & SS G513



Please Consider Your Environmental Responsibilities
Do Not Print Unless Necessary