BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI

INSTRUCTION DIVISION

FIRST SEMESTER 2020-2021

COURSE HANDOUT(PART-II)

Date: 17/08/2020

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.	**: BITS F463**
Course Title	**: Cryptography**
Instructor In Charge	: Ashutosh Bhatia (ashutosh.bhatia@pilani.bits-pilani.ac.in)

Description: This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. We will cover topics such as encryption (secret-key and public-key), message integrity, digital signatures, user authentication, key management, cryptographic hashing, Network security protocols (SSL, IPsec), public-key infrastructure, digital rights management, and a bit of advancement in modern cryptology such as Identity Based Encryption, Steganography and Watermarking, Quantum Cryptographic and Zero-Knowledge protocols.

Prerequisites: The course is self-contained, however a basic understanding of probability theory, information theory, complexity theory and modular arithmetic from number theory will be helpful. The course is intended for advanced undergraduates and master students.

Course Objectives: Lectures deal with the basic methods to solve three key problems of the transmission of information. All three problems are of large practical importance and their solutions are based on elegant theoretical results. On successful completion of the course students should be able to: understand basic principles and results of the theory of secure communication; know principles and problems of basic cryptosystems for encryption (both secret and public key), digital signing and authentication; know methods to create core cryptographic protocols primitives; analyze and practically use simple cryptosystems; be experienced in methods of quantum cryptography and steganography

Text Book:
[T1] B.A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, 2nd Edition, 2011, Mcgraw Hill Education.

Reference Books:

[R1] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th Edition, 2014, Pearson.

[R2] Douglas R. Stinson, "Cryptography Theory and Practice", Chapman & Hall/CRC, Third Edition, 2006.

[R3] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. Available online at: **http://cacr.uwaterloo.ca/hac/**

[R4] S.Goldwasser, M. Bellare, Lecture Notes on Cryptography, 2008. Available online at: **https://cseweb.ucsd.edu/~mihir/papers/gb.pdf**

[R5] O. Goldreich, Foundations of Cryptography Volume 1: Basic Tools, Cambridge University Press, 2004. Available online at: **http://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html**

[R6] O. Goldreich, Foundations of Cryptography Volume 2: Basic Applications, Cambridge University Press, 2004. Available online at: **http://www.wisdom.weizmann.ac.il/~oded/ focdrafts.html**

[R7] Cryptography – 1, an online course on "Coursera", Taught By: Prof. Dan Boneh, Dept. of Computer Science and Electrical Engineering, Stanford University. URL: https://www.coursera.org/learn/crypto

[R8] https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability

[R9] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition 1995, John Wiley & Sons

COURSE PLAN

Module No.	Lecture Session	Reference	Learning outcomes
Module 1 Course Introduction, Background	L1-L5	T1-CH 1,2,3	Course Introduction, Security Overview (Goals, attacks and mechanisms). Classical Encryption Techniques, Mathematics of Cryptography: Integer Arithmetic, Modular Arithmetic, Extended Eulid Algorithm, Linear Congruence.
Module 2 Symmetric Encryption and Modern Symmetric Ciphers	L6-L12	T1-CH. 4,5,6,7,8	Mathematics of Symmetric Key Cryptography, Modern Block Ciphers and their components, Feistel Ciphers, Differential and Linear Cryptanalysis, Modern stream Ciphers, Data Encryption Standard (DES), Advanced Data Encryption Standard (AES), Modes of Operation of block and stream ciphers (ECB, CBC, OFB etc.)
Module 3 Asymmetric Encryption	L13-L20	T1-Ch. 9,10	Fermet's Little Theorem, Euler Theorem, Chinese Remainder Theorem, Exponentiation and Logarithms, RSA, Elgamal and Elliptic Curve Crypto Systems,
Module 4 Message Integrity, Message Authentication and Cryptographic Hash	L21-L26	T1-Ch.11,12	Hash Function, Cryptographic Hash Functions, Applications of Crypto Hash Functions, Birthday Problem, Block, Ciphers as Hash Functions, Secure Hash Algorithm (SHA), Message Security Requirements, MAC, HMAC, Using Symmetric Ciphers for MACs. Cipher-based Message Authentication

Function, Message Authentication Code			Code (CMAC), Authenticated Encryption.
Module 5 Digital Signatures, Entity Authentication and Key Management	L27-33	T1-Ch. 13, 14, 15	Digital Signature, Attacks on Digital Signature, Digital Signature Algorithm (DSA), Key Distribution Using KDC, Key Distribution Using Public Keys, Distribution of Public Keys, Entity Authentication and Message Authentication, Password-based Authentication, Challenge-Response based Authentication Protocols, , User Authentication Using Public Keys, Zero knowledge Proofs,
Module 6 Advanced Topics	L34-L37	-	Identity based encryption, homomorphic encryption, secret sharing, secure multi party computation
Module 6 Network Security	L38-40	T1-Ch. 16,17,18,19	Application Layer Security: PGP, Transport Layer Security: SSL and TLS, Security at network Layer: IPSec

EVALUATION SCHEME:

Component	Duration	Weightage (%)	Date & Time
Test-T1	30 mins	14%	Sep, 16 (During class hour)
Test-T2	30 mins	14%	Oct, 14 (During class hour)
Test-T3	30 min	14%	Nov, 18 (During class hour)
Seminar	30 min	5%	After MidSem
Programming Assignment	2 weeks	8%	Second Week of Sep.
Term Project	Complete Semester	20%	From the beginning only. Involves continuous evaluation
Comprehensive	2 hours	25%	TBA

7. **CHAMBER CONSULTATION HOUR:** TBD

8. **MAKE-UP Policy:** For all three tests (combined), only one makeup is permitted, which will be conducted after completing all tests. More specifically, if a student has missed one or more tests (because of any genuine reason for which makeup can be granted), he/she can take only one makeup for 14% weightage. No separate makeups will be given for tests under any circumstances. No makeup for any other component. The makeup for compre would be given as per institute rules.
Prior permission from I/C is a must for makeup of any evaluation component.

9. **NOTICES:** All announcement related to the course will be done by sending broadcast or personal mails.

Instructor–in-charge