Birla Institute of Technology & Science, Pilani
Hyderabad Campus

Academic – Undergraduate Studies Division
SECOND SEMESTER 2018-2019
Course Handout Part II

In addition to part-I (General Handout for all courses appended to the time table) this portion gives further specific details regarding the course.

Course No. : BITS F463
Course Title : Cryptography
Instructor-in-Charge : Prof. G Geethakumari

Scope and Objectives of the Course:
Cryptography is an indispensable tool for protecting information in computer systems. Learning to reason about the security of cryptographic constructions and to apply this knowledge to real-world applications forms the crux of this course.
The objectives of the course are:

- Insight into private key cryptographic schemes and their implementation as well as Public key cryptographic mechanisms and their applciations
- Hands-on exposure to cryptographic algorithms to various real-life security applications in the cyber space

Textbooks:
T1: Cryptography and Network Security: Principles and Practice, William Stallings, 6th Edition, Pearson Education, 2014.

Reference books:
R1: Cryptography and Network Security, Behrouz A. Forouzan, McGraw-Hill, 2007
R2: Applied Cryptography, Bruce Schneier, Wiley Student Edition, Second Edition, Singapore, 2010
R3: Handbook of Applied Cryptography: Alfred Menezes, Paul van Oorschot, and ScoF Vanstone, CRC Press, NY, 2001.
R4: Cryptography: Theory and Practice, Douglas Stinson, Chapman and Hall/CRC, 3rd Edition, 2005.

Online Study Material:
http://online.stanford.edu/course/cryptography
https://www.coursera.org/course/crypto

Course Plan:

Lecture No.	Learning objectives	Topics to be covered	Chapter in the Text Book
1	Overview of Computer Security Concepts and relevance of cryptography	OSI Security Architecture, Security attacks, Models and Mechanisms	T1 Chapter 1
2-3	Introduction to Cryptography	Understanding of classical cryptosystems	T1 Chapter 2
4-5	To learn about various symmetric ciphers and standards	Classical Encryption Techniques	T1 Chapter 2
6-8		Block Ciphers and the Data Encryption Standard	T1 Chapter 3
9-11		Basic Concepts in Number Theory and Finite Fields	T1 Chapter 4
12-14		Advanced Encryption Standard	T1 Chapter 5
15-17		Block Cipher Operation	T1 Chapter 6
18-19		Pseudorandom Number Generators	T1 Chapter 7.1 -7.3
20-21		Stream Ciphers	T1 Chapter 7.4 – 7.8
22-23	To learn about various asymmetric ciphers and standards	More on Number Theory	T1 Chapter 8
24-26		Public-Key Cryptography and RSA	T1 Chapter 9
27-29		Other Public-Key Cryptosystems	T1 Chapter 10
30-32	Learn about cryptographic data integrity algorithms	Cryptographic Hash functions	T1 Chapter 11
33-35		Message Authentication Codes	T1 Chapter 12
36-38		Digital Signatures	T1 Chapter 13
39-42	To learn about the role of mutual trust in key management schemes	Key Management and Distribution; User Authentication	T1 Chapter 14, Chapter 15

Evaluation Scheme:

Component	Duration	Weightage (%)	Date & Time	Nature of Component
Mid Sem Test	1 hr 30 min	30%	16/3 11.00 -12.30 PM	Closed Book
Quizes(Two)		10%		Closed Book
Assignments/Term Projects (Take Home)		20%		Open Book
Comprehensive Exam	3 hrs	40%	13/05 AN	Closed Book

Note: For the Assignments/Term Projects (Take Home) component of 20%, exposure to basic programming (let us say, in C) would be useful.

Chamber Consultation Hour: To be announced in the class

Notices: The notices for this course would be put up in the CSIS N/B as well as in CMS.

Make-up Policy: No makeup exam allowed without prior permission. For take home evaluation component, there is no makeup.

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