Birla Institute of Technology & Science, Pilani
Hyderabad Campus

SECOND SEMESTER 2021-2022

Course Handout Part II

Date: 15.01.2022

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**

1. 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

2. Textbooks:

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

3. 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.

4.Online Study Material:

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

5. Course Plan:

Lecture No.	Learning objectives	Topics to be covered	Chapter in the Text Book
1	To get an overview of Computer Security Concepts and relevance of cryptography	OSI Security Architecture, Security attacks, Models and Mechanisms	T1 Chapter 1
2-3	To get an insight into the 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 know 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	To understand various 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 study about the role of mutual trust in key management schemes	Key Management and Distribution; User Authentication	T1 Chapter 14, Chapter 15

6. Evaluation Scheme:

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

Sl No.	**Component**	**Duration**	**Weightage (%)**	**Date & Time**	**Nature of Component**
1	Mid Sem Test	90 min	35%	16/03 11.00am to12.30pm	Closed Book
2	Programming Assignments (online) (*evenly spaced*) **2Nos**		25%	TBA	Open Book
3	Comprehensive Exam	120 min	40%	19/05 AN	Closed Book

"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."

7.Consultation Hour: To be announced in the class.

8.Notices: The notices for this course would be put up in CMS.

9.Make-up Policy: No makeup exam allowed without prior permission.

10.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
BITS F463