Birla Institute of Technology & Science, Pilani
Hyderabad Campus

FIRST SEMESTER 2024-2025

Course Handout Part II

Date: 01.08.2024

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. S Dey**

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: Theory and Practice, Douglas R. Stinson, Maura B. Paterson. Chapman and Hall/CRC, 4rd Edition, 2014.

3. Reference books:

R1: Cryptography and Network Security, Behrouz A. Forouzan, D. Mukhop0adhyay McGraw-Hill, 2015
R2: Cryptography and Network Security: Principles and Practice, William Stallings, 7th Edition.

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 insight into the Introduction to Cryptography	Introduction to Cryptography, idea of key, public and symmetric key	T1 Chapter 1
2-6	Understanding of basic classical cryptosystems and related mathematics	Conguence, Shift cipher, affine cipher, substitution cipher, permutation cipher, cryptanalysis	T1 Chapter 2.1,2.2

6-8	Mathematical formulation of security	Shannon’s theory, one time pad	T1 Chapter 3
9-10	Introduction to stream and block ciphers	Block Ciphers and SPN	T1 Chapter 4.1, 4.2
11-13		Advanced Encryption Standard	T1 Chapter 4.6
14		Block Cipher Operation	T1 Chapter 4.7
15-17		Stream Ciphers, ChaCha	T1 Chapter 4.8
18		Pseudorandom Number Generators	R2 Chapter 8
20-21	To know about various asymmetric ciphers and standards	More on Number Theory	T1 Chapter 6.2
22-23		Public-Key Cryptography and RSA	T1 Chapter 6.3 6.4
24-37		Other Public-Key Cryptosystems, discrete log problem, el gamal, Elliptic Curve	T1 Chapter 7
27-29	To understand various cryptographic data integrity algorithms	Cryptographic Hash functions	T1 Chapter 5
30-32		Message Authentication Codes	T1 Chapter 5.5
33-36		Signature schemes	T1 Chapter 8.1, 8.2, 8.3
37-40	To study about the key management schemes	Key Management and Distribution;	T1 Chapter 11.1, 11.2 Chapter 12.1, 12.2
40-41	Post Quantum Cryptography	Lattice based cryptography	T1 Chapter 9.2

6. Evaluation Scheme:

Sl No.	Component	Duration	Weightage (%)	Date & Time	Nature of Component
1	Mid Sem Test	90 min	30%	07/10 - 11.30 - 1.00PM	Closed Book

innovate achieve lead

2	Assignments		20%	TBA	Open Book
3	Quiz		10%	TBA	closed book
4	Comprehensive Exam	120 min	40%	09/12 FN	Closed Book

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