Birla Institute of Technology & Science, Pilani
Hyderabad Campus

01-08-2019

**FIRST SEMESTER 2019-2020**

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* : Dr. Odelu Vanga

**Scope and Objectives of the Course:**

Cryptography is a field of computer science and mathematics that focusses on techniques for secure communication between two parties, while a third-party is present. Goal of this course is to learn the cryptographic constructions and analysis, and apply this knowledge to the real-world applications.

**The objectives of the course are:**

- To understand the fundamentals of cryptography and its applications.
- To acquire knowledge on symmetric-key ciphers used to achieve data confidentiality.
- To gain knowledge on asymmetric-key ciphers and applications to various key management techniques.
- To understand hash functions and digital signatures used to provide integrity, authentication, and non-repudiation.
- To understand how to design and implement security protocols in the real-world applications.

**Textbooks:**

- T1: Cryptography: Theory and Practice, Douglas Stinson, Chapman and Hall/CRC, 3rd Edition, 2006.

**Reference books:**

- R1: Cryptography and Network Security: Principles and Practice, William Stallings, 6th Edition, Pearson Education, 2014
- 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 and Network Security, Behrouz A. Forouzan, McGraw-Hill, 2007
- R5: Lecture Notes on Cryptography, Goldwasser Shafi and Mihir Bellare, 1996.

**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 |
|---|---|---|---|
| 1-2 | To get introduced to cryptography and its applications | • Introduction to Secure Communication<br>• Primary Goals of Cryptography<br>• Security Mechanisms | T1 Chapter 1<br>R1 Chapter 1 |
| 3-10 | To understand the basic cryptographic techniques and their analysis | • Classical encryption techniques<br>• Stream Ciphers | T1 Chapter 1<br>R1 Chapter 2 |
| 11-13 | To understand main elements of Shannon's approaches to cryptography and use of information theory in cryptography | • Short note on Probability Theory<br>• Perfect Secrecy<br>• Entropy | T1 Chapter 2 |
| 14-15 | To learn pseudorandom sequences & modern symmetric-key ciphers | • Pseudorandom Bit Generator<br>• Blum-Blum-Shub Generator | T1 Chapter 8 |
| 16-18 | | • Feistel Cipher<br>• Data Encryption Standard (DES) | T1 Chapter 3<br>R1 Chapter 3 |
| 19-22 | | • Finite Fields<br>• Advanced Encryption Standard (AES) | T1 Chapter 5<br>R1 Chapter 4 & 5 |
| 23-27 | To learn number theory concepts and applications to asymmetric-key ciphers | • Prime Numbers, Fermat and Euler's Theorems<br>• Euclidean Algorithm<br>• Chinese Remainder Theorem<br>• Primality Testing: Miller-Rabin & AKS-Algorithm | T1 Chapter 5<br>R1 Chapter 8 |
| 28-31 | | • RSA Cryptosystem<br>• Integer Factorization | T1 Chapter 5<br>R1 Chapter 9 |
| 32-33 | | • ElGamal Cryptosystem<br>• Discrete Logarithm Problem | T1 Chapter 6 |
| 34-38 | | • Elliptic Curves Over Finite Fields<br>• Elliptic Curve Cryptography (ECC)<br>• Diffie-Hellman Problems | T1 Chapter 6<br>R1 Chapter 10 |
| 39-42 | To learn digital signatures, hash functions, and their applications to information security | • Hash Functions<br>• Digital Signature Algorithm<br>• ElGamal Digital Signature<br>• ECC-based Digital Signature | T1 Chapter 7<br>R1 Chapter 12 & 13 |

**Evaluation Scheme:**

| Component | Duration | Weightage (%) | Date & Time | Nature of Component |
|---|---|---|---|---|
| Mid-Sem Exam | 90 min | 35% | 4/10, 9.00 -- 10.30 AM | Closed Book |
| Term Project (Implementation of one research paper from IEEE/ACM) | -- | 20% | | Open Book |
| Comprehensive Exam | 3 hrs | 45% | 11/12 FN | Closed Book |

***Note: Class Test schedule will be announced at most four days before the test.***

**Chamber Consultation Hour:** To be announced in the class.

**Notices:** The notices for this course would be put up in the CSIS N/B and/or CMS.

**Make-up Policy:** No makeup exam allowed without prior permission. For the *Term Project* 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 any type of academic dishonesty is not acceptable.

**INSTRUCTOR-IN-CHARGE**