



---

**SECOND SEMESTER 2020-2021**

Course Handout Part II

**Date: 16.01.2021**

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 applications
- 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, 6<sup>th</sup> 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, 3<sup>rd</sup> Edition, 2005.

**Online Study Material:**

<http://online.stanford.edu/course/cryptography>

<https://www.coursera.org/course/crypto>

**4. 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		More on Number Theory	T1 Chapter 8
24-26	To learn about various asymmetric ciphers and standards	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

## 5. Evaluation Scheme:



Sl No.	Component	Duration	Weightage (%)	Date & Time	Nature of Component
1	Mid Sem Test	90 min	35%	02/03 3.30 - 5.00PM	Open Book
2	Programming Assignments(online): <b>2Nos</b>	TBA	35% (17.5% pre -mid)		Open Book
3	Comprehensive Exam	120 min	30%	05/05 AN	Open Book

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

**7. Notices:** The notices for this course would be posted in CMS.

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

**9. 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**

