Second semester 2015-16

CourseHandoutPartII

InadditiontoPart-I(GeneralHandoutforallcoursesappendedtothetimetable)thisportiongivesfurtherspecificdetailsregardingthecourse.

CourseNo.:BITS F463

CourseTitle: **Cryptography**

Instructor: **Abhishek Mishra**

Email:abhishek.mishra@pilani.bits-pilani.ac.in

Course Objectives: To learn about complexity theoretic and number theoretic background required for modern cryptography. To learn about basic tools and applications used in modern cryptography.

Text Book:

[T1] B.A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, 2nd Edition, 2011, Mcgraw Hill Education.

Reference Books:

[R1] S.Goldwasser, M. Bellare, Lecture Notes on Cryptography, 2008. Available online at: **https://cseweb.ucsd.edu/~mihir/papers/gb.pdf**

[R2] O. Goldreich, Foundations of Cryptography Volume 1: Basic Tools, Cambridge University Press, 2004. Available online at: **http://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html**

[R3] O. Goldreich, Foundations of Cryptography Volume 2: Basic Applications, Cambridge University Press, 2004. Available online at: **http://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html**

[R4] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. Available online at: **http://cacr.uwaterloo.ca/hac/**

[R5] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th Edition, 2014, Pearson.

[R6] W. Trappe, L.C. Washington, Introductionto Cryptography with Coding Theory, 2nd Edition, 2007, Pearson.

[R7] D.R. Stinson, Cryptography: Theory and Practice, 3rd Edition, 2005, CRC.

[R8] H. Delfs, H. Knebel, Introduction to Cryptography: Principles and Applications, 2nd Edition, 2007, Springer.

Lecture Plan:

Lecture	Topics
1	Impagliazzo's Five Worlds
2 - 6	Number Theoretic Background
7 - 8	Classical Cryptography
9 - 12	One-Way Functions
13	Pseudorandom Generators
14 - 17	Block Ciphers
18 - 19	Pseudorandom Functions
20 - 23	Private-Key Encryption
24 - 27	Public-Key Encryption
28 - 30	Hash Functions
31 - 33	Message Authentication
34 - 37	Digital Signatures
38 - 39	Key Distribution
40	Protocols

Evaluation:

Component	Mode	Weightage	Duration	Remarks
Quiz 1	Open Book	10%	40 minutes	In February
Mid Semester Exam	Open Book	30%	90 minutes	16/3 2:00 -3:30 PM
Quiz 2	Open Book	10%	40 minutes	In April
Comprehensive Exam	Open Book	50%	180 minutes	9/5 FN

Open Book Policy: Only hard copies are allowed (lecture notes, text book, or reference books).

Make-up Policy: Make-up exam may be arranged only in genuine cases with prior permission.

Malpractise Regulation: A student will get 0 if found cheating.

Chamber Consultation Hour: 11:00 to 12:00 on Saturdays (6121S).

Notices: All notices will be posted on Nalanda.