BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, Pilani
Pilani Campus
AUGS/ AGSR Division

SECOND SEMESTER 2019-20
COURSE HANDOUT

Date: 06.01.2020

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 : **Abhishek Mishra**
Instructor(s) :
Tutorial/Practical Instructors:

1. Course Description: The course presents an introduction to Cryptography.

2. Scope and Objective of the Course: To learn about complexity theoretic and number theoretic background required for modern cryptography. To learn about basic tools and applications used in modern cryptography. To learn about some cryptographic protocols.

3. Text Books:
[T1] B.A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, 3rd Edition, 2015, McGraw-Hill Education.

4. 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, 7th Edition, 2017, Pearson.

[R6] W. Trappe, L.C. Washington, Introduction to 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.

[R9] S. Arora, B. Barak, Computational Complexity: A Modern Approach, 2009, Cambridge University Press. Available online at: **http://theory.cs.princeton.edu/complexity/book.pdf**

5. Course Plan:

Lecture	Topics
1	Impagliazzo's Five Worlds.
2	Divisibility.
3	Euclid's Extended GCD Algorithm.
4	Congruences, Fermat's Theorem, Euler's Theorem.
5	Modular Exponentiation Algorithm.
6	Groups, Subgroups, Primitive Roots.
7	Shift Cipher, Substitution Cipher, Affine Cipher.
8	Vigenere Cipher, Permutation Cipher, Cryptanalysis of Classical Ciphers.
9	Strong One-Way Functions, Weak One-Way Functions, Non-Uniformly Strong One-Way Function.
10	One-Way Functions as Collections. Examples of One-Way Functions. Examples of One-Way Collections.
11	RSA Collection. Polynomial-Time Reductions. Chinese Remainder Theorem. Quadratic Residues.
12	Rabin Function. Discrete Logarithm Problem. Trapdoor One-Way Permutations. RSA Trapdoor.

13	One-Time Pad. Pseudo-Random Bit Generators. Polynomial-Time Indistinguishability. Pseudo-Random Distribution, Pseudo-Random Generator, Blum-Blum-Shub Pseudo-Random Generator.
14	Data Encryption Standard.
15	Properties of DES. Key Recovery Attacks on Block Ciphers, Double-DES. Triple-DES, DESX.
16	Rings and Fields. Examples of Rings and Fields. Polynomial Rings over Fields. Galois Fields.
17	Advanced Encryption Standard.
18	Function Family, Random Functions and Permutations.
19	Pseudo-Random Functions and Permutations. Pseudo-Random Permutations under Chosen Plaintext Attack (CPA). Pseudo-Random Permutations under Chosen Ciphertext Attack (CCA). Security Against Key Recovery. The Birthday Attack.
20	Symmetric Encryption Schemes. Modes of Operations: Electronic Code Book (ECB) Mode, Cipher Block Chaining with Random Initial Vector (CBC$) Mode, Cipher Block Chaining with Counter Mode (CBCC), Counter Mode with a Random Starting Point (CTR$), Counter Mode with a Counter Starting Point (CTRC).
21	Indistinguishability under CPA. Attack on ECB. Attack on any Deterministic, Stateless Scheme. Attack on CBCC.
22	Indistinguishability under CCA. CCA on CTR$ Scheme. CCA on CBC$ Scheme.
23	Public Key Encryption Schemes. Polynomial-Time Indistinguishability. Semantic Security. Legendre and Jacobi Symbols.
24	RSA Public Key Cryptosystem, Mental Poker, Extracting Partial Information from the RSA Function, Low Exponent Attack on RSA. Rabin's Public Key Cryptosystem.
25	Hard-Core Predicates, Goldreich-Levin Construction of a Hard-Core Predicate. Bit Security of RSA. One-Way

	Predicates, Collection of One-Way Predicates.
26	A Set of Trapdoor Predicates based on the RSA Assumption. Encrypting Single Bits using Trapdoor Predicates. Encrypting Single Bits using Hard-Core Predicates. Efficient Probabilistic Encryption.
27	Secure Hash Algorithm (SHA).
28	Collision Resistant Hash Functions. Collision Finding Attacks: Exhaustive Search Collision Finding Attack, Random-Input Collision Finding Attack, Birthday Attack. Collision-Resistance under Hidden-Key Attack
29	Message Authentication Scheme. Message Authentication Code (MAC). Forgery. MAC Security.
30	Examples of Forgeable MACs.
31	PRF MACs, CBC MACs.
32	Diffe-Hellman (DH) Secret Key Exchange Protocol, DH Problem, DH Assumption. Digital Signatures, Digital Signatures using the Trapdoor Function Model, DH Digital Signature Scheme. Attacks against Digital Signatures. Types of Forgery. Security Definition of Digital Signatures.
33	RSA Digital Signature Scheme. El Gamal's Digital Signature Scheme. Rabin's Digital Signature Scheme.
34	Interactive Proofs. Interactive Proof for Graph Non-Isomorphism. Interactive Proof for Quadratic Non-Residuosity.
35	Zero Knowledge Proofs. Zero Knowledge Proof for Graph Isomorphism.
36	Quantum Computation.
37	EPR Paradox, Quantum Protocol for the Parity Game.
38	Secret Sharing.
39	Elliptic Curves.
40	Elliptic Curve Cryptography.

6. Evaluation Scheme:

Component	Duration	Weightage (%)	Date & Time	Nature of component (Close Book/ Open Book)
Mid-Semester Test	90 Min.	35	3rd March, 14:00 – 15:30	Open Book
Comprehensive Examination	3 h	45	5th May, 8:00 – 11:00	Open Book
Quiz 1	40 Min.	10	In February	Open Book
Quiz 2	40 Min.	10	In April	Open Book

7. Chamber Consultation Hour: 15:00 – 16:00, Friday (6121S).

8. Notices: All notices will be posted on Nalanda.

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

10. Note (if any):

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

Abhishek Mishra
Instructor-in-charge
Course No. BITS F463