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

SECOND SEMESTER 2020-21
COURSE HANDOUT

Date: 18.01.2021

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 : **Abhishek Mishra**
Instructor(s) : **Shashank Gupta**
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	Background, Motivation and Introduction to Number Theory and Cryptography
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.
10	One-Way Functions as Collections. Examples of One-Way Functions. Examples of One-Way Collections.
11	RSA Algorithm, Chinese Remainder Theorem,
12	RSA Digital Signature Scheme. El Gamal's Digital Signature Scheme. Rabin's Digital Signature Scheme.
13	Rabin Function. Discrete Logarithm Problem. Trapdoor One-Way Permutations. RSA Trapdoor.
14	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.
15	One-Time Pad. Pseudo-Random Bit Generators. Pseudo-Random Distribution, Pseudo-Random Generator, Blum-Blum-Shub Pseudo-Random Generator.
16	Data Encryption Standard.
17	Properties of DES. Key Recovery Attacks on Block Ciphers, Double-DES. Triple-DES

18	Advanced Encryption Standard.
19	Rings and Fields. Examples of Rings and Fields. Polynomial Rings over Fields. Galois Fields.
20	Secret Sharing.
21	Function Family, Random Functions and Permutations.
22	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.
23	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).
24	Indistinguishability under CPA. Attack on ECB. Attack on any Deterministic, Stateless Scheme. Attack on CBCC.
25	Indistinguishability under CCA. CCA on CTR$ Scheme. CCA on CBC$ Scheme.
26	Public Key Encryption Schemes. Polynomial-Time Indistinguishability. Semantic Security. Legendre and Jacobi Symbols.
27	RSA Public Key Cryptosystem, Mental Poker, Extracting Partial Information from the RSA Function, Low Exponent Attack on RSA. Rabin's Public Key Cryptosystem.
28	Hard-Core Predicates, Goldreich-Levin Construction of a Hard-Core Predicate. Bit Security of RSA. One-Way Predicates, Collection of One-Way Predicates.
29	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.
30	Secure Hash Algorithm (SHA).
31	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
32	Message Authentication Scheme. Message Authentication Code (MAC). Forgery. MAC Security.
33	Examples of Forgeable MACs.
34	PRF MACs, CBC MACs.
35	Interactive Proofs. Interactive Proof for Graph Non-Isomorphism. Interactive Proof for Quadratic Non-Residuosity.
36	Zero Knowledge Proofs. Zero Knowledge Proof for Graph Isomorphism.

37	Quantum Computation.
38	EPR Paradox, Quantum Protocol for the Parity Game.
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.	30	To Be Announced	Open Book
Comprehensive Examination	2 h	40	7th May, FN	Open Book
Quiz 1	50 Min.	15	In February	Open Book
Quiz 2	50 Min.	15	In April	Open Book

7. Chamber Consultation Hour:

Abhishek Mishra: 13:00 – 14:00, Friday (with prior appointment on email).

Shashank Gupta: 13:00 -14:00 Monday (with prior appointment on email).

8. Notices: All notices will be posted on https://nalanda-aws.bits-pilani.ac.in.

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

10. Google Meet ID for Lecture: https://meet.google.com/hbd-jjys-ggz (for Tuesday and Thursday at 4th hour), https://meet.google.com/tow-iafn-veq (for Wednesday at 10th hour)

11. Open Book Policy: Everything is allowed except for cheating.

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