Course work for PhD students aspiring to work in "Cryptology"

The following courses will be offered to the first semester Ph.D. students aspiring to work in the area of Cryptology and Security:

- DM: Discrete Mathematics
- PDS: Introduction to computer Programming and Data Structure
- Cr: Cryptology
- CyS: Introduction to Selected Topics in Cyber Security
- RM: Research Methodology

The time table and details of each courses is given below.

Routine

	11:45 – 13:15	14:15 – 15:45	16:00 – 17:30
Monday	DM	-	PDS
Tuesday	RM	CyS	-
Wednesday	Cr	RM	-
Thursday	DM	CyS	PDS
Friday	Cr	-	-

1. Discrete Mathematics

A. **Description:** This course will discuss basic Combinatorial and Algebraic ideas of Mathematics.

B. **Pre-requisites:** High School level Mathematics.

C. **Outline of the syllabus**

1. The Foundations - Logic and Proofs: Propositional logic, Predicates and Quantifiers, Rules of Inference, Proof methods and strategies.
2. Combinatorics: Sets, Functions, Relations, Equivalence relation, Partitions, PO Set, Lattice; Basics of counting, Pigeonhole principle, Permutation, Combination, Binomial and Multinomial Theorem, Generating permutation and combination, Inclusion-Exclusion and its application; Recurrence relation, Solving linear recurrence relation, Generating functions; Basic Number theory, Divisibility, Congruence, GCD, Euclidean Algorithm, Extended Euclidean Algorithm, Chinese Remainder theorem, RSA.
3. Graph Theory: Graphs and di-graphs, Basic terminologies (clique, independent set, vertex cover, degree, regular, complement), Graph models, Isomorphism, Representation of graphs, Connectivity, Eulerian paths and circuits, Hamiltonian paths and circuits, Knight's Tour; Graph traversal, Topological Sorting, Shortest path algorithms, Tree, Counting trees (Prufer Code), Minimal Spanning Trees, Planar graphs, Euler's Formula, Kuratowski's Theorem, Five-color Theorem, Bi-partite Matching, Halls Theorem, Stable Matching, Matching in any graph, Tutte's Theorem, Coloring of graphs, Chromatic Number, Brooks Theorem, Vizing's Theorem, Art Gallery Problem.

D. **Duration:** 45 hours (15 weeks, 3 hours per week).

E. **Learning outcome and the objective of the course**
This is one of the foundational classes in the CS curriculum. It is a direct or indirect prerequisite to courses in Algorithms, Theory of Computation, Compilers, Artificial Intelligence, Data Security, Computer Graphics, Operating Systems, Cryptology, etc. The class has two major themes.

(a) Mathematical Reasoning: You will learn logic and proof techniques so you can show that a mathematical statement is true.

(b) Discrete Structures: You will learn important mathematical structures – used to represent objects and their relationships – in Computer Science. These discrete structures include sets, functions and relations, graphs, etc.

Both skills are important for designing algorithms, researching in Cryptology.

F. **References**

(a) K. H. Rosen: Discrete Mathematics and Its Applications (8th Edition), McGraw Hill, 2019.

(b) N. L. Biggs: Discrete Mathematics, Clarendon Press, 1985.

(c) C. L. Liu: Elements of Discrete Mathematics, McGraw Hills, 1985.

(d) J. A. Bondy, U. S. R. Murty: Graph Theory, Graduate texts in mathematics 244, Springer, 2008.

(e) D. West: Introduction to Graph Theory, Prentice Hall, 2000.

(f) R. Diestel: Graph Theory, Graduate texts in mathematics 173, Springer-Verlag Berlin Heidelberg, 2017.

(g) B. Bollobas: Modern Graph Theory, Graduate texts in mathematics, Springer, 2002.

G. **Assessment methodology:** Mid-Semestral and End-Semestral Examination.

H. **Pedagogic methodology:** Lectures, presentations.

This course is proposed by Rana Barua and Nilanjan Datta.

2. Introduction to Computer Programming and Data Structure

A. **Description:** This course is aimed at introducing students a thorough and practical introduction to data structures and enabling them to develop computer programs for problem solving at a basic level.

B. **Pre-requisites:** None.

C. **Outline of the syllabus:**

- The Evolution of Programming Languages
- Compiler, Interpreter, Assembler
- Imperative languages: Introduction to imperative language; syntax and constructs of a specific language (preferably C);
  (a) Variables, assignments
  (b) Basic input/output, Main program, If-statement, Logical operators, Loops, Output formatting, Parameters, return values, Debugger
  (c) Arrays, Pointers, Dynamic Memory Allocation, Structures
  (d) Basic structures: Lists, Strings, Dictionary, Values and references
  (e) Basics of program design, Programming style, Exceptions
  (f) Functions and Recursion: Parameter passing, procedure call, call by value, call by reference, recursion, scope of variables.
  (g) Linked lists: Implementation of linked lists, inserting, deleting, and inverting a linked list, Stacks and Queues.
  (h) Matrix Algorithms: Matrix addition, multiplication, and inverse calculation. Finding Eigen values and Eigen vectors. Efficient Algorithms for large/sparse matrices.
  (i) Algorithm for Polynomials: Polynomial addition and multiplication, division.
  (j) File handling: principles of data storage and manipulation
  (k) Matrix Algorithms: Finding Eigen values and Eigen vectors of a large Matrix. Polynomial addition and multiplication.
  (l) Object-oriented programming: Classes and objects (Python)
  (m) Trees: Recursive and non-recursive traversal of trees; Balanced binary search trees (AVL tree implementation); Hashing.
- In addition, the following concepts need to be covered during the course of the lab session:
  (a) testing the program, developing test-plan, developing tests.
  (b) version management.
  (c) concept of debugging using gdb.
  (d) concept of writing shell scripts, using bash/tcsh.
  (e) concept of makefiles.

D. **Duration:** 45 hours (15 weeks, 3 hours per week).

E. **Learning outcome and the objective of the course**
On completion of the course the student should have the following learning outcomes defined in terms of knowledge and skills:

(a) Knowledge: The student
  i. can explain the basic concepts of structured and object-oriented programming.
  ii. knows the principles of algorithmic thinking and programming

iii. understands how programming is used to solve problems, motivated by the student's own subject specialization.

(b) Skills: The student is able to

i. implement simple programs
ii. use stepwise refinement to solve problems.
iii. make use of available programming language libraries
iv. extend and adapt code written by other programmers
v. process structured data sets
vi. develop, debug and test application programs.

F. **References**

(a) B. W. Kernighan and D. M. Ritchi: The 'C' Programming Language, Prentice Hall, Englewood Cliffs, NJ, 1980.

(b) B. Gottfried: Programming in C, Schaum Outline Series, New Delhi, 1996.

(c) B. Stroustrup: The C++ Programming Language, 2nd ed., Addison-Wesley, California, 1995.

(d) D. M. Arnow and G. Weiss: Introduction to Programming using Java, Addison-Wesley, London, 1999.

(e) T. W. Pratt and M. V. Zelkowitz: Programming Languages: Design and Implementation, 4th ed., Prentice Hall, Englewood Cliffs, 2001.

(f) T. A. Standish: Data Structures, Algorithms and Software Principles, Addison-Wesley, Reading, Mass., 1995.

(g) A. M. Tannenbaum and M. J. Augesestein: Data Structures Using PASCAL, Prentice Hall, New Jersey, 1981.

(h) D. E. Knuth: The Art of Computer Programming. Vol. 1, 2nd ed. Narosa/Addison-Wesley, New Delhi/London, 1973.

(i) E. Horowitz and S. Sahni: Fundamentals of Data Structures, CBS, New Delhi, 1977.

(j) A. Aho, J. Hopcroft, and J. Ullman: Data Structures and Algorithms, Addison-Wesley, Reading, Mass., 1983.

(k) T. Coreman, C. Leiserson and R. Rivest: Introduction to Algorithms, McGraw Hill, New York, 1994.

(l) S. Sahani: Data Structure, Algorithms and Applications in JAVA, McGraw Hill, New York, 2000.

G. **Assessment methodology:** Written and Programming assignments, Examinations.

H. **Pedagogic methodology:** Lectures, presentations, and Programming session.

This course is proposed by Subhamay Maitra, Laltu Sardar and Ritankar Mandal.

3. Cryptology

A. **Description:** Cryptology is concerned with the conceptualization, definition, and construction of computing systems that address security concerns. This course is aimed at providing a basic understanding of cryptographic concepts, tools and how to apply them in defining cryptographic tasks and solving new cryptographic problems using existing and new tools.

B. **Pre-requisites:** Basic Knowledge of Probability, Combinatorics, Number Theory.

C. **Outline of the syllabus:**

1. Introduction: Classical Ciphers, Shannon Cipher, Perfect Security, Computational Ciphers and Semantic Security.
2. Encryption: Stream Ciphers, Pseudo random generators, LFSR based stream ciphers, RC4 and its Cryptanalysis; Block ciphers: Design principle, AES and its design rationale, light-weight block cipher design; Security Notions, Modes of operation: ECB, CBC, OCB, Counter mode.
3. Cryptanalysis: Goal and power of an adversary; Differential and Linear Cryptanalysis; Some advanced cryptanalysis (integral, impossible differential) and its applications.
4. Hash Function: Collision resistant (CR) hash functions, birthday attacks CR hash, The Merkle-Damgard paradigm, Joux's multi-collsion attacks; Universal hash functions (UHF), constructing UHFs.
5. Message Integrity: Message authentication codes (MACs); Designing MACs from CR hash, Case Study: HMAC, Sponge based MACs; Designing MACs from UHF, The Carter-Wegman MACs, Nonce based MACs.
6. Authenticated Encryption (AE): Motivation, Security, Designing AE: Generic Paradigm, Integrated AE; Features of AE, Light-weight AE design.
7. Public Key Cryptosystems: Basics of Number theory, Number theoretic Algorithm, Primality testing algorithm, Integer Factorization Problem, Discrete Logarithm Problem, Diffie Hellman Key Exchange Protocol, RSA Encryption and Its variants, Elgamal Encryption Scheme, Digital Signatures, Commitment Scheme, Secret Sharing, Fiat-Shamir Identification Scheme.

D. **Duration:** 45 hours (15 weeks, 3 hours per week).

E. **Learning outcome and the objective of the course:**

The objective of this course is to provide a basic understanding of cryptographic concepts, mathematical tools used for cryptography and how to use these tools in solving cryptographic problems, building new cryptographic primitives, analyzing the security of cryptographic protocols, and understanding key management and key exchange issues at a basic level. The focus is given on the basic mathematical tools as well as some new advanced cryptographic tools and the advances of research using those tools.

After successfully completing the course, students are expected to (i) understand the basic cryptographic tools and popular cryptographic algorithms, (ii) develop ideas for defining new cryptographic problems and provide solutions for them, (iii) design and implement new cryptographic algorithms using existing and new tools, (iv) analyze the security of various cryptographic protocols.

F. **References:**

(a) D. Boneh, V. Shoup: A Graduate Course in Applied Cryptography, online draft: `https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf`.

(b) J. Katz and Y. Lindell: Introduction to Modern Cryptography, Chapman & Hall/CRC, 2007.

(c) D. R. Stinson: Cryptography Theory and Practice, 3rd ed., Chapman & Hall/CRC, 2006.

(d) K. Sakiyama, Y. Li and Y. Sasaki: Security of Block Ciphers: From Algorithm Design to Hardware Implementation, Published by Wiley & Sons, Incorporated, John, 2016. ISBN 10: 1118660013.

(e) B. S. Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley and Sons, New York, 1995.

(f) A. Menezes, P. C. Van Oorschot and S. A. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.

(g) N. Koblitz: A course in number theory and cryptography, GTM, Springer.

(h) W. Stallings: Cryptography and Network Security.

(i) V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press

(j) Steven D. Galbraith: Mathematics of Public Key Cryptography, Cambridge University Press

G. **Assessment methodology:** Assignments, Examinations.

H. **Pedagogic methodology:** Lectures, presentations, and Tutorial sessions.

This course is proposed by Nilanjan Datta and Avijit Dutta.

4. Introduction to Selected Topics in Cybersecurity

A. **Description:** With the widespread use of the Internet and other information networks, and the concurrent prevalence of cyber attacks, cybersecurity has become an important issue for network users. Individuals and organizations are devoting substantial resources to defend themselves against cyber attacks. However, despite these efforts and expenditures, cyber attacks are continuing. Thus, it is necessary to study the issues and develop better defenses against cyber attacks.

This course will cover several important topics in cybersecurity in order to provide a basis for understanding the issues, review what defenses are currently implemented and identify methods that might help in improving cyber security. Since cyber security attacks are primarily launched over computer networks, the course will focus on the analysis of network traffic. Methods to detect, prevent and mitigate cyber attacks will be discussed in detail.

The course will provide a number of tools and techniques in cyber traffic analytics to enable security managers to better develop cyber defense. Methods to evaluate the cost-effectiveness of alternate strategies will be considered. The course will also provide the background needed to further investigate cyber attacks and to conduct future research in this area.

B. **Pre-requisites:** None

C. **Outline of the syllabus:**

1. Overview of cybersecurity; The major problem areas.
2. Selected topics to be covered; Their significance; Motivation to study cybersecurity.
3. Situational Awareness for Cybersecurity.
4. Attack models; Types; Characteristics; Detection.
5. Network Characteristics.
6. Vulnerability assessment.
7. Impacts of attacks on enterprise networks; Damages; Costs.
8. Security and Defense Models.
9. Cyber traffic analytics; Parameters; Monitoring; Profiling; Anomaly detection.
10. Metrics for Cybersecurity.
11. Mitigation and mitigation effectiveness.
12. Cost-effectiveness of strategies.

D. **Duration:** 45 hours (15 weeks, 3 hours per week).

E. **Learning outcome and the objective of the course:** Students should have developed an awareness of the key issues in cybersecurity. They should have acquired a knowledge of different types of cyberattacks, how vulnerabilities are assessed, and the impacts of cyber attacks. They will be introduced to cyber-traffic analytic methods and should have an overview of different mitigation strategies, as well as methods to evaluate the strategies.

F. **References**

(a) Network Defense and Countermeasures: Principles and Practices William Chuck Easttom II.

(b) Network Security Through Data Analysis: From Data to Action Michael Collins.

(c) Network Security A Beginner's Guide: Eric Maiwald.

Plus Assigned Readings

G. **Assessment methodology:** There will be a Midterm (40%) and a Final (60%). Tests will have True/False, Multiple Choice and Short-Answer questions.

H. **Pedagogic methodology:** The course will be taught through lectures, assigned readings and class discussion.

The syllabus for this course is proposed by Soumyo D. Moitra.

5. Research Methodology

A. **Description:** The primary objective of this course is to enable the students, irrespective of their disciplines, in developing the most appropriate methodology for their research studies; and to make them familiar with the art of exploiting different research methods and techniques. The participants of the course should obtain a guideline on how to write, publish, present, and review scientific papers. The course aims to guide the students regarding the publication ethics and misconducts. It is expected that the course will assist in the accomplishment of exploratory as well as result-oriented research studies.

B. **Pre-requisites:** Knowledge of Mathematics at high school level.

C. **Outline of the syllabus:**

(a) **Fundamentals of Research**:

Basics: Definition, Purpose and Classification of research, Fundamentals of research methods, Writing a research proposal;

Problem Identification: Review of literature, Broadening knowledge base in the specific research area, Bringing clarity and focus to the research problem, Writing a research proposal, Writing research reports/papers;

Identifying variables: The difference between a concept and a variable, Converting concepts into variables, Types of variable, Types of measurement scale. (6× 1.5 hr=9 hr)

(b) **Research Design**:

Selecting a study design: Differences between quantitative and qualitative study designs, Study designs in quantitative research,

Data collection: Selecting a method of data collection, Differences in the methods of data collection in quantitative and qualitative research, Major approaches to information gathering, Methods of data collection in qualitative research. (4× 1.5 hr=6 hr)

(c) **Fundamentals of Statistics**: Frequency, Measure of Central Tendency, Dispersion, Regression and Interpretation of Results.

(10×1.5 hr=15 hr)

(d) **Basics of Probability**: Definition of Probability, Conditional Probability, Bayes' Random Variable, Probability Distribution. (6× 1.5 hr=9 hr)

(e) **Optimization Techniques**: Maxima & Minima, Condition of Optimality, Linear Programming Problem (Introduction, Formation of LPP, Graphical method of solution). (4×1.5 hr= 6 hr)

(f) **Research Ethics**:

Philosophy & Ethics: Introduction to Philosophy, definition, nature and scope, concepts, branches, nature of moral philosophy, nature of moral judgements and reactions, Ethics with respect to science and research, Intellectual honesty and research integrity;

Scientific misconducts: Falsification, Fabrication, and Plagiarism, Redundant publications; duplicate and overlapping publications, Selective reporting and misrepresentation of data, Conflict of interest;

Publication misconduct: parallel submission, authorship and contributorship, Ethical issues regarding the sponsoring organisation, Restrictions imposed by the sponsoring organisation, The misuse of information. (6× 1.5 hr= 9 hr)

(g) **Practical Session**: Application of software; Latex, Beamer, Presentation towards communication skill for professional development, Audience analysis and persuasion techniques, Use of plagiarism detection soft ware like Turnitin, Urkund and other open source soft ware tools.
(4× 1.5 hr= 6 hr)

D. **Duration:** 60 hours (15 weeks, 4 hours per week).

E. **Learning outcome and the objective of the course:** Attending the course will reduce the probability for a student to be derailed from the research track. After completion of the course, a student should learn how to complete a project within a time bound in a scientific way. It is expected that the course can generate the awareness amongst the students about the publication ethics and publication misconducts. It is also expected that a student can write, present and communicate his/her research problem(s) professionally.

F. **References:**

(a) Research Methodology Methods & Techniques, C. R. Kothari, New Age International (P) Limited, Publisher, 2004.

(b) Research Methodology: A Step-by-Step Guide for Beginners (Fourth Edition), Ranjit Kumar, SAGE publishing, 2015.

(c) Fundamental of Research Methodology and Statistics, Y.K. Singh, New Age International (P) Limited, 2006.

(d) Research Methods and Statistics: A Critical Thinking Approach, Sherri L Jackson, American Psychological Association, 5th edition, Cengage Learning, 2014

(e) Research Ethics for Scientists: A Companion for Students, C. Neal Stewart Jr., Wiley Publishing, 2011.

(f) The student's guide to research ethics, Paul Oliver, Open University Press, McGraw-Hill Education, McGraw-Hill House, second edition, 2010.

G. **Assessment methodology:** Continuous assessment will be done through tutorials, assignments, quizzes, and group discussions. Weightage will be given for active participation. Written examination may also be conducted.

H. **Pedagogic methodology:** Class room teaching, guest lectures, group discussions, and practical sessions.

The syllabus for this course is prepared by Arpita Maitra.