M-Tech in Cryptology and Security:
Tentative Course Structure and Syllabus

M.Tech in Cryptology and Security is a two year program offered in the Kolkata center of the Indian Statistical Institute. The course is designed to impart in-depth theoretical and practical knowledge in the area of cryptology and information security. It is designed to provide the basic background in mathematics, statistics and computer science followed by specialized instructions on various theoretical and practical aspects of the field.

The students on successful completion of the course, may take up

- a professional career in a industry/government organization which specializes in information security.
- an academic career to further study and research in theoretical and practical aspects of cryptology, information security and related disciplines.

The Course Structure

Semester 1

In semester 1 there would be two pools of courses. A student have to take all two courses in Pool A and three courses from Pool B. The Pool B courses which a student is required to take would be decided by a faculty advisor based on the background of the student.

Pool A

A.1 Discrete Mathematics

A.2 Computing Systems I (OS & Architecture)

Pool B

B.1 Algebra and Number Theory

B.2 Probability and Statistics

B.3 Automata Theory, Languages and Computation

B.4 Computing Lab (Programming and Data Structures)

Semester 2

1. Design and Analysis of Algorithms
2. Cryptology
3. Information and Coding Theory
4. Computing Systems II (Computer Networks and Data Bases)
5. Computing Systems Security I

Semester 3

1. Advanced Cryptology
2. Computing Systems Security II
3. Cryptographic and Security Implementations
4. Elective 1
5. Elective 2

Semester 4

Dissertation and/or industry internship.

Tentative list of electives

1. Quantum Cryptology and Security
2. Topics in Privacy
3. Topics in Security
4. Topics in Cryptology
5. Computational Number Theory
6. Machine Learning for Security
7. Blockchains and Cryptocurrencies
8. Social and Legal Aspects of Security

Detailed Syllabus

Discrete Mathematics

1. Combinatorics: Sets, Diagonalization and the Pigeonhole Principle, Multinomial theorem, principle of inclusion exclusion; Recurrence relations - classification, summation method, extension to asymptotic solutions from solutions for subsequences; Linear homogeneous relations, characteristic root method, general solution for distinct and repeated roots, non-homogeneous relations and examples, generating functions and their application to linear homogeneous recurrence relations, non-linear recurrence relations, exponential generating functions, brief introduction to Polya theory of counting.

2. Graph Theory: Graphs and digraphs, complement, isomorphism, connectedness and reachability, adjacency matrix, Eulerian paths and circuits in graphs and digraphs, Hamiltonian paths and circuits in graphs and tournaments, trees; Minimum spanning tree, rooted trees and binary trees, planar graphs, Euler's formula, statement of Kuratowskey's theorem, dual of a planer graph, independence number and clique number, chromatic number, statement of Four-color theorem, dominating sets and covering sets.

3. Logic: Propositional calculus: propositions and connectives, syntax; Semantics: truth assignments and truth tables, validity and satisfiability, tautology; Adequate set of connectives; Equivalence and normal forms; Compactness and resolution; Formal reducibility - natural deduction system and axiom system; Soundness and completeness. Introduction to Predicate Calculus: Syntax of first order language; Semantics: structures and interpretation; Formal deductibility; First order theory, models of a first order theory (definition only), validity, soundness, completeness, compactness (statement only), outline of resolution principle.

References:

1. Jiři Matoušek, Jorosalav Nešetřil : Invitation to Discrete Mathematics, 2nd ed., Oxford University Press, 2006.

2. F. S. Roberts: Applied Combinatorics, 2nd ed.,Pearson Education/ Prentice Hall, Englewood Cliffs, NJ, 2005.

3. Peter J. Cameron: Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, 1994.

4. N. Deo: Graph Theory with Applications to Engineering and Computer Science, Prentice Hall, Englewood Cliffs, 1974.

5. J. L. Mott, A. Kandel and T. P. Baker: Discrete Mathematics for Computer Scientists, Reston, Virginia, 1983.

6. D. F. Stanat and D. E. McAllister: Discrete Mathematics in Computer Science, Prentice Hall, Englewood Cliffs, 1977.

7. C. L. Liu: Elements of Discrete Mathematics, 2nd ed., McGraw Hill, New Delhi, 1985.

8. R. A. Brualdi: Introductory Combinatorics, North-Holland, New York, 1977.

9. Reingold et al.: Combinatorial Algorithms: Theory and Practice, Prentice Hall, Englewood Cliffs, 1977.

10. J. A. Bondy and U. S. R. Murty: Graph Theory with Applications, Macmillan Press, London, 1976.

11. E. Mendelsohn: Introduction to Mathematical Logic, 2nd ed. Van-Nostrand, London, 1979.

12. L. Zhongwan: Mathematical Logic for Computer Science, World Scientific, Singapore, 1989.

13. Lewis and Papadimitriou: Elements of Theory of Computation (relevant chapter on Logic), Prentice Hall, New Jersey, 1981.

14. Joseph R. Shoenfield: Mathematical Logic, CRC Press, 1967

Automata Theory, Languages and Computation

1. **Automata and Languages:**Finite automata, regular languages, regular expressions, equivalence of deterministic and non-deterministic finite automata, minimization of finite automata, closure properties, Kleenes theorem, pumping lemma and its application, Myhill-Nerode theorem and its uses; Context-free grammars, context -free languages, Chomsky normal form, closure properties, pumping lemma for CFL, push down automata.

2. **Computability:** Computable functions, primitive and recursive functions, universality, halting problem, recursive and recursively enumerable sets, parameter theorem, diagonalisation, reducibility, Rices Theorem and its applications. Turing machines and variants; Equivalence of different models of computation and Church-Turing thesis.

3. **Complexity:** Time complexity of deterministic and nondeterministic Turing machines, P and NP, NP-completeness, Cooks Theorem, other NP -Complete problems.

References:

1. Sipser: Introduction to The Theory of Computation, PWS Pub. Co., New York, 1999.

2. J. E. Hopcroft, J. D. Ullman and R. Motwani: Introduction to Automata Theory, Languages and Computation, Addison- Wesley, California, 2001.

3. M. D. Davis, R. Sigal and E. J. Weyuker: Complexity, Computability and Languages, Academic Press, New York, 1994.

4. J. E. Hopcroft and J. D. Ullman: Introduction to Automata Theory, Languages and Computation, Addison-Wesley, California, 1979.

5. H. R. Lewis and C. H. Papadimitriou: Elements of The Theory of Computation, Prentice Hall, Englewood Cliffs, 1981.

6. M. R. Garey and D. S. Johnson: Computers and Intractability: A Guide to The Theory of NPCompleteness, Freeman, New York, 1979.

Introduction to Computing Systems I

1. **Computer Organization & Architecture:**

   (a) Binary systems, boolean algebra, boolean operations, minimization of boolean operations

   (b) Combinatorial and sequential logic

   (c) Processor design

   (d) Floating point arithmetic

   (e) Control Unit Design: Hardware control unit design, hardware programming language, microprogramming, horizontal, vertical and encoded-control microprogramming, microprogrammed control unit design.

   (f) Memory Organization: Random and serial access memories, ROMs, addressing

   (g) I/O Organization: Different techniques of addressing I/O devices, data transfer techniques, interrupts, bus control.

2. **Operating Systems:**

   (a) Basic architectural concepts, interrupt handling, concepts of batch-processing, multiprogramming, time- sharing, real-time operations; Resource Manager view, process view and hierarchical view of an OS.

   (b) Processor management: Scheduling, concurrent processes, critical sections, process co-ordination, deadlocks.

   (c) Memory management: Partitioning, paging, virtual memory, demand-paging, cache

   (d) Device Management: Scheduling algorithms -FCFS, shortest-seek-time-first, SCAN, C-SCAN, LOOK, C-LOOK algorithms, spooling, spool management algorithm.

   (e) Information Management: Concepts of file systems and access methods,

   (f) Case study of Unix file system.

References:

1. Z. Kohavi: Switching and Finite Automata Theory, 2nd ed., McGraw Hill, New York, 1978.

2. J. P. Hayes: Computer Architecture and Organization, 2nd ed., McGraw Hill, New York, 1988

3. P. Pal Choudhury: Computer Organization and Design, Prentice Hall of India, New Delhi, 1994.

4. M. M. Mano: Computer System Architecture, 3rd ed., Prentice Hall of India, New Delhi, 1993.

5. Y. Chu: Computer Organization and Micro-Programming, Prentice Hall, Englewood Cliffs, 1972.

6. D. A. Patterson and J. L. Hennessy: Computer Organization and Design, Revised Printing, 3 rd ed.: The Hardware/Software Interface, The Morgan Kaufmann Series in Computer Architecture and Design, July 2007.

7. W. Stallings: Computer Organization and Architecture: Principles of Structure and Function, 2nd ed., Macmillan, New York, 1990.

8. A. Silberschatz, P. B. Galvin, G. Gagne: Operating Systems Concepts, 9th ed., John Wiley and Sons, New York, 2005.

9. A. S. Tannenbaum: Mode Operating Systems, Pearson, 2016.

10. S. E. Madnick and J. J. Donovan: Operating Systems, McGraw Hill, New York, 1974.

Algebra and Number Theory

1. Group Theory: Elementary properties, subgroups, cosets, normal groups, quotient groups, cyclic groups, homomorphiosm and isomorphism, Isomorphisn theorem, permutation groups, Sylow's theorem and application, Application to Number theory: Lagrange's theorem , Euler's theorem, Fermat's theorem.

2. Rings and fields: Rings, Ideals, maximal ideals, quotient rings, Integral domains, principal ideal domain(PID), Euclidean domain(ED), ring of integers as example of PID and ED, Euclidean algorithm for GCD, extended Euclidean algorithm, finding modular inverse of an integer, Chinese Remainder Theorem(CRT), Euler's ϕ-function, quadratic residues.

3. Polynomials: Polynomial rings as ED and PID, irreducible polynomials, factorization, maximal ideals.

4. Vector spaces: subspaces, linear independence, basis, dimension, direct sum and complement, isomorphism

5. Linear transformation and matrices, algebra of matrices, rank and inverse, normal forms

6. System of linear equations, algorithms for solving linear equations

7. Determinants and their elementary properties

8. Finite Fields: elementary properties, construction

9. Selected Topics in Elementary Number Theory.

References:

1. D. F. Stanat and D. E. McAllister: Discrete Mathematics in Computer Science, Prentice Hall, Englewood Cliffs, 1977.
2. C. S. Sims: Abstract Algebra: A Computational Approach, John Wiley, New York, 1984.
3. L. L. Domhoff and F. E. Hohn: Applied Modem Algebra, Macmillan, New York, 1978.
4. J. B. Fraleigh: First Course in Abstract Algebra, Narosa/Addison-Wesley, New Delhi/Reading, 1982/1978.
5. I. N. Herstein: Topics in Algebra, Vikas Pub., New Delhi 1987.
6. G. Birkhoff and S. McLane: A Survey of Modem Algebra, 4th ed. Macmillan, New York, 1977.
7. D. Burton: Elementary Number Theory, 7th ed., McGraw Hill Education, 2017.
8. R. Lidl and H. Niederreiter: Introduction to Finite Fields and their Applications, Cambridge University Press, London, 1994.
9. H. Cohen: A Course in Computational Number Theory, Springer-Verlag, Berlin, 1993.
10. G. A. Jones and J. M. Jones: Elementary Number Theory, Springer-Verlag, London, 1998.

Probability and Statistics

1. Probability Theory
   (a) Probability, conditional probability and independence.
   (b) Random variables and their distributions (discrete and continuous), bivariate and multivariate distributions.
   (c) Laws of large numbers, central limit theorem (statement and use only).
   (d) Introduction to Stochastic process: Markov chains, random walks, queueing theory.
2. Statistics
   (a) Descriptive statistics: measures of location, spread, skewness, kurtosis; measures of association.
   (b) Estimation techniques.
   (c) Tests of Hypothesis.
   (d) Simulation techniques.

References:

1. W. Feller: An Introduction to Probability Theory and its Applications (Volume I and II), 3rd ed. John Wiley, New York, 1973.

2. P. G. Hoel, S. C. Port and C. J. Stone: Introduction to Probability Theory, University Book Stall/ Houghton Mifflin, New Delhi/New York, 199811971. 15

3. K. L. Chung: Elementary Probability Theory and Stochastic Processes, Springer-Verlag, New York, 1974.

4. S. M. Ross: Stochastic Processes, John Wiley, New York, 1983.

Computing Lab (Programming and Data Structures)

1. **Data Structures**
   (a) Introduction to problem-solving and basic algorithms.
   (b) Introduction to running time - basic concepts.
   (c) C programming: loops, arrays, pointers, structures, functions, recursion, file handling.
   (d) Basic data structures: Linked lists, Stacks, Queues, and their applications.
   (e) Searching and Sorting algorithms and their implementations.
   (f) Hash Tables.
   (g) Non-linear data structures: Graphs, Trees and some applications (BFS, DFS, tree traversals, BST etc.)

2. **Programming Tools and Techniques**
   (a) Program testing, developing test-plan, developing tests.
   (b) Version management, concept of CVS/SVN.
   (c) Concept of debugging and using debugging tools.
   (d) Writing shell scripts, using bash/tcsh.
   (e) Different compilation options and optimizations, concept of makefiles.

References:

1. L. Nyhoff, C++ An Introduction to Data Structures, Prentice Hall, Englewood Cliffs, 1998.

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

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

4. T. A. Standish: Data Structure Techniques, Addison-Wesley, Reading, Mass., 1980.

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

6. R. L. Kruse: Data Structures and Program Design in C, Prentice Hall of India, New Delhi, 1996.

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

8. B. Salzberg: File Structures: An Analytical Approach, Prentice Hall, New Jersey, 1988.

9. P. E. Livadas: File Structure: Theory and Practice, Prentice Hall, New Jersey, 1990.

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

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

12. Wood: Data Structure, Algorithms and Performance, Addison-Wesley, Reading, Mass., 1993.

13. B. W. Kernighan and D. M. Ritchie: The C Programming Language, Prentice Hall of India, 1994.

14. B. Gottfried: Programming in C, Schaum Outline Series, New Delhi, 1996.

15. B. W. Kernighan and R. Pike: The Unix Programming Environment, Prentice Hall of India, 1996.

Design and Analysis of Algorithms

1. Complexity measure and asymptotic notations, worst, best and average case analysis.

2. Complexity analysis of different searching and sorting algorithms.

3. Divide and conquer algorithms.

4. Greedy algorithms and applications in optimization.

5. Dynamic programming techniques and applications in optimization.

6. Graph algorithms.

7. NP-completeness.

References:

1. J. Kleinberg, E. Tardos: Algorithm Design, Pearson Education, 2006.

2. A. Aho, J. Hopcroft and J. Ullman; The Design and Analysis of Computer Algorithms, A. W. L, International Student Edition, Singapore, 1998

3. S. Baase: Computer Algorithms: Introduction to Design and Analysis, 2nd ed., Addison-Wesley, California, 1988.

4. T. H. Cormen, C. E. Leiserson and R. L. Rivest: Introduction to Algorithms, Prentice Hall of India, New Delhi, 1998.

5. E. Horowitz and S. Sahni: Fundamental of Computer Algorithms, Galgotia Pub. /Pitman, New Delhi/London, 1987/1978.

6. K. Mehlhorn: Data Structures and Algorithms, Vol. 1 and Vol. 2, Springer-Verlag, Berlin, 1984.

7. . A. Borodin and I. Munro: The Computational Complexity of Algebraic and Numeric Problems, American Elsevier, New York, 1975.

8. D. E. Knuth: The Art of Computer Programming, Vol. 1, Vol. 2 and Vol. 3. Vol. 1, 2nd ed., Narosa/Addison-Wesley, New Delhi/London, 1973; Vol. 2: 2nd ed., Addison-Wesley, London, 1981; Vol. 3: Addison-Wesley, London, 1973.

9. S. Winograd: The Arithmetic Complexity of Computation, SIAM, New York, 1980

Cryptology

1. Classical ciphers
2. Information Theoretic Security
3. Stream ciphers
4. Block ciphers
5. Cryptanalysis of Block and Stream Ciphers
6. Formal models for block and stream ciphers: Pseudorandom generators, Pseudorandom functions and permutations
7. Symmetric key encryption: Notion of CPA and CCA security with examples.
8. Symmetric key authentication.
9. Cryptographic hash functions.
10. Modern modes of operations: Authenticated Encryption, Tweakable Enciphering schemes.
11. Introduction to public key encryption, computational security and computational assumptions.
12. The Diffie Hellman key exchange.
13. The RSA, ElGamal, Rabin and Pailler encryption schemes
14. Digital Signatures
15. Introduction to Elliptic Curve Cryptosystems.
16. Public key infrastructures

References:

1. Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, Chapman & Hall/CRC, 2007.

2. Douglas R. Stinson: Cryptography Theory and Practice, 3rd ed., Chapman & Hall/CRC, 2006.

3. Dan Boneh, Victor Shoup: A Graduate Course in Applied Cryptography, online draft available at `http://toc.cryptobook.us/`.

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

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

Information and Coding Theory

1. Information Theory:
   (a) Concepts of Entropy its characterization and related properties
   (b) Asymptotic Equipartition Property
   (c) Data compression: Optimal codes, Huffman codes, Shannon-Fano coding, robustness of coding techniques
   (d) Channel capacity, fundamental theorem of information theory, applications.
2. Coding Theory:
   (a) Basics of coding theory
   (b) Linear Codes: Properties, Hamming Bound, MDS Codes
   (c) Cyclic codes: Hamming Codes, BCH Codes, Reed-Solomon Codes
   (d) Non-linear codes: Hadamard codes
   (e) Convolution codes
   (f) Construction of codes using combinatorial Designs
3. Fundamentals of Network Coding.

References:

1. T. M. Cover, J. A. Thomas: Elements of Information Theory, 2nd ed., Wiley Interscience, 2005.

2. R. Ash: Information Theory, Interscience Publ., Singapore, 1965.

3. E. R. Berlekamp: Algebraic Coding Theory, McGraw Hill, New York, 1986.

4. S. Lin: An Introduction to Error-Correcting Codes, Prentice Hall, Englewood Cliffs, 1970.

5. W. W. Peterson et al: Error Correcting Codes, Wiley, London, 1961.

6. R. W. Hamming: Coding and Information Theory, Prentice Hall, Englewood Cliffs, 1980.

7. A. Khinchin, Mathematical Foundations of Information Theory, Dover Publn., London, 1957.

8. F. J. McWilliams and N. J. Sloane: Theory of Error Correcting Codes, Parts I and II, North-Holland, Amsterdam, 1977.

9. V. Pless: Introduction to the Theory of Error Correcting Codes, 3rd ed., John Wiley, New York, 1982.

Introduction to Computing Systems II

1. **Computer Networks:**
   (a) OSI Stack: Details of layers of the OSI stack
   (b) Application layer protocols in details.
   (c) Routing Algorithms
   (d) Internet: IP protocol, Internet control protocols ICMP, APR and RAPP, Internet routing protocols OSPF, BGP and CIDR.
   (e) Wireless networks
2. **Database Management Systems**
   (a) Entity relationship model
   (b) Relational Model
   (c) Structured query language
   (d) Normalization
   (e) Crash recovery
   (f) Concurrency control

References:

1. A. Tannenbaum: Computer Networks, 3rd ed., Prentice Hall India, 1996.

2. W. Stallings: ISDN and Broadband ISDN With Frame Relay and ATM, Prentice Hall, Englewood Cliffs, 1995.

3. W. Stallings: Local and Metropolitan Area Networks, 4th ed., Macmillan, New York, 1993.

4. Kaufman, R. Perlman and M. Speciner: Network Security, Prentice Hall, Englewood Cliffs, 1995.

5. V. P. Ahuja: Design and Analysis of Computer Communication Networks, McGraw Hill, New York, 1987.

6. L. Gracial and I. Widjaja: Communication Networks, Tata-McGraw Hill, New Delhi, 2000.

7. L. L. Paterson and B. S. Davie: Computer Network, Morgan Kaufman, San Mateo, 2000.

8. H. F. Korth and A. Silberschatz: Database System Concepts, McGraw Hill, New Delhi, 1997.

9. R. A. Elmasri and S. B. Navathe: Fundamentals of Database Systems, 3rd ed., Addison-Wesley, 1998.

10. R. Ramakrishnan: Database Management Systems, 2nd ed., McGraw Hill, New York, 1999.

Computing Systems Security I

1. Introduction to basic security services:
   Confidentiality, integrity, availability, non-repudiation, privacy.

2. Anatomy of an Attack:
   Network Mapping using ICMP queries, TCP Pings, traceroutes, TCP and UDP port scanning, FTP bounce scanning, stack fingerprinting techniques, Vulnerability scanning, System and Network Penetration, Denial of Service.

3. Network Layer Protocols attacks and defense mechanisms:
   Hacking Exploits in ARP, IP4, IPv6, ICMP based DOS, ICMP covert Tunneling, Network Controls against flooding, Network Monitoring, SSL, IPSEC.

4. Transport Layer Protocols Attacks and Defense mechanisms:
   Covert TCP, TCP Syn flooding DOS, TCP Sequence Number Prediction attacks, TCP session hijacking, UDP Hacking Exploits, Network security controls for defense mechanism, OS hardening, kernel parameter tuning, DDOS & DDOS Mitigation, Stateful firewall, application firewalls, HIDS, NIDS and IPS.

5. Application Layer Protocol Attacks and Defense mechanisms:
   DNS spoofing attacks, DNS cache poisoning attacks, organization activity finger printing using DNS, SMTP vulnerability and Hacking Exploits, Mails relays, SMTP Security and Controls, HTTP hacking, Buffer Overflow Attacks, SQL Injection, Cross Side Scripting HTTP security and controls.

6. Malware detection and prevention

References:

1. Ross Anderson: Security Engineering, 2nd ed., Wiley. Available online: `http://www.cl.cam.ac.uk/~rja14/book.html`.

2. C.P. Pfleeger, S.L. Pfleeger, J. Margulies: Security in Computing, 5th ed., Prentice Hall, 2015.

3. David Wheeler: Secure Programming HOWTO. Available online: `https://www.dwheeler.com/secure-programs/`.

4. Michal Zalewski: Browser Security Handbook, Michael Zalewski, Google. Available online: `https://code.google.com/archive/p/browsersec/wikis/Main.wiki`.

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

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

Advanced Cryptology

1. Theoretical construction of pseudorandom objects: One way functions, pseudorandom generators, pseudorandom functions and pseudorandom permutations.

2. Secure Multiparty Computations.

3. Elliptic curves and bilinear pairings.

4. Lattice Based Cryptology.

References:

1. Oded Goldreich: Foundations of Cryptography Vol 1

2. Oded Goldreich: Foundations of Cryptography Vol 2

3. Dan Boneh, Victor Shoup: A Graduate Course in Applied Cryptography, online draft available at `http://toc.cryptobook.us/`.

4. Steven D. Galbraith: Mathematics of Public Key Cryptography, Cambridge University Press, 2012

5. Rafael Pass and Abi Shelat: A Course in Cryptography, Lecture notes. Available online: `https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf`

6. Daniele Micciancio, Shafi Goldwasser, Complexity of Lattice Problems: A Cryptographic Perspective, Kluwer, 2002.

7. Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press 2008.

8. S. Chatterjee, P. Sarkar: Identity-Based Encryption, Springer, 2011.

Computing Systems Security II

1. Cellular networks, Access Technologies, GSM, CDMA, GPRS, 3G networks, Wireless LAN, WLAN security.
2. Operating Systems Security:
   (a) Access Control Fundamentals
   (b) Generalized Security Architectures
   (c) Analysis of security in Unix/Linux and problems with the design of its security architecture
   (d) Analysis of security in Windows and problems with its security architecture
   (e) Security Kernels: SCOMP design and analysis, GEM-SOS design
   (f) Difficulties with securing Commercial Operating Systems (Retrofitting Security)
   (g) Security issues in Virtual Machine Systems
   (h) Security issues in sandboxing designs: design and analysis of Android.
3. Database Security:
   (a) Introduction: Security issues faced by enterprises
   (b) Security architecture
   (c) Administration of users
   (d) Profiles, password policies, privileges and roles
   (e) Database auditing

References:

1. Ross Anderson: Security Engineering, 2nd ed., Wiley. Available online: `http://www.cl.cam.ac.uk/~rja14/book.html`.
2. C.P. Pfleeger, S.L. Pfleeger, J. Margulies: Security in Computing, 5th ed., Prentice Hall, 2015.
3. David Wheeler: Secure Programming HOWTO. Available online: `https://www.dwheeler.com/secure-programs/`.
4. Michal Zalewski: Browser Security Handbook, Michael Zalewski, Google. Available online: `https://code.google.com/archive/p/browsersec/wikis/Main.wiki`.
5. M. Gertz, S. Jajodia (Eds.): Handbook of Database Security, Springer, 2008.
6. B. S. Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley and Sons, New York, 1995.
7. A. Menezes, P. C. Van Oorschot and S. A. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.

Cryptographic and Security Implementations

This course would be project based, by the end of the course each student should do two non-trivial implementation projects in the following broad areas:

1. Cryptographic Implementations:
   (a) Instruction set architecture of modern processors with emphasis on instructions dedicated for cryptographic use.
   (b) Programming in micro controllers.
   (c) Software side channel attacks and countermeasures.
   (d) Principles of hardware design.
   (e) Introduction to hardware description languages.
   (f) Hardware side channel attacks, fault attacks and countermeasures.
   (g) Crypto libraries.
2. Security Implementations:
   (a) Logging, Auditing and Log Monitoring
   (b) Enforcing password complexity, aging, and lockout
   (c) Implementing Security Access Control
   (d) File locks, database locks
   (e) Firewall and Antivirus implementation and setup.
   (f) Intrusion Detection and Malware Detection.

References:

1. N. Ferguson, B. Schneier: Practical Cryptography, Wiley, 2003.
2. B. S. Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley and Sons, New York, 1995.
3. F. Rodríguez-Henríquez, A. Díaz Pérez, N. A. Saqib, etin Kaya Koc: Cryptographic Algorithms on Reconfigurable Hardware, Springer.
4. Luca Giancane: Side-Channel Attacks and Countermeasures, LAP Lambert Academic Publishing, 2012.
5. Eric Cole: Network Security Bible, 2nd ed., Wiley 2009.

Quantum Information and Cryptography

1. Introduction to Quantum Information.
2. States, Operators, Measurements.
3. Quantum Entanglement.

4. Quantum Teleportation.
5. Super-dense coding.
6. Quantum gates and circuits.
7. Quantum search.
8. Shor's factoring algorithm and its implication towards security in quantum world.
9. Quantum key distribution.
10. Quantum secret sharing and multiparty computation.

References:

1. Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press, 2002.
2. An Introduction to Quantum. Computing, Phillip Kaye, Raymond Laflamme, and Michele Mosca. Oxford U. Press, New York, 2007.
3. Presskil Lecture notes. Available online: `http://www.theory.caltech.edu/~preskill/ph229/`.
4. Quantum Computer Science, N. David Mermin, Cambridge University Press 2007.

Topics in Privacy

1. Review of cryptographic protocols: Homomorphic Encryption, group signatures, blind signatures, anonymous credential management, commitment schemes, zero-knowledge proofs, proof of knowledge, ZK-SNARK, oblivious transfer, secure multiparty computation, Oblivious RAM, private set intersections, private information retrieval.
2. Perturbation, K-anonymity, L-diversity
3. Differential privacy
4. De-anonymization techniques
5. Privacy preserving analytics
6. Applications: Mixnets, Onion Routing (TOR), e-cash, e-voting, location privacy, profiling
7. Privacy for outsourced data
8. Privacy risk analysis
9. Privacy Ethics: Privacy compliance, GDPR, HIPPA etc.

References:

1. Cynthia Dwork, Aaron Roth: The Algorithmic Foundations of Differential Privacy (Foundations and Trends in Theoretical Computer Science).
2. Jonathan Katz and Yehuda Lindell: Introduction to Modern Crypography, Second Edition, CRC Press.
3. Rafael Pas and abi shelat, A Course in Cryptography, Lecture notes. Available online: https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf
4. Internet Resources and research papers.

Topics in Security

Topics related to contemporary and emerging areas in security would be discussed.:

1. Digital Forensics
2. Penetration testing and Vulnerability Analysis
3. Biometrics
4. Cybersecurity for critical infrastructure
5. Game theory and security

References:

1. Gerard Johansen: Digital Forensics and Incident Response, Packt Publishing Limited 2017
2. Wil Allsopp: Advanced Penetration Testing, Wiley 2017
3. A.K. Jain, A. A. Ross, K. Nandakumar, Introduction to Biometrics, Springer 2011
4. John Chirillo, Scott Blaul: Implementing Biometric Security, Wiley 2003
5. Recent papers and internet resources.

Topics in Cryptology

In depth study in some contemporary and emerging areas in cryptology. The list will be updated from time to time. Topics may include but not limited to

1. Algorithms for factoring and discrete logarithms
2. Cryptosystems based on Isogenies,
3. Secure Multiparty Computation
4. Homomorphic Encryption

5. Cloud Cryptology
6. Authenticated encryption

References:

1. H. Cohen: A Course in Computational Algebraic Number Theory, Springer 1996
2. Steven D. Galbraith: Mathematics of Public Key Cryptography, Cambridge University Press, 2012
3. Dan Boneh, Victor Shoup: A Graduate Course in Applied Cryptography, online draft available at `http://toc.cryptobook.us/`.
4. Recent research papers and internet resources.

Computational Number Theory

1. Divisibility, primality, GCD, factorization.
2. Congruences: Basic properties; solving linear congruences, chinese remainder theorem. eulers ϕ function, quadratic residiues.
3. Computing with integers: Asymptotic notations, Integer arithmetic, computing in Z_n.
4. Euclid's Algorithm: Division Algorithm, extended Euclidean Algorithm, Computing modular inverses.
5. Distribution of primes: Chebyshev's Theorem and the distribution of primes, Betrands postulate, prime number Theorem.
6. Probabilistic Algorithms: Basic definitions, gnerating a random prime, generating a random factored number. Primality testing- Miller rabin; generating random primes using Miller-Rabin, Factoring and computing Euler's ϕ function.
7. Finding generators and discrete log in Z_p^*. Diffie-Hellman key exchange. Testing quadratic residuosity. Computing modular square root. Quadratic residuposity assumption.
8. Subexponential-time discrete log and factoring.
9. Algorithms for finite fields.
10. Special topics.

References:

1. Victor Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press
2. Abhijit Das: Computational Number Theory, CRC Press

Machine Learning for Security

This course would provide introduction to basic techniques and tools of machine learning and would include a few case studies of using these techniques in security applications.

1. Supervised Learning
   (a) Setup for supervised learning
   (b) Regression, logistic regression
   (c) Generative learning algorithms, Gaussian Discriminant analysis, Naive Bayes
   (d) Nonparametric methods, k-nearest neighbor classification
   (e) Supervised neural networks: Perceptrons, Multilayered perceptrons, radial basis functions
   (f) Maximum margin classifiers, support vector machines
   (g) Model selection and feature selection
   (h) Ensemble methods: Bagging and Boosting
2. Unsupervised learning
   (a) Clustering, K-means
   (b) Expectation maximization, Mixture of Gaussians
   (c) Factor analysis
   (d) Principal component analysis and Independent component analysis.
3. Possible case studies:
   (a) Machine learning for intrusion detection.
   (b) Machine learning for side channel analysis.
   (c) Privacy preserving machine learning.
   (d) Adversarial machine learning.

References:

1. Tom M. Mitchell: Machine Learning, McGraw Hill Education
2. C. Bishop: Pattern Recognition and Machine Learning, Springer
3. Trevor Hastie, Robert Tibshirani: The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, 2009.
4. Recent research papers

Blockchains and Cryptocurrencies

This course will provide introduction to blockchains and cryptocurrencies including Bitcoin and contracts. Basic tools will be introduced first, followed by implementation of practical blockchain protocols.

1. Motivation and overview of blockchains.
2. Building blocks: Hash functions, signature schemes, zero-knowledge proofs, consensus algorithms.
3. Bitcoin: Transactions, blocks, mining, scripting, attacks on mining.
4. Proof of work, proof of stake, proof of burn, proof of storage.
5. Smart contracts
6. Privacy issues: Anonymity, mixing techniques, privacy with ZK-Snarks.
7. Permissioned blockchains: Distributed consensus, sharing algorithms, privacy issues.
8. Scaling issues: Lightning networks, Payment networks.
9. Platforms and ledgers: Ethereum, Ripple, Hyperledger, Algorand, etc.
10. Altcoins and their analysis.
11. Applications: Banking and finance, Data Sharing, Supply-chain, etc.

References:

1. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S Goldfeder, J. Clark: Bitcoin and Cryptocurrency Technologies, Princeton University Press. 2017.
2. A. M. Antonopoulos: Mastering Bitcoin: Programming the Open Blockchain, O'Reilly, 2017.
3. Web Resources.

Social and Legal Aspects of Security

1. History of Cryptology/Security
2. Relationship between law/politics/social issues and cryptography/security
3. Motivations at National and International Level
4. Export control or Cryptologic/Security products
5. Indian Cyber Law: (i) Information Technology Law in India (ii) Selected Cyber Law Cases (iii) Selected Adjudicating Officer Orders (iv) Data Privacy Law in India (v) IT Act Audit & Compliance (vi) Documentation Issues (vii) International Cyber Crime Law (viii) Emerging Issues in Cyber Law.

6. Various facets of Cyber Crime and Investigation
7. Copyright management
8. Social Issues: Social welfare schemes such as Aadhar.
9. Electronic voting.
10. Security Ethics.

References:

1. Ross Anderson: Security Engineering, 2nd ed., Wiley. Available online: `http://www.cl.cam.ac.uk/~rja14/book.html`.
2. Susan Landau: Surveillance or Security? The Risks Posed by New Wiretapping Technologies, MIT Press, 2011
3. Whitfield Diffie and Susan Landau: Privacy on the Line The Politics of Wiretapping and Encryption, MIT Press, 2007
4. Helen Nissenbaum: Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009.