Department of Computer Science and Engineering

Curriculum for M Tech in Computer Science and Engineering (Information Security)

Semester 1

	Code	Title	L	T	P/S	Cr
1	CS 6101	Mathematical Foundations of Computer Science	3	0	2	4
2	CS 6213	Foundations of Information Security	3	0	2	4
3	CS 6103	Software Systems Lab	1	0	6	4
4		Elective	3	0	2	4
5		Elective	3		0/2	3/4
		Total credits				19/20

Semester 2

	Code	Title	L	T	P/S	Cr
1	CS 6204	Term Paper-I (optional)	0	0	6	3
2		Elective	3	0	2	4
3		Elective	3	0	2	4
4		Elective	3	0	2	4
5		Elective	3		0/2	3/4
6		Elective (optional)	3		0/2	3/4
		Total credits				16 to 23

Semester 3

	Code	Title	L	T	P/S	Cr
1	CS 7298	Project				8
		Elective (optional)	3		0/2	3/4
		Total credits				8/11/12

Semester 4

	Code	Title	L	T	P/S	Cr
1	CS 7299	Project				12
		Total credits				12

Minimum Requirements

1. A Candidate should have earned a total of at least 60 credits, including at least 20 credits from project work
2. The number of electives credited by a student can be varied subject to minimum credit requirements for completion of the course.

Credits for elective courses may vary depending on the practical work involved

LIST OF ELECTIVES

	Code	Title	Credit
1.	CS 6102	Compiler Design	4
2.	CS 6110	Algorithms and Complexity	4
3.	CS 6112	Operating System Design	4
4.	CS 6121	Computability Theory	3
5.	CS 6122	Computer Architecture	4
6	CS 6123	Database Design	4
7	CS 6124	Topics in Programming Languages	4
8	CS 6125	Computer Networking	4
9	CS 6131	Logic and Computation	3
10.	CS 6132	Topics in Algorithms	4
11	CS 6133	Game Theory	4
12	CS 6134	Quantum Computation	3
13	CS 6135	Logic for Computer Science	4
14	CS 6136	Topics in Combinatorial Algorithms	4
15	CS 6141	Distributed Computing	4
16	CS 6142	Topics in Computer Architecture	4
17	CS 6143	Trends in Middleware Systems	4
18	CS 6144	Multicore Systems	4
19	CS 6151	Software Engineering	4
20	CS 6152	Object Oriented Modeling and Design	4
21	CS 6154	Topics in Database Design	4
22.	CS 6161	Embedded Systems and Applications	4
23.	CS 6171	Natural Language Processing	4
24.	CS 6172	Computational Intelligence	4
25.	CS 6173	Image Processing	4
26.	CS 6174	Pattern Recognition	4
27	CS 6181	Bioinformatics	4
28.	CS 6201	Cryptography	4
29.	CS 6211	Formal Methods in Secure Computing	4
30.	CS 6212	Network Security	4
31.	CS 6214	Advanced Topics in Information Security	4
32.	CS 6231	Theoretical aspects of cryptographic algorithms	3
33.	CS 6232	Cryptocomplexity	4
34.	CS 6233	Information Theory and Coding	4
35.	CS 6261	Perimeter Security	4
36.	CS 6271	Data Compression	4
37.	CS 6282	Pragmatics of Information Security	4
38.	CS 6283	Computer Laws and Ethics	3
39.	CS 6284	Security Policies and Assurance	3
40.	CS 6285	Information Security Management	4

41.	CS 6286	Metrics for Information Security Assessment	4
42	MA 8152	Fuzzy Set Theory and Applications	3
43	MA 7156	Advanced Topics in Graph Theory	3

BRIEF SYLLABUS

CS 6201 : Cryptography

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Review of number theory and algebra, computational complexity, probability and information theory, primality testing.Cryptography and cryptanalysis, symmetric key encryption, DES, Triple DES, AES, RC4, modes of operation. public key encryption, RSA cryptosystem, Diffie-Hellman, elliptic curve cryptography, Rabin, ElGamal, Goldwasser-Micali, Blum-Goldwasser cryptosystems. Message authentication, digital signature algorithms. Security handshake pitfalls, Strong password protocols.

CS 6204: Term Paper

Prerequisite: Nil

L	T	P	C
0	0	6	3

Total Hours: 0+84

The aim of this course is to introduce the student to research, and to acquaint him with the process of presenting his work through seminars, technical reports and research papers.

CS 6211: Formal Methods in Secure Computing

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Decidability of security, Access control, take grant model, SPM, Expressive power of models, typed access control models Authentication and key establishment, Freshness, general design principles, common attacks, forward secrecy, multiparty authentication, Anonymity Protocol Verification and Correctness, Logic based Models, BAN Logic, Spi calculus Strand space based analysis, Applicability to group protocols

CS 6212 : Network Security

Prerequisite: Foundations of Information Security

L	T	P	C
3	0	2	4

Total Hours: 42+28

Review of wired/wireless network protocols, intrusion detection systems, malicious software. Review of cryptographic algorithms and protocols, cryptanalysis, authentication and signature protocols. Kerberos, PKI, real-time communication security, IPSec: AH, ESP, IKE. SSL/TLS, e-mail security, PEM and S/MIMIE, PGP, web security, network management security, wireless security.

CS 6213: Foundations Of Information Security

Prerequisite: Discrete Mathematics, Computer Networks

L	T	P	C
3	0	2	4

Total Hours: 42+28

Security Taxonomy. System security- Access Control - Security Models as basis for OS security. Introduction to DB Security. Software vulnerabilities Topological worms. Internet propagation models for worms.Cryptography, Secret vs. Public, Secret Key - DES, Public Key - RSA, Cryptographic hash - SHA1, Discrete Log - Diffie Helman, Digital certificates and PKI Protocol One way and two way authentication, Centralised Authentication, Biometrics for authentication - methods and error types. Network layer security - IPSec, Transport layer security - SSL. Attacks Firewalls.

CS 6214: Advanced Topics in Information Security

Prerequisite: Foundations of Information Security

L	T	P	C
3	0	2	4

Total Hours: 42+28

Cryptography - Practical considerations on cryptographic algorithms - Performance and Robustness.Network Security - DNS attacks and DNSSEC. Cross-site scripting XSS worm, SQL injection attacks. Intrusion Detection Systems (IDS). Security in current domains - Wireless LAN security - WEP details. bluetooth security issues. Security in current applications.

CS 6231: Theoretical aspects of cryptographic algorithms

Prerequisite: Foundations of Information Security

L	T	P	C
3	0	0	3

Total Hours: 42

Euclid's algorithm for integers and polynomials – applications to modular inversion, Rational polynomial approximation etc.Quadratic reciprocity and application to Primality testing.Polynomial and integer factorization. Applications to cryptography and coding theory.

CS 6232: Cryptocomplexity

Prerequisite: Analysis of Algorithms, Foundations of Information Security

L	T	P	C
3	0	2	4

Total Hours: 42+28

Review of Relevant Mathematics, Complexity Theory, Foundations of Cryptology, Hierarchies based on NP.Randomized algorithms and Complexity classes, probabilistic Polynomial time classes, Quantifiers, Graph Isomorphism and lowness.RSA Cryprosystem, primality and factoring, Primality Tests, Factoring Methods, Security of RSA. Diffie Hellman's, ElGamal's and other protocols, Arthur Merlin Games and Zero knowledge.

CS 6233 : Information Theory and Coding

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Introduction to probability, information, noiseless coding, noisy coding, cyclic redundancy checkspermutation of sets, finite fields, linear codes, bounds for codesprimitive polynomials, RS and BCH codes Concatenated codes, curves and codes.

CS 6261 : Perimeter Security

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Computer security, attacks, methods of defense.Intrusion detection, audit records, statistical, rule-based and distributed intrusion detection, responses to intrusion detection, honeypots, password management, malicious software, viruses and related threats, virus countermeasures Firewalls, design of firewalls, trusted systems, Trojan horse defense Security planning, risk analysis, security policies, physical security, covert communication, steganography tools, digital watermarking.

CS 6271: Data Compression

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Introduction, Basic Techniques, Dictionary Methods Image Compression, Transform based techniques, Wavelet Methods, adaptive techniques Video compression, Audio Compression, Fractal techniques.Comparison of compression algorithms. Implementation of compression algorithms.

CS 6282: Pragmatics of Information Security

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Information Security: Issues and Solutions. Evolution of cryptography and cryptographic protocols, relationship with mathematical developments. Vulnerability, Threat, Risk Assessments and Managements. Critical Assets**.** Enterprise security - Policy, Standards, Guidelines and Procedures. Legal requirements

CS 6283: Computer Law and Ethics

Prerequisite: Nil

L	T	P	C
3	0	0	3

Total Hours: 42

Intellectual property rights, computer software copyrights, copyright in databases and electronic publishing, law of confidence, patent laws, trademarks, product designs, international law .

Computer contracts, liability for defective hardware and software, software contracts, web and hardware contracts, electronic contracts and torts, liabilities. Computer crime, computer fraud, hacking, unauthorized modification of information, piracy, computer pornography and harassment. Cyber laws in India, IT Act 2000, data subjects' rights, ethical issues in computer security, case studies.

CS 6284: Security Policies and Assurance

Prerequisite: Nil

L	T	P	C
3	0	0	3

Total Hours: 42

Security policies, policy languages, confidentiality policies, Bell-LaPadula model, controversies over the model. Integrity policies, Biba model, Lipner's model, Clark-Wilson models, Chinese wall model, clinical information systems security policy, noninterference and policy composition. Assurance and trust, building secure and trusted systems, waterfall model, other models of development. Assurance in requirements definition and analysis, assurance during system and software design, assurance during implementation and integration.

CS 6285: Information Security Management

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Information as an Asset – creation and maintenance. Information Security Management (ISM) in organizations. Information Asset Management and Risk analysis. Perimeter security. Use of biometrics in this context. Access control models and Role based approaches for organizational hierarchy. Firewalls, VPNs and IDS. Managing wireless network security. Application Security. choice of security architecture for thirdparty software and turnkey software projects. Choosing the building blocks of information systems of the firm with security considerations – Disaster recovery approaches business continuity. Security models and frameworks. Security standards and compliance needs in different business domains. IT Act and other legal requirements

CS 6286: Metrics for Information Security Assessment

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours: 42+28

Introduction to information security and the concept of information assurance. Need for measurement for assessment and improvement Types/classification of metrics - qualitative vs. quantitative. Operational, Incident and Compliance metrics. Developing good metrics –Probabilistic Risk Assessment. Modeling approaches for security metrics: Graph theoretic models like attack trees and defense trees, Game theoretic models. Information security management metrics at various organizational levels. Tools and technologies for information security assessment.

Detailed Syllabus

CS 6201 : Cryptography

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (9 hours)
Review of number theory and algebra, computational complexity, probability and information theory, primality testing.
Module 2: (10 hrs)
Cryptography and cryptanalysis, symmetric key encryption, DES, Triple DES, AES, RC4, modes of operation.
Module 3: (13 hrs)
public key encryption, RSA cryptosystem, Diffie-Hellman, elliptic curve cryptography, Rabin, ElGamal, Goldwasser-Micali, Blum-Goldwasser cryptosystems.
Module 4: (10 hrs)
Message authentication, digital signature algorithms. Security handshake pitfalls, Strong password protocols.

References

1. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004.
2. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a public World, 2/e, Prentice Hall, 2002.
3. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
4. H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, Springer-Verlag, 2002.

CS 6204: Term Paper

Prerequisite: Nil

L	T	P	C
0	0	6	3

Total Hours (0+84)

The aim of this course is to introduce the student to research, and to acquaint him/her with the process of presenting his work through seminars, technical reports and research papers.
The student is expected to do an extensive literature survey and analysis in an area related to computer science, chosen by him, under the supervision of a faculty member from the department. The study should preferably result in design ideas, designs, algorithms, theoretical contributions in the form of theorems and proofs, new methods of proof, new techniques or heuristics with analytical studies, implementations and analysis of results.
The student should give two seminars on his work, one in the middle of the semester and the other at the end of the semester, and submit a technical report.

References

Articles from ACM/IEEE Journals/Conference Proceedings and equivalent documents, standard textbooks and web based material, approved by the supervisor.

CS 6213: Foundations Of Information Security

Prerequisite: Discrete Mathematics, Computer Networks

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (10 hours)

Introductory Topics: Security Taxonomy, Domain of information security.

System security topics : Access Control - MAC. DAC, RBAC. Security Models as basis for OS security - BLP, Biba, Chinese Wall and Clark Wilson. Introduction to DB Security. Software vulnerabilities - Buffer and stack overflow, Phishing. Malware - Viruses, Worms and Trojans. Topological worms. Internet propagation models for worms.

Module 2: (12 hours)

Cryptography Topics: Secret vs. Public, Secret Key - DES, Public Key - RSA, Cryptographic hash - SHA1, Discrete Log - Diffie Helman, Digital certificates and PKI

Module 3: (9 hours)

Protocol topics: One way and two way authentication, Centralised Authentication, Needham-Schroeder protocol, Kerberos. Biometrics for authentication - methods and error types.

Module 4: (11 hours)

Network security topics: Network layer security - IPSec, Transport layer security - SSL. Attacks - DoS, DDoS, ARP spoofing, session hijacking. Firewalls - placement and configuration.

References

1. Bernard Menezes, Network security and Cryptography, Cengage Learning India, 2010.
2. Dieter Gollmann. Computer Security, John Wiley and Sons Ltd., 2006.
3. Charles P Pfleeger, Shari Lawrence Pfleeger. Security in Computing, Education, 2005.
4. Furnell, Katsikas, Lopez, Patel. Securing Information and Communication Systems: Principles, Technologies and Applications,Artech House Inc., 2008.
5. H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, Springer-Verlag, 2002.
6. Whitman and Mattord, Principles of Information Security, Cengage Learning, 2006.
7. Speed and Ellis, Internet Security, Elsevier Science, 2003.

CS 6211: Formal Methods in Secure Computing

Prerequisite: Discrete Mathematics, Theory of Computation

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (10 hours)
Decidability of security, Access control, take grant model, SPM, Expressive power of models, typed access control models

Module 2: (8 hours)
Authentication and key establishment, Freshness, general design principles, common attacks, forward secrecy, multiparty authentication, Anonymity

Module 3: (12 hours)
Protocol Verification and Correctness, Logic based Models, BAN Logic, Spi calculus

Module 4: (12 hours)
Strand space based analysis, Applicability to group protocols

References

1. Willis H Ware, Charles P Pfleeger, Shari Lawrence Pfleeger, Security in Computing , Prentice Hall, Third Edition, 2003
2. Theo Dimitrakos, Fabio Martinelli Formal Aspects In Security And Trust: Ifip TN Wg1.7 Workshop on Formal Aspects in Security, Springer, 2005
3. Computer Security Handbook, 4th Edition. Seymour Bosworth, M E Kabay (Editors). John Wiley, 2002.
4. M. Bishop and S. S. Venkatramanayya, Introduction to Computer Security, Pearson Education Asia, 2005.
5. M. Abadi and A. D. Gordon, A Calculus for Cryptographic Protocols — The Spi Calculus, Research report SRC 149, 1998.
6. L. Buttyán and J. P. Hubaux, A Formal Analysis of Syverson's Rational Exchange Protocol. IEEE Computer Security Foundations Workshop, 2002.
7. C. Caleiro, L. Viganò, and D. Basin, On the Semantics of Alice&Bob Specifications of Security Protocols. Theoretical Computer Science, vol. 367, no. 1–2, 2006, pp. 88-122.
8. C. Haack and A. Jeffrey, Pattern-matching Spi-calculus, Proc. FAST'04, IFIP series 173, 2004, pp. 193-205.
9. A. Huima, Efficient Infinite-State Analysis of Security Protocols, Workshop on Formal Methods and Security Protocols, 1999.
10. C. Meadows, A formal framework and evaluation method for network denial of service, In Proc. of the 12th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, vol. 9, no. 1, 2001, pp. 47–74.
11. J. Millen and V. Shmatikov, Constraint solving for bounded-process cryptographic protocol analysis, in 8th ACM Conference on Computer and Communication Security, Nov. 2001, pp. 166–175.
12. N. Nisan and A. Ronen, Algorithmic Mechanism Design. in Proc. 31st Annual ACM Symposium on Theory of Computing, Atlanta, GA, 1999, pp. 129-140.

13. P. Syverson and I. Cervesato, The Logic of Authentication Protocols. Lecture Notes in Computer Science, vol. 2171, 2001, pp. 63–136.
14. F. J. Thayer, Strand Spaces: Proving Security Protocols Correct. Journal of Computer Security, vol. 7, Issue 2-3, Jan. 1999, pp.191-230.

CS 6212 : Network Security

Prerequisite: Foundations of Information Security

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (10hrs)
Review of wired/wireless network protocols, intrusion detection systems, malicious software.

Module 2: (10hrs)
Review of cryptographic algorithms and protocols, cryptanalysis, authentication and signature protocols.

Module 3: (12hrs)
Kerberos, PKI, real-time communication security, IPSec: AH, ESP, IKE.

Module 4: (10 hrs)
SSL/TLS, e-mail security, PEM and S/MIMIE, PGP, web security, network management security, wireless security.

References

1. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a public World, 2/e, Prentice Hall, 2002.
2. Kurose J. F. & Ross K. W., Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education Asia, 3/e, 2005.
3. Schiller J., Mobile Communications, Pearson Education Asia,2/e, 2004.
4. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.

CS 6231: Theoretical aspects of cryptographic algorithms

Prerequisite: Nil

L	T	P	C
3	0	0	3

Total Hours (42)

Module 1(9 hrs)
Euclid's algorithm for integers and polynomials – two squares theorem, applications to modular inversion, Rational polynomial approximation etc.

Module 2: (10 hrs)
Quadratic reciprocity and application to primality testing.

Module 3: (10 hrs)
Polynomial and integer factorization, algorithms, deterministic algorithm.

Module 4: (13 hrs)
Rings, Finite Fields and Applications to cryptography and coding theory.

References:

1. V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press, Second Print edition, 2008.
2. J. Von Zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, 2003.
3. Journal of Algorithms. Elsevier.

CS 6232: Cryptocomplexity

Prerequisite: Analysis of Algorithms

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (9 hours)
Review of Relevant Mathematics, Complexity Theory, Foundations of Cryptology, Hierarchies based on NP.

Module 2: (10 hrs)
Randomized algorithms and Complexity classes, probabilistic Polynomial time classes, Quantifiers, Graph Isomorphism and lowness.

Module 3: (10 hrs)
RSA Cryprosystem, primality and factoring, Primality Tests, Factoring Methods, Security of RSA.

Module 4: (13 hrs)
Diffie Hellman's, ElGamal's and other protocols, Arthur Merlin Games and Zero knowledge.

References

1. Jorg Roth, Complexity Theory and Cryptology – An introduction to cryptocomplexity, Springer, 2005.
2. H. Anton, Elementary Linear algebra, John Wiley and Sons, New York, Eighth Edition, 2000.
3. G. Brassard. A note on the complexity of cryptography, IEEE Transactions on Information Theory, 25(2):232-233, 1979.

CS 6233 : Information Theory and Coding

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (12 hrs)
Introduction to probability, information, noiseless coding, noisy coding, cyclic redundancy checks

Module 2: (10 hrs)
Permutation of sets, finite fields, linear codes, bounds for codes Hamming (Sphere-Packing) Bound. Gilbert-Varshamov Bound. Singleton Bound.

Module 3: (10 hrs)
Primitive polynomials, Testing for Primitivity. Periods of LFSR's. Vandermonde Determinants. Check Matrices for Cyclic Codes. RS Codes. Hamming Codes (Again). BCH Codes. Decoding BCH Codes.

Module 4: (10 hrs)
Concatenated codes, curves and codes. Plane Curves. Curves in Higher Dimensions. Geometric Goppa Codes.

References:

1. P. Garrett, The Mathematics of Coding Theory: Information, Compression, Error Correction and Finite Fields, Pearson Education, 2004.
2. Shu Lin, Daniel J Costello, Error Control Coding - Fundamentals and Applications, Prentice Hall Inc. Englewood Cliffs.
3. San Ling, Coding Theory – A First Course. Cambridge Press, 2004.

CS 6261 : Perimeter Security

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (6 hrs)
Computer security, attacks, methods of defense.

Module 2: (12 hrs)
Intrusion detection, audit records, statistical, rule-based and distributed intrusion detection, responses to intrusion detection, honeypots, password management, malicious software, viruses and related threats, virus countermeasures

Module 3: (12 hrs)
Firewalls, design of firewalls, trusted systems, Trojan horse defense

Module 4: (12 hrs)
Security planning, risk analysis, security policies, physical security, covert communication, steganography tools, digital watermarking.

References:

1. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005.
2. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
3. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003.
4. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.

CS 6271: Data Compression

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (10 hrs)

Introduction to data compression-Basic Techniques- Runlength encoding, RLe Text compression, RLE image compression, Move-to-front coding, Scalar quantization.Statistical Methods- Information theory concepts, variable sixe codes, prefix codes, Shanon fanon coding, Huffman coding, Adaptive Huffman, Arithmetic coding.

Module 2: (10 hrs)

Dictionary methods- string compression, LZ77 sliding window, MZW, Gif images. Image Compression- Approaches to image compression, intuitive methods, image transform, test images, JPEG, Progressive image compression, Vector quantization,

Module 3: (10 hrs)

Wavelet Methods- Fourier transform, frequency domain, Fourier image compression, CWT and inverse CWT, Haar transform, filter bank, DWT, JPEG 2000. Video compression- analog video, Composite and component video, digital video, video compression, MPEG.

Module 4: (12hrs)

Audio Compression- Sound, digital audio, human auditory system, MPEG-1 audio layer. Fractal based compression- IFS. Comparison of compression algorithms. Implementation of compression algorithms.

References

1. David Solomon, Data compression: The Complete Reference, 2nd edition, Springer-Verlag, New York. 2000.
2. Stephen Welstead, Fractal and Wavelet Image Compression Techniques, PHI, NewDelhi-1, 1999.
3. Khalid Sayood, Introduction to Data compression, Morgan Kaufmann Publishers, 2003 reprint.

CS 6282: Pragmatics of Information Security

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (7 hrs)
Taxonomy of information security. Information as an asset. Need for securing information in the contexts of individuals, organizations, business, and government. Impact of information security on ensuring security in a broader context.

Module 2: (11 hrs)
Evolution of cryptography – from Enigma to Elliptic Curve Cryptography. Interlinkings with number theory and other developments in mathematics. Development of cryptographic protocols. Concept of cryptocomplexity.

Module 3: (11 hrs)
Information security in the context of Trust and Privacy. Models of trust and computational aspects. Difference between privacy and security. Relevance of privacy rights from individual and organizational viewpoints – links with information security. Security as a dynamic equilibrium between attacks and defenses. Modeling attack and defense mechanisms using game theoretic concepts.

Module 4: (13 hrs)
Enterprise security - Policy, Standards, Guidelines and Procedures. The balance between operational security and compliance/legal requirements in specific domains – An example of financial (SOX) or health (HIPAA) may be adopted. International standardization – ISO 27000 series (1 to 6) – salient features.

References

1. Security Engineering with patterns: origins, theoretical model, and new applications. Markus Schumacher. LNCS 2754, Springer.
2. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.
3. Information Security Management Handbook, 5th Edition, Harold Tipton, Micki Krause (Editors) Auerbach / CRC Press, 2004
4. Computer Security Handbook, 4th Edition. Seymour Bosworth, M E Kabay (Editors). John Wiley, 2002.
5. ISO Standards in information security. http://www.27000.org/ Last accessed April 2, 2010.
6. J M Seigneur. Trust, Security and Privacy in Global Computing. Ph.D. Thesis, University of Dublin, 2005. Accessed online www.tara.tcd.ie/bitstream/2262/699/1/TCD-CS-2006-02.pdf April 2, 2010.

CS 6284: Security Policies and Assurance

Prerequisite: Nil

L	T	P	C
3	0	0	3

Total Hours (42)

Module 1 (10 Hrs)
Security policies, policy languages, confidentiality policies, Bell-LaPadula model, controversies over the model.
Module 2 (12 Hrs)
Integrity policies, Biba model, Lipner's model, Clark-Wilson models, Chinese wall model, clinical information systems security policy, noninterference and policy composition.
Module 3 (10 Hrs)
Assurance and trust, building secure and trusted systems, waterfall model, other models of development.
Module 4 (10 Hrs)
Assurance in requirements definition and analysis, assurance during system and software design, assurance during implementation and integration.

References

1. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.
2. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004.
3. C. P. Fleeger and S. L. Fleeger, Security in Computing, 3/e, Pearson Education, 2003.

CS 6283: Computer Law and Ethics

Prerequisite: Nil

L	T	P	C
3	0	0	3

Total Hours (42)

Module 1 (10 Hrs)
Intellectual property rights, computer software copyrights, copyright in databases and electronic publishing, law of confidence, patent laws, trademarks, product designs, international law .

Module 2 (12 Hrs)
Computer contracts, liability for defective hardware and software, software contracts, web and hardware contracts, electronic contracts and torts, liabilities.

Module 3 (10 Hrs)
Computer crime, computer fraud, hacking, unauthorized modification of information, piracy, computer pornography and harassment.

Module 4 (10 Hrs)
Cyber laws in India, IT Act 2000, data subjects' rights, ethical issues in computer security, case studies.

References

1. D. Bainbridge, Introduction to Computer Law, 5/e, Pearson Education, 2004.
2. P. Duggal, Cyber law: the Indian Perspective, 2005.
3. C. P. Fleeger and S. L. Fleeger, Security in Computing, 3/e, Pearson Education, 2003.

CS 6214: Advanced Topics in Information Security

Prerequisite: Foundations of Information Security

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (12 hours)
Cryptography - Practical considerations on cryptographic algorithms - Performance and Robustness.Time complexity of DES and RSA. Attacks on DES and RSA. Public Key Cryptography Standard (PKCS). Linear cryptanalysis. Birthday attack on hash schemes. ECC and AES, Identity based encryption.

Module 2: (11 hours)
Network Security - DNS attacks and DNSSEC. Cross-site scripting XSS worm, SQL injection attacks. Intrusion Detection Systems (IDS). DDoS detection and prevention in a network, IP Traceback.

Module 3: (11 hours)
Security in current domains - Wireless LAN security - WEP details. wireless LAN vulnerabilities - frame spoofing. Cellphone security - GSM and UMTS security. Mobile malware - bluetooth security issues.

Module 4: (8 hours)
Security in current applications Cases from any two of the three topics: Online banking or Credit Card Payment Systems, Web Services Security, RFIDs.

References

1. Bernard Menezes, *Network security and Cryptography*, Cengage Learning India, 2010.
2. Dieter Gollmann. Computer Security, John Wiley and Sons Ltd., 2006.
3. Charles P Pfleeger, Shari Lawrence Pfleeger. Security in Computing, Education, 2005.
4. Furnell, Katsikas, Lopez, Patel. Securing Information and Communication Systems: Principles, Technologies and Applications,Artech House Inc., 2008.
5. H. Delfs and H. Knebl. Introduction to Cryptography: Principles and Applications, Springer-Verlag, 2002.
6. Goldwasser and Bellare. Lecture Notes on Cryptography. Available online from http://cseweb.ucsd.edu/~mihir/papers/gb.pdf . Last Accessed March 26, 2010.
7. Whitman and Mattord. Principles of Information Security, Cengage Learning, 2006.

CS 6285: Information Security Management

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (10 hours)
Information as an Asset – creation and maintenance. Information systems in organizations of a global setting – Building blocks and review of current status. Threats to information systems. Information Security Management (ISM) in organizations. Information Asset Management and Risk analysis.

Module 2: (10 hours)
Managing Physical and Environmental security. Perimeter security. Use of biometrics in this context. Access control models and Role based approaches for organizational hierarchy. Managing Network Security. Firewalls, VPNs and IDS. Digital certificates and CAs. Managing wireless network security.

Module 3: (10 hours)
Application Security. Business Applications – choice of security architecture for thirdparty software and turnkey software projects. Choosing the building blocks of information systems of the firm with security considerations – OS and databases, email and web servers.

Module 4: (12 hours)
Disaster recovery approaches business continuity. Security models and frameworks. Security standards and compliance needs in different business domains. IT Act and other legal requirements – relevance to organizations operating in the country.

References

1. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, John Wiley and Sons Ltd., 2009.
2. Tipton and Krause, Information Security Management Handbook, Fourth Edition, Auerbach, 2000.
3.Furnell, Katsikas, Lopez, Patel, Securing Information and Communication Systems: Principles, Technologies and Applications, Artech House Inc., 2008.
4. Whitman and Mattord. Management of Information Security, Cengage Learning, 2007.

CS 6286: Metrics for Information Security Assessment

Prerequisite: Nil

L	T	P	C
3	0	2	4

Total Hours (42+28)

Module 1: (15 hours)

Introduction to information security and the concept of information assurance. Need for measurement for assessment and improvement. Introduction to metrics – review of quality metrics. Attributes of good metrics. Types/classification of metrics - qualitative vs. quantitative. Performance metrics and financial metrics. Hybrid approaches. Operational, Incident and Compliance metrics.

Module 2: (8 hours)

Developing good metrics – Statistical modeling, Value at Risk, Factor Analysis of Information Risk, Probabilistic Risk Assessment.

Module 3: (10 hours)

Modeling approaches for security metrics: Graph theoretic models like attack trees and defense trees, Game theoretic models. Study of some existing information security metrics from Government-University initiatives and Industry initiatives.

Module 4: (9 hours)

Information security management metrics at various organizational levels. Operational, management and governance metrics. Tools and technologies for information security assessment.

References

1. W K Brotby, Information Security Management Metrics, CRC Press, 2009.
2. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, John Wiley and Sons Ltd., 2009.
3. Whitman and Mattord, Management of Information Security, Cengage Learning, 2007.

Additional materials include Online SOAR (state of the art) reports available from international agencies and ISO/IEC 27004:2009 standard.