M.TECH. COMPUTER SCIENCE AND ENGINEERING
(INFORMATION SECURITY)

(CBCS)

REGULATIONS, CURRICULUM AND SYLLABUS

(With effect from the Academic Year 2011 – 12)

PONDICHERRY UNIVERSITY
PUDUCHERRY – 605 014.

PONDICHERRY UNIVERSITY
PUDUCHERRY – 605 014.

REGULATIONS FOR POST GRADUATE (M.TECH.) PROGRAMMES IN THE DISCIPLINE OF

Computer Science and Engineering (CBCS)

(WITH EFFECT FROM JULY 2011)

M. Tech. **Computer Science and Engineering (Information Security)**

1.0 ELIGIBILITY

Candidates for admission to the first semester of four semester M.Tech. (Computer Science and Engineering – Information Security) should have passed B.E / B.Tech in Computer Science and Engineering / Information Technology/ Electronics and Communication Engineering/ Electrical and Electronics Engineering/ Electronics and Instrumentation Engineering / Bio informatics or MCA through regular course of study from an AICTE approved institution or an examination of any University or authority accepted by the Pondicherry University as equivalent thereto, with at least 55% marks in the degree examination or equivalent CGPA.

Note:

1. Candidates belonging to SC/ST who have a mere pass in the qualifying examination are eligible.
2. There is no age limit for M.Tech. programmes.

2.0 ADMISSION

The admission policy for various M.Tech. programmes shall be decided by the respective institutes offering M.Tech. programmes subject to conforming to the relevant regulations of the Pondicherry University.

3.0 STRUCTURE OF M.Tech. PROGRAMME

3.1 General

3.1.1. The M.Tech. Programmes are of semester pattern with 16 weeks of instruction in a semester.

3.1.2 The programme of instruction for each stream of specialization will consist of:

(i) Core courses (Compulsory)

(ii) Electives
(iii) Laboratory
(iv) Seminar
(v) Directed Study
(vi) Project work

3.1.3 The M.Tech. Programmes are of 4 semester duration.

3.1.4. Credits will be assigned to the courses based on the following general pattern:

(i) One credit for each lecture period
(ii) One credit for each tutorial period
(iii) Two credits for practical course
(iv) Two credits for seminar
(v) Twenty three credits for Project work divided into 9 credits for Phase-I and 14 credits for Phase – II

One teaching period shall be of 60 minutes duration including 10 minutes for discussion and movement.

3.1.5 Regulations, curriculum and syllabus of the M.Tech. programme shall have the approval of Board of Studies and other Boards/ Committees/ Councils, prescribed by the Pondicherry University. The curriculum should be so drawn up that the minimum number of credits and other requirements for the successful completion of the programme will be as given in Table – 1.

Table 1: Minimum credits and other requirements

Sl.No.	Description	Requirements
		M.Tech (Full-Time)
1	Number of semesters	4
2	Min. number of credits of the programme	72
3	Max. number of credits of the programme	75
4	Min. Cumulative Grade Point Average for pass	5

5	Min. successful credits needed for registering in the next semester	Sem. I: 10
		Sem. II: 25
		Sem. III: 40
6	Min. period of completion of programme (consecutive semesters)	4
7	Max. period of completion of programme (consecutive semesters)	8
8	Number of core and Elective courses	12
9	Seminar /Laboratory	1
10	Laboratory	1
11	Directed study	1
12	Project work (semesters)	2

3.1.6 A core course is a course that a student admitted to the M.Tech. programme must successfully complete to receive the degree. A student shall register for all the core courses listed in the curriculum. Core courses in a particular specialization are offered by the department concerned.

3.1.7 Elective courses are required to be chosen from the courses offered by the department(s) in that particular semester from among the approved courses. A core course of one department may be chosen as an elective by a student from other department.

3.1.8 Each student is required to make a seminar presentation on any chosen topic connected with the field of specialization. Preparation and presentation of a seminar is intended to investigate an in-depth review of literature, prepare a critical review and

develop confidence to present the material by the student. The seminar shall be evaluated by a Department Committee constituted for this purpose, based on a report submitted by the candidate and a viva-voce conducted at the end of the semester.

3.1.9 Project work is envisaged to train a student to analyze independently any problem posed to him/her. The work may be analytical, experimental, design or a combination of both. The student can undertake the project work in the department concerned or in an industry/research laboratory approved by the Chairperson/Vice-Chairperson. The project report is expected to exhibit clarity of thought and expression. The evaluation of project work will be a continuous internal assessment based on two reviews, an internal viva-voce and an external viva-voce examination.

3.1.10 Directed study is a theory course required to be credited by each student under the close supervision of a faculty member of the department. The title of the course and syllabus are to be formulated by the designated faculty member and approved by the vice-chairperson, taking into account the broad area in which the student proposes to pursue his/her project work.

3.1.11 A student who has acquired the minimum number of total credits for the award of Degree will not be permitted to register for more courses for the purpose of improving his /her cumulative grade point average (see Table 1).

3.1.12 The medium of instruction, examination, seminar, directed study and project work will be in English.

3.2 Grading

3.2.1 Based on the performance of each student in a semester, letter grades will be awarded to each course at the end of the semester. The letter grades, the corresponding grade point and the description will be as shown in Table – 2.

TABLE 2: Letter Grade and the Corresponding Grade Point

GRADE	POINTS	DESCRIPTION
S	10	EXCELLENT
A	9	VERY GOOD
B	8	GOOD
C	7	ABOVE AVERAGE
D	6	AVERAGE
E	5	SATISFACTORY
F	0	FAILURE
FA	-	FAILURE DUE TO LACK OF ATTENDANCE/ FAILURE BY ABSENCE

3.2.2 A student is deemed to have completed a course successfully and earned the appropriate credit if and only if, he /she receive a grade of E and above. The student should obtain 40% of marks in end-semester examination in a subject to earn a successful grade. A subject successfully completed cannot be repeated at any time.

3.2.3 The letter grades do not correspond to any fixed absolute mark. Each student is awarded a grade depending on his/her performance in relation to the performance of other students taking or has taken the course. For example, S does not mean he/ she has secured 100% or 95%, but, rather that he /she is in the top 5% of all the students who have taken / are taking the course, in the judgement of the teachers. Grades shall be awarded based on the absolute marks in a meeting of the M.Tech Programme Committee to be held not later than 10 days after the last day of semester examination. Normally, not more than 5% of the students in any written/ laboratory course shall be awarded the grade S and not more than one–third awarded A grade. Average marks in the class shall normally be C grade excepting in the case of practical /project where it may be B grade.

4.0 REGISTRATION

4.1 Each student, on admission, shall be assigned a Faculty Advisor, who shall advise the student about the academic programme and counsel him/her on the choice of courses depending on his/her academic background and objective.

4.2 With the advice and consent of the Faculty Advisor, the student shall register for courses he/ she plans to take for the semester before the commencement of classes. No student shall be permitted to register for courses exceeding 30 contact hours per week nor shall any student be permitted to register for any course without satisfactorily completing the prerequisites for the course, except with the permission of the teacher concerned in the prescribed format.

4.3 If the student feels that he/she has registered for more courses than he/she can handle, he/she shall have the option of dropping one or more of the courses he/she has registered for, with the consent of his/her Faculty Advisor, before the end of 3rd week of the semester. However, a student to retain his/her status should register for a minimum of 10 credits per semester.

4.4 Students, other than newly admitted, shall register for the courses of their choice in the preceding semester by filling in the prescribed forms.

4.5 The college shall prescribe the maximum number of students in each course taking into account the physical facilities available.

4.6 The college shall make available to all students a bulletin, listing all the courses offered in every semester specifying the credits, the prerequisites, a brief description or list of topics the course intends to cover, the faculty offering the course, the time and place of the classes for the course.

4.7 In any department, preference shall be given to those students for whom the course is a core-course, if, the demand for registration is beyond the maximum permitted number of students.

4.8 Normally, no course shall be offered unless a minimum of 3 students are registered.

5.0 EVALUATION

5.1 Evaluation of theory courses shall be based on 40% continuous internal assessment and 60% end-semester examination. Evaluation of laboratory course shall be based on 50% internal assessment and 50% end-semester examination. In each course, there shall be a 3 hour end-semester examination.

5.2 The seminar will be evaluated internally for 100 marks. The total marks for the project work will be 300 marks for phase-I and 400 marks for phase-II. The allotment of marks for external valuation and internal valuation shall be as detailed below:

Seminar (Internal valuation only):100 Marks

First review		30 marks
Second review		30 marks
Report and Viva voce		40 marks
	Total	**100 marks**

Project work – (Phase – I): 300 Marks

Internal valuation			
	Guide		50 marks
	First Evaluation		50 marks
	Second Evaluation		50 marks
		Total	**150 marks**
External valuation			
	Evaluation (External Examiner Only)		50 marks
	Viva voce (50 for Ext. + 50 for Int.)		100 marks
		Total	**150 marks**

Project work – (Phase – II): 400 Marks

Internal valuation			
	Guide		100 marks
	First Evaluation		50 marks
	Second Evaluation		50 marks
		Total	**200 marks**
External valuation			
	Evaluation (External Examiner Only)		50 marks
	Viva voce (75 for Ext. + 75 for Int.)		150 marks
		Total	**200 marks**

Internal valuation should be done by a committee comprising of not less than 3 faculty members appointed by the Vice-Chairperson.

5.3 The directed study shall be evaluated internally and continuously as detailed below:

Test I	: 15 Marks
Test II	: 15 Marks
Assignment	: 10 Marks
Final test covering the whole syllabus	: 60 Marks
Total	: 100 Marks

5.4 The end-semester examination shall be conducted by the department for all the courses offered by the department. Each teacher shall, in the 4th week of the semester, submit to the Vice-Chairperson, a model question paper for the end-semester examination. The end-semester paper shall cover the entire course.

5.5 The department shall invite 2 or 3 external experts for evaluating the end-semester examinations and grading. Each expert will be asked to set the question paper(s) for the course(s) he/she is competent to examine for the end-semester examination based on the model question paper submitted by the teacher concerned. The teacher and the expert concerned shall evaluate the answer scripts together and award the marks to the student. If, for any reason, no external expert is available for any paper, then, the teacher concerned shall set the question paper(s) for the end-semester examination, and the teacher himself/herself shall evaluate the papers and award the marks.

5.6 In the department, after the evaluation of the end-semester examination papers, all the teachers who handled the courses and the external experts together shall meet with the M.Tech. Programme Committee (see 7.0) and decide the cut-offs for grades in each of the courses and award the final grades to the students.

5.7 Continuous internal assessment mark of 40 for a theory course shall be based on two tests (15 marks each) and one assignment (10 marks). A laboratory course carries an internal assessment mark of 50 distributed as follows: (i) Regular laboratory exercises and records – 20 marks (ii) Internal laboratory test – 20 marks and (iii) Internal viva-voce – 10 marks.

5.8 Every student shall have the right to scrutinize his/her answer scripts, assignments etc. and seek clarifications from the teacher regarding his/her evaluation of the scripts immediately after or within 3 days of receiving the evaluated scripts.

5.9 The department shall send all records of evaluation, including internal assessment for safe-keeping, to the college administration, as soon as all the formalities are completed.

5.10 At the end of the semester, each student shall be assigned a grade based on his/ her performance in each subject, in relation to the performance of other students.

5.11 A student securing F grade in a core course must repeat that course in order to obtain the Degree. A student securing F grade in an elective course may be permitted to choose another elective against the failed elective course, as the case may be, in consultation with the Faculty Adviser.

5.12 A student shall not be permitted to repeat any course(s) only for the purpose of improving the grade in a particular course or the cumulative grade point average (CGPA).

5.13 In exceptional cases, with the approval of the Chairperson, PG Programme committee, make–up examination(s) can be conducted to a student who misses end-semester examination(s) due to extreme medical emergency, certified by the college Medical Officer, or due to time-table clash in the end-semester examination between two courses he/she has registered for, in that semester.

5.14 All eligible students shall appear for end-semester examinations.

5.15 No student who has less than 75% attendance in any course will be permitted to attend the end-semester examinations. However, a student who has put in 60-75% attendance in any course and has absented on medical grounds will have to pay a condonation fee of Rs.200/- for each course and produce a medical certificate from a Government Medical Officer not below the rank of R.M.O. or officer of equal grade to become eligible to appear for the examinations. A student with less than 60% attendance shall be given the grade of FA. He/ She shall have to repeat that course if it is a core course, when it is offered the next time.

6.0 SUMMER TERM COURSE

6.1 A summer term course (STC) may be offered by the department concerned on the recommendations of M.Tech. Programme Committee. A summer term course is open only to those students who had registered for the course earlier and failed. No student

should register for more than two courses during a summer term. Those students who could not appear for examination due to lack of attendance will not be allowed to register for the same course offered in summer, unless, certified by the Vice-Chairperson concerned and the Principal.

6.2 Summer term course will be announced at the end of even semester. A student has to register within the stipulated time by paying the prescribed fees.

6.3 The number of contact hours per week for any summer term course will be twice that of a regular semester course. The assessment procedure in a summer term course will be similar to the procedure for a regular semester course.

6.4 Withdrawal from a summer term course is not permitted.

7.0 M.Tech. PROGRAMME COMMITTEE

7.1 Every M.Tech. Programme shall be monitored by a committee constituted for this purpose by the college. Each committee shall consist of all teachers offering the courses for the programme and two student members or 10% of students enrolled whichever is less. The HOD or a senior faculty in the rank of a Professor shall be the Vice-Chairperson, nominated by the Head of the Institution. There shall be a common Chairperson in the Rank of Professor nominated by the Head of the Institution for all the P.G. programmes offered by the institute. There can be a common coordinator in the rank of Professor nominated by the Head of the Institution.

7.2 It shall be the duty and responsibility of the committee to review periodically the progress of the courses in the programme, discuss the problems concerning the curriculum and syllabi and conduct of classes. The committee may frame relevant rules for the conduct of evaluation.

7.3 The committee shall have the right to make suggestions to individual teachers on the assessment procedure to be followed for his/her course. It shall be open to the

committee to bring to the notice of the Head of the Institution any difficulty encountered in the conduct of the classes or any other pertinent matter.

7.4 The committee shall meet at least twice a semester – first at the beginning of the semester, and second at the end of the semester. In the second meeting, the committee excluding student members but with the external experts invited by the Chairperson PG Programme Committee, shall finalize the grades of the students.

8.0 MINIMUM REQUIREMENTS

8.1 To be eligible towards continuing the Programme, a student must have earned a certain number of successful credits at the end of each semester as given in Table – 1. If he /she fails to satisfy this criterion in any semester, he/she shall be placed on scholastic probation in the succeeding semester. If he/she fails to earn the number of credits by the end of that year (including courses taken in summer), then, he/she shall be asked to discontinue the Programme.

8.2 Students are expected to abide by all the rules of the college and maintain a decorous conduct. Any deviation will be referred to the Head of the Institution for suitable action.

8.3 No student who has any outstanding dues to the college, hostel, library or laboratory or against whom any disciplinary action is contemplated/ pending, will be eligible to receive his/her degree.

9.0 DECLARATION OF RESULTS,RANK AND ISSUE OF GRADE CARD

9.1 The PG Programme (CBCS) office shall display the grades as soon as possible after the finalization of the grades. The student shall have the right, for a look at the evaluated examination scripts and represent to the M.Tech. Programme Committee for review if he/she feels aggrieved by the evaluation within a week from the commencement of succeeding semester classes.

9.2 The College shall issue at the beginning of each semester a grade card to the student, containing the grades obtained by the student in the previous semester (s) and his/her Grade Point Average (GPA) and his/her Cumulative Grade Point Average (CGPA).

9.3 The grade card shall list:

a) Title of the course(s) taken by the student.
b) Credits associated with each course.
c) Grade secured by the student.
d) Total credits earned by the student in that semester.
e) GPA of the student.
f) Total credits earned by the student till that semester and
g) CGPA of the student.

9.4 The GPA shall be calculated as the weighted average of the Grade Points weighted by the credit of the course as follows:

The product of the credit assigned to each course and the grade point associated with the grade obtained in the course is totaled over all the courses and the total is divided by the sum of credits of all the courses and rounded off to two decimal places.

For example, a student securing grade A in a 4 credit course, grade B in a 2 credit course, grade S in a 3 credit course and grade F in a 3 credit course, will have a GPA as:

(9 x 4 + 8 x 2 + 10 x 3 + 0 x 3)/ (4+2+3+3) =82 /12=6.83/10.0

The sum will cover all the courses the student has taken in that semester, including those in which he/she has secured grade F. Grades FA are to be excluded for calculating GPA and CGPA.

9.5 For computing CGPA, the procedure described in 9.4 is followed, except, that the sum is taken over all the courses the student has studied in all the semesters till then. If

a student has repeated any course, the grade secured by him/her in the successful attempt only will be taken into account for calculating CGPA.

9.6 To convert CGPA into percentage marks, the following formula shall be used:

$$\% \text{ Mark} = (\text{CGPA} - 0.5) \times 10$$

9.7 A candidate who satisfies the course requirements for all semesters and passes all the examinations prescribed for all the four semesters within a maximum period of 10 semesters reckoned from the commencement of the first semester to which the candidate was admitted shall be declared to have qualified for the award of degree.

9.8 A candidate who qualifies for the award of the degree shall be declared to have passed the examination in **FIRST CLASS** with **DISTINCTION** upon fulfilling the following requirements:

(i) Should have passed all the subjects pertaining to semesters 1 to 4 in his/her first appearance in 4 consecutive semesters starting from first semester to which the candidate was admitted.

(ii) Should not have been prevented from writing examinations due to lack of attendance

(iii) Should have secured a CGPA of 8.50 and above for the semesters 1 to 4.

9.9 A candidate who qualifies for the award of the degree by passing all the subjects relating to semesters 1 to 4 within a maximum period of 6 consecutive semesters after his/her commencement of study in the first semester and in addition secures CGPA not less than 6.5 shall be declared to have passed the examination in **FIRST CLASS**.

9.10 All other candidates who qualify for the award of degree shall be declared to have passed the examination in **SECOND CLASS**.

9.11 A student with CGPA less than 5.0 is not eligible for the award of degree.

9.12 For the award of University rank and gold medal, the CGPA secured from 1st to 4th semester should be considered and it is mandatory that the candidate should have passed all the subjects from 1st to 4th semester in the first appearance and he/she should

not have been prevented from writing the examination due to lack of attendance and should not have withdrawn from writing the end-semester examinations.

10.0 PROVISION FOR WITHDRAWAL

A candidate may, for valid reasons, and on the recommendation of the vice-chairperson and chairperson be granted permission by the Head of the Institution to withdraw from writing the entire semester examination as one unit. The withdrawal application shall be valid only if it is made earlier than the commencement of the last theory examination pertaining to that semester. Withdrawal shall be permitted only once during the entire programme. Other conditions being satisfactory, candidates who withdraw are also eligible to be awarded DISTINCTION whereas they are not eligible to be awarded a rank/ gold medal.

11.0 TEMPORARY DISCONTINUATION FROM THE PROGRAMME

If a candidate wishes to temporarily discontinue the programme for valid reasons, he/she shall apply to the Chairperson, PG Programme committee, through the Head of the department in advance and secure a written permission to that effect. A candidate after temporary discontinuance may rejoin the programme only at the commencement of the semester at which he/she discontinued, provided he/she pays the prescribed fees. The total period of completion of the programme reckoned from the commencement of the first semester to which the candidate was admitted shall not in any case exceed 8 consecutive semesters including the period of discontinuance.

12.0 POWER TO MODIFY

12.1 Notwithstanding anything contained in the foregoing, the Pondicherry University shall have the power to issue directions/ orders to remove any difficulty.

12.2 Nothing in the foregoing may be construed as limiting the power of the Pondicherry University to amend, modify or repeal any or all of the above.

****

M.TECH COMPUTER SCIENCE AND ENGINEERING

(Information Security)

CURRICULUM AND SCHEME OF EXAMINATION

(Total number of credits required for the completion of the programme: 72)

SEMESTER – I

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.		CORE – I	3	1	0	4	40	60	100
2.		CORE – II	3	1	0	4	40	60	100
3.		CORE – III	3	1	0	4	40	60	100
4.		Elective – I	3	0	0	3	40	60	100
5.		Elective – II	3	0	0	3	40	60	100
6.		Elective – III	3	0	0	3	40	60	100
7.	CS 991	Seminar / Laboratory – I	-	-	3	2	100	-	100
						23	340	360	700

SEMESTER – II

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.		CORE – IV	3	1	0	4	40	60	100
2.		CORE - V	3	1	0	4	40	60	100
3.		CORE – VI	3	1	0	4	40	60	100
4.		Elective – IV	3	0	0	3	40	60	100
5.		Elective –V	3	0	0	3	40	60	100

6.		Elective – VI	3	0	0	3	40	60	100
7.	CS 992	Laboratory - II	-	-	3	2	50	50	100
						23	290	410	700

SEMESTER – III

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.	CS 993	Project Phase-I	-	-	16	9	150	150	300
2.	CS 994	Directed Study	-	-	3	3	100	-	100
						12	250	150	400

SEMESTER – IV

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.	CS 995	Project Phase II	-	-	24	14	200	200	400
						14	200	200	400

LIST OF CORE SUBJECTS:

CS 951 MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

CS 952 ADVANCED DATA STRUCTURES AND ALGORITHMS

CS 953 INTERNALS OF OPERATING SYSTEMS

CS 954 NETWORK SECURITY

CS 955 CYBER LAW AND SECURITY POLICIES

CS 956 COMPUTER SECURITY, AUDIT ASSURANCE AND RISK MANAGEMENT

LIST OF ELECTIVE SUBJECTS:

CS961	**ADVANCED DATABASE TECHNOLOGY**
CS962	**AGENT TECHNOLOGY**
CS963	**BIOMETRIC SECURITY**
CS964	**INFORMATION THEORY AND CODING**
CS965	**APPLIED CRYPTOGRAPHY**
CS966	**DEPENDABLE DISTRIBUTED SYSTEMS**
CS967	**DESIGN OF EMBEDDED SYSTEMS**
CS968	**FUNDAMENTALS OF FINANCIAL MANAGEMENT**
CS969	**ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM**
CS970	**INFORMATION SECURITY POLICIES IN INDUSTRIES**
CS971	**MOBILE WIRELESS SECURITY**
CS972	**SECURITY ASSESSMENT AND VERIFICATION**
CS973	**SECURE SOFTWARE ENGINEERING**
CS974	**SECURED NETWORK PROTOCOLS**
CS975	**SECURITY THREATS**
CS976	**STEGANOGRAPHY AND DIGITAL WATERMARKING**
CS977	**TRUST MANAGEMENT IN E-COMMERCE**
CS978	**BANKING TECHNOLOGY MANAGEMENT**
CS979	**GAME THEORY**
CS980	**DESIGN OF SECURED ARCHITECTURES**
CS981	**MULTICORE ARCHITECTURE AND PARALLEL ALGORITHMS**
CS982	**ETHICAL HACKING**
CS983	**OBJECT ORIENTED SOFTWARE ENGINEERING**
CS984	**DISTRIBUTED SYSTEMS SECURITY**

CS951-MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

UNIT I

Topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences: Definitions and properties – linear congruences, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol.

UNIT II

Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.

UNIT III

Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption - Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.

UNIT IV

Primality and Factoring: Pseudoprimes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the quadratic seieve method.

UNIT V

Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization.

Note: Theorem Proofs are excluded for examination but the statements of the theorems and solving problems are included.

REFERENCES

1. Neal Koblitz, "A Course in Number Theory and Cryptography", 2nd Edition, Springer, 2002.
2. Johannes A. Buchman, "Introduction to Cryptography", 2nd Edition, Springer, 2004.
3. Serge Vaudenay, "Classical Introduction to Cryptography – Applications for Communication Security", Springer, 2006.
4. Victor Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005.
5. A. Manezes, P. Van Oorschot and S. Vanstone, "Hand Book of Applied Cryptography", CRC Press, 1996.
6. S.C. Coutinho, "The Mathematics of Ciphers – Number Theory and RSA Cryptography", A.K. Peters, Natick, Massachusetts, 1998.

CS952 ADVANCED DATA STRUCTURES AND ALGORITHMS

UNIT I

Mathematical Induction - Asymptotic Notations – Algorithm Analysis - NP-Hard and NP-Completeness – Recurrence Equations – Solving Recurrence Equations – Memory Representation of Multi-dimensional Arrays – Time-Space Tradeoff.

UNIT II

Heapsort – Quicksort – Topological sort - Sorting in Linear Time – Elementary Data Structures – Hash Tables – Binary Search Trees – AVL Trees – Red-Black trees – Multi-way Search Trees – B-Trees- Fibonacci Heaps – van Emde Boas Trees – Data Structures for Disjoint Sets.

UNIT III

Algorithm Design Techniques: Divide-and-Conquer – Greedy – Dynamic Programming – Amortized Analysis - Backtracking – Branch-and-Bound techniques.

UNIT IV

Elementary graph Algorithms – Minimum Spanning Trees – Single-Source Shortest Paths- All-Pairs Shortest Paths – Maximum Flow - Multithreaded Algorithms – Matrix Operations.

UNIT V

Linear programming – Polynomials and FFT – Number-Theoretic Algorithms – Computational Geometry –NP-Completeness – Approximation Algorithms.

REFERENCES

1. Thomas H. Coreman, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, “Introduction to Algorithms”, PHI, 3rd Edition, 2010.
2. G. Brassard and P. Bratley, “Algorithmics: Theory and Practice”, Printice –Hall, 1997.
3. E. Horowitz, S.Sahni and Dinesh Mehta, “Fundamentals of Data structures in C++”, Uiversity Press, 2007.
4. E. Horowitz, S. Sahni and S. Rajasekaran, “Computer Algorithms/C++”, 2nd Edition, University Press, 2007.
5. Alfred V. Aho, Jeffrey D. Ullman, John E. Hopcroft, “Data Structures and Algorithms”, Addison Wesley.

CS953 - INTERNALS OF OPERATING SYSTEMS

UNIT I

Introduction to Kernel - Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. Files INODES, Structure of a regular file, Directories, Super block, Inode assignment.

UNIT II

System calls - OPEN, Read, Close, Write, Create, CHMOD, CHOWN, Pipes, Mounting and Unmounting. Process - Layout the system memory, Context, Process control, process creation, signals, Process scheduling, time, clock.

UNIT III

Inter-Process Communications - Process tracing, System V IPC, Shared Memory, Semaphores. Network Communications - Socket programming: Sockets, descriptors, Connections, Socket elements, Stream and Datagram Sockets.

UNIT IV

Windows Operating system - versions, Concepts and tools, Windows internals, System Architecture, Requirements and design goals, Operating system model, Architecture overview, Key system components. System mechanisms - Trap dispatching, object manager, Synchronization, System worker threads, Windows global flags, Local procedural calls, Kernel event tracing.

UNIT V

Windows Management Mechanisms - The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.

REFERENCES

1. Maurice J. Bach, “The Design of the Unix Operating System”, Prentice Hall of India, 1991.

2. Mark E. Russinovich and David A. Solomon, “Microsoft® Windows® Internals”, 4th Edition, Microsoft Press, 2004.

3. William Stallings, “Operating Systems: Internals and Design Principles”, 5th Edition, Prentice Hall, 2005.

CS954 - NETWORK SECURITY

UNIT I

Introduction to Security in Networks – Characteristics of Networks – Intrusion – Kinds of security breaches – Plan of attack - Points of vulnerability – Methods of defense – Control measures – Effectiveness of controls

UNIT II

Basic encryption and decryption – Encryption techniques – Characteristics of good encryption systems – Secret key cryptography – Data Encryption Standard – International Data Encryption Algorithm – Advanced Encryption Standard – Hash and MAC algorithms

UNIT III

Public Key encryptions – Introduction to number theory - RSA algorithm – Diffie-Hellman – Digital Signature standard – Elliptic Curve cryptography - Digital signatures and authentication – Trusted intermediaries – Security handshake pitfalls

UNIT IV

Secure sockets – IPsec overview – IP security architecture – IPsec-Internet Key Exchanging(IKE) – IKE phases – encoding – Internet security – Threats to privacy – Packet sniffing – Spoofing - Web security requirements – Real Time communication security – Security standards–Kerberos.X.509AuthenticationService.

UNIT V

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles – Trusted systems – Electronic payment protocols. Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

REFERENCES

1. William Stallings, “Cryptography and Network Security: Principles and Standards”, Prentice Hall India, 3rd Edition, 2003.

2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Prentice Hall India, 2nd Edition, 2002.

3. Charles P. Pleeger, “Security in Computing”, Pearson Education Asia, 5th Edition, 2001.

4. William Stallings, “Network Security Essentials: Applications and standards”, Person Education Asia, 2000.

CS955 - CYBER LAW AND SECURITY POLICIES

UNIT I

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT II

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

UNIT III

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT IV

Information security: fundamentals-Employee responsibilities- information classification-Information handling- Tools of information security- Information processing-secure program administration.

UNIT V

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

REFERENCES

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997.

CS956 - COMPUTER SECURITY, AUDIT ASSURANCE AND RISK MANAGEMENT

UNIT I

Essentials of computer security - Sources of security threats – Intruders, Viruses, Worms and related threats - Threat identification - Threat analysis - Vulnerability identification and Assessment - Components of Computer Security - Physical security – System access control - Goals of Security - Efforts to secure computer networks – Ethical issues in Computer Security- Operational issues, Human issues.

UNIT II

Cryptography - Public Key Cryptography – Principles of Public Key Cryptosystems – The RSA Algorithm – Key Management – Authentication – Elements, types and methods – Digital Signature – Intrusion Detection System (IDS) – Types and challenges – Intrusion prevention system (IPS) – Firewalls - Design Principles, Scanning, filtering and blocking.

UNIT III

Vulnerabilities – Sources of vulnerabilities, Vulnerability identification and Assessment, Cyber crime and Hackers, Viruses and content filtering - Security Assessment, Analysis and Assurance – Computer network security protocol and standards - Security Policies – Integrity policies – confidentiality policies - Security models - Access Control Matrix Model, Take-Grant Protection Model.

UNIT – IV

Security Monitoring and Auditing - Assurance and Trust, Need for Assurance, Role of Requirements in Assurance, Audit Assurance in Software Development Phases, Building Secure and Trusted Systems - Designing an Auditing System, Implementation Considerations, Auditing to Detect Violations of a security Policy, Auditing Mechanisms, Audit Browsing.

UNIT-V

Risk management and security planning – Risk management Process Overview- Cost-Benefit Analysis, Risk Analysis, Laws and Customs, Human Issues, Organizational issues - Information system Risk analysis – System approach to risk management, Threat assessment, Assets and safeguards, modes of risk analysis – Effective risk analysis, Qualitative Risk analysis, Value analysis

REFERENCES

1. Matt Bishop, “Computer Security: Art and Science”, Addison-Wesley Professional, 2003.
2. Joseph M.Kizza, “Computer Network security”, Springer, 2005
3. Matt Bishop, “Introduction to Computer Security”, Addison-Wesley Professional, 2005.
4. Thomas R.Peltier, “Information Security Risk Analysis”, CRC Press, 2001.
5. C.A.Roper, “Risk management for Security professional”, Elsevier, 1999.

CS961 - ADVANCED DATABASE TECHNOLOGY

UNIT I

Relational Data Model – SQL - Database Design - Entity-Relationship Model – Relational Normalization – Embedded SQL – Dynamic SQL – JDBC – ODBC. Case Studies

UNIT II

Object Databases - Conceptual Object Data Model – XML and Web Data – XML Schema – Distributed Data bases – OLAP and Data Mining – ROLAP and MOLAP. Case Studies

UNIT III

Processing Basics – Heuristic Optimization – Cost, Size Estimation - Models of Transactions – Architecture – Transaction Processing in a Centralized and Distributed System – TP Monitor. Case Studies for Real time Systems

UNIT IV

Schedules – Concurrency Control – Objects and Semantic – Locking – Crash, Abort and Media Failure – Recovery – Atomic Termination – Distributed Deadlock – Global Serialization – Replicated Databases – Distributed Transactions in Real World. Case Studies

UNIT V

Security – Encryption – Digital Signatures – Authorization – Authenticated RPC - Integrity - Consistency - Database Tuning - Optimization and Research Issues. Case Studies

REFERENCES:

1. Philip M. Lewis, Arthur Bernstein and Michael Kifer, “Databases and Transaction Processing: An Application-Oriented Approach”, Addison-Wesley, 2002.
2. R. Elmasri and S.B. Navathe, “Fundamentals of Database Systems”, 3rd Edition, Addison Wesley, 2004.
3. Abraham Silberschatz, Henry. F. Korth and S.Sudharsan, “Database System Concepts”, 4th Edition, Tata McGraw Hill, 2004.
4. Raghu Ramakrishnan and Johannes Gehrke, “Database Management Systems”, 3rd Edition, TMH, 2003.

CS962 - AGENT TECHNOLOGY

UNIT I

Agent Definition - History - Intelligent Agents - Agent Programming Paradigms – Agent Vs Object - Aglet - Mobile Agents – Agent Frameworks - Agent Reasoning.

UNIT II

Interaction between Agents - Reactive Agents - Cognitive Agents – Interaction protocols - Agent coordination -Agent negotiation - Agent Cooperation – Agent Organization - Self - interested agents in electronic commerce applications.

UNIT III

Agents and Multi-agent Systems- Problem Solving and Knowledge Representation - Reasoning Systems and Learning Systems- Agent Oriented Methodologies and Frameworks- Agent Interoperability- Logics for Multiagent Systems – Interface Agents - Agent Communication Languages - Agent Knowledge representation - Agent adaptability - Belief Desire Intension - Mobile Agent Applications.

UNIT IV

Situational Calculus - Representation of Planning - Partial order Planning - Practical Planning – Conditional Planning – Replanning Agents - Distributed Problem Solving and Task Sharing - Result Sharing - Distributed Planning - Distributed Plan Representations -Distributed Planning and Execution - Search Algorithms for Agents - Constraint satisfaction - Path finding - problem Two player games.

UNIT V

Agent Security Issues - Mobile Agents Security - Protecting Agents against Malicious Hosts - Untrusted Agent -Black Box Security - Authentication for agents - Security issues for aglets- Agent oriented analysis and design, Gaia methodology, MASE, OPEN process framework, Tropos, Agent UML.

REFERENCES :

1. Bradshaw, "Software Agents", MIT Press, 2000.
2. Russel & Norvig, "Artificial Intelligence: a modern approach", Prentice Hall, 1994.
3. Richard Murch and Tony Johnson, "Intelligent Software Agents", Prentice Hall, 2000.
4. Gerhard Weiss, "Multi-agent systems A modern approach to Distributed Artificial Intelligence", MIT press, 1999.
5. Michael Wooldridge, "Introduction to Multi-agent systems", John Wiley & Sons, 2001.
6. Vijayan Sugumaran, "Distributed Artificial Intelligence, Agent Technology, and Collaborative Applications (Advances in Intelligent Information Technologies), Information Science Reference"; 1st Edition, 2008.
7. Nicholas R. Jennings and Michael Woodridge, "Agent Technology: Foundations, Applications and markets", Springer Verlag Publishing, 1998.

CS963 - BIOMETRIC SECURITY

UNIT I

Biometrics- Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

UNIT II

Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern - Technical description – characteristics - strengths – weaknesses –deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics.

UNIT III

Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - signature and handwriting technology - Technical description – classification - keyboard / keystroke dynamics - Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

UNIT IV

Multi biometrics: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan.

UNIT V

Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

REFERENCES

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002.

2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2005.

3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004.

CS964 - INFORMATION THEORY AND CODING

UNIT I

Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

UNIT II

Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

UNIT III

Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

UNIT IV

Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding.

UNIT V

Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

REFERENCES :

1. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.

2. Viterbi, "Information theory and coding", McGraw Hill, 1982.

3. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

CS965 – APPLIED CRYPTOGRAPHY

UNIT I

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols

UNIT II

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public-Key Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

UNIT III

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer - Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

UNIT IV

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - One-Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes

UNIT V

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ong-chnorr-Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

REFERENCES

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.
4. William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson Education, 2003.

CS966 - DEPENDABLE DISTRIBUTED SYSTEMS

UNIT I

Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification - Fault-detection and location - Fault containment - Byzantine failures - Fault injection - Fault-tolerant techniques - Performability metrics.

UNIT II

Fault-tolerance in real-time systems - Space-time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block - Imprecise computation; (m,k)- deadline model) - Adaptive fault-tolerance - Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model – Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives.

UNIT III

Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem.

UNIT IV

Banking and bookkeeping – Introduction – How computers systems works – Wholesale payment system – Automatic teller Machine – Monitoring systems – Introduction – Prepayment meters – Taximeters, Tachographs and trunk speed limits. Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology.

UNIT V

Bio metrics – Introduction – Handwritten signature – face recognition – fingerprints – Iris codes – Voice recognition. Emission Security – Introduction – Technical Surveillance and countermeasures – Passive Attacks – Active Attacks. Electronic and Information warfare – Introduction – Basics – Communication system – Surveillance and target acquisition – IFF system – Directed Energy Weapon – Information Warefare. Telecom Security – Introduction – Phone Breaking – Mobile phones – Network attack and defense - Protecting E-commerce systems- E – policy – Management issues – systems evaluation and assurance.

REFERENCES

1. Ross J Anderson and Ross Anderson, “Security Engineering: A guide to building dependable distributed systems”, Wiley, 2001.
2. David Powell, “A generic fault-Tolerant architecture for Real-Time Dependable Systems”, Springer, 2001.
3. Hassan B Diab and Albert Y. Zomaya, “Dependable computing systems: Paradigm, Performance issues and Applications”, Wiley series on Parallel and Distributed Computing, 2000.

CS967 DESIGN OF EMBEDDED SYSTEMS

UNIT - I

Embedded Computing - Challenges of Embedded Systems – Embedded system design process. Embedded processors – ARM processor – Architecture, ARM and Thumb Instruction sets

UNIT - II

Embedded C Programming - C-looping structures – Register allocation – Function calls – Pointer aliasing – structure arrangement – bit fields – unaligned data and endianness – inline functions and inline assembly – portability issues.

UNIT - III

Optimizing Assembly Code - Profiling and cycle counting – instruction scheduling – Register allocation – conditional execution – looping constructs – bit manipulation – efficient switches – optimized primitives.

UNIT - IV

Processes and Operating systems - Multiple tasks and processes – Context switching – Scheduling policies – Interprocess communication mechanisms – Exception and interrupt handling - Performance issues.

UNIT - V

Embedded System Development - Meeting real time constraints – Multi-state systems and function sequences. Embedded software development tools – Emulators and debuggers. Design methodologies – Case studies – Windows CE – Linux 2.6x and RTLinux – Coding and sending application layer byte stream on a TCP/IP network using RTOS Vxworks – Embedded system for a smart card.

REFERENCES

1. Andrew N Sloss, D. Symes, and C. Wright, “ARM System Developers Guide”, Morgan Kaufmann / Elsevier, 2006.
2. Michael J. Pont, “Embedded C”, Pearson Education, 2007.
3. Wayne Wolf, “Computers as Component: Principles of Embedded Computer System Design”, Morgan Kaufmann / Elsevier, 2nd Edition, 2008.
4. Steve Heath, “Embedded System Design”, Elsevier, 2nd Edition, 2003.
5. Raj Kamal, “Embedded Systems – Architecture, Programming and Design”, 2nd Edition, McGraw-Hill companies, 2008.

CS968 - FUNDAMENTALS OF FINANCIAL MANAGEMENT

UNIT I

Introduction to Financial Management - The Role of Financial Management - Business, Tax, and Financial Environments - Valuation - Time Value of Money - Valuation of Long-Term Securities - Risk and Return

UNIT II

Tools of Financial Analysis and Planning - Financial Statement Analysis - Funds Analysis, Cash-Flow Analysis, and Financial Planning - Working Capital Management - Overview of Working Capital Management - Cash and Marketable Securities Management - Accounts Receivable and Inventory Management - Short-Term Financing

UNIT III

Investment in Capital Assets - Capital Budgeting and Estimating Cash Flows - Capital Budgeting Techniques - Risk and Managerial Options in Capital Budgeting - The Cost of Capital, Capital Structure, and Dividend Policy - Required Returns and the Cost of Capital - Operating and Financial Leverage - Capital Structure Determination - Dividend Policy

UNIT IV

Intermediate and Long-Term Financing - The Capital Market - Long-Term Debt, preferred Stock, and Common Stock - Term Loans and Leases

UNIT V

Special Areas of Financial Management - Convertibles, Exchangeables, and Warrants - Mergers and Other Forms of Corporate Restructuring - International Financial Management

REFERENCES

1. James C. Van Horne and John M. Wachowicz, "Fundamentals of Financial Management", 11th Edition, ISBN: 81-203-2016-6.
2. Chandra, "Fundamentals of Financial Management", Tata McGraw Hill, 2008.
3. J.VanHorne and John Wachowicz, "Fundamentals of financial Management", Pearson, 2008.
4. Eugene F. Brigham and Joel F. Houston, "Fundamentals of Financial Management", South – western cengage learning, 2009.

CS969 ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM

UNIT I

Access control – Introduction - Attenuation of privileges – Trust and Assurance – Confinement problem - Security design principles– Identity Management models – local –Network - federal – global web identity – XNS approach for global Web identity - Centralized enterprise level Identity Management.

UNIT II

Elements of trust paradigms in computing – Third party approach to identity trust – Kerberos - Explicit third party authentication paradigm – PKI approach to trust establishment - Attribute certificates – Generalized web of trust models – Examples.

UNIT III

Mandatory access control - Comparing information flow in BLP and BIBA models – Combining the BLP and BIBA models – Chinese wall problem.

UNIT IV

Discretionary access control and Access matrix model – definitions – Safety problem – The take grant protection model – Schematic protection model – SPM rules and operations – Attenuating – Applications

UNIT V

Role based access control – Hierarchical Access Control - Mapping of a mandatory policy to RABC – Mapping discretionary control to RBAC – RBAC flow analysis – Separation of Duty in RBAC – RBAC consistency properties - The privileges perspective of separation of duties – Functional specification for RBAC .

REFERENCES

1. Messaoud Benantar, “Access Control Systems, Security, Identity Management and Trust Models“, Springer Publications, 2006.
2. Messoud Benantar, “Access Control Systems: Security, Identity Management and Trust Models”, Springer, 2009.
3. Elena Ferrari and M. Tamer A-zsu , “Access Control In Data Management Systems”, Morgan & Claypool Publishers, 2010.

CS970 - INFORMATION SECURITY POLICIES IN INDUSTRIES

UNIT I

Introduction to Information Security Policies – About Policies – why Policies are Important – When policies should be developed – How Policy should be developed - Policy needs – Identify what and from whom it is being protected – Data security consideration – Backups, Archival storage and disposal of data - Intellectual Property rights and Policies – Incident Response and Forensics - Management Responsibilities – Role of Information Security Department - Security Management and Law Enforcement – Security awareness training and support .

UNIT II

Policy Definitions – Standards – Guidelines - Procedures with examples - Policy Key elements - Policy format and Basic Policy Components - Policy content considerations - Program Policy Examples - Business Goal Vs Security Goals - Computer Security Objectives - Mission statement Format – Examples - Key roles in Organization - Business Objectives - Standards – International Standards.

UNIT III

Writing The Security Policies - Computer location and Facility construction - Contingency Planning - Periodic System and Network Configuration Audits - Authentication and Network Security – Addressing and Architecture – Access Control – Login Security – Passwords – User Interface – Telecommuting and Remote Access – Internet Security Policies – Administrative and User Responsibilities – WWW Policies – Application Responsibilities – E-mail Security Policies.

UNIT IV

Establishing Type of Viruses Protection - Rules for handling Third Party Software - User Involvement with Viruses - Legal Issues- Managing Encryption and Encrypted data - Key Generation considerations and Management - Software Development policies -Processes - Testing and Documentation- Revision control and Configuration management - Third Party Development - Intellectual Property Issues

UNIT V

Maintaining the Policies - Writing the AUP - User Login Responsibilities - Organization's responsibilities and Disclosures- Compliance and Enforcement – Testing and Effectiveness of Policies - Publishing and Notification Requirements of the Policies- Monitoring, Controls and Remedies - Administrator Responsibility - Login Considerations - Reporting of security Problems - Policy Review Process - The Review Committee-Sample Corporate Policies – Sample Security Policies

REFERENCES

1. Scott Barman, "Writing Information Security Policies", Sams Publishing, 2002.

2. Thomas.R.Peltier, "Information Policies, Procedures and Standards", CRC Press, 2004.

CS971 - MOBILE WIRELESS SECURITY

UNIT I

Wireless Fundamentals: Wireless Hardware- Wireless Network Protocols- Wireless Programming WEP Security. Wireless Cellular Technologies – concepts – Wireless reality – Security essentials – Information classification standards - Wireless Threats: Cracking WEP - Hacking Techniques- Wireless Attacks – Airborne Viruses.

UNIT II

Standards and Policy Solutions – Network Solutions – Software Solutions – Physical Hardware Security- Wireless Security – Securing WLAN – Virtual Private Networks – Intrusion Detection System – Wireless Public Key infrastructure. Tools – Auditing tools – Pocket PC hacking – wireless hack walkthrough.

UNIT III

Security Principles – Authentication – Access control and Authorization – Non-repudiation-privacy and Confidentiality – Integrity and Auditing –Security analysis process. Privacy in Wireless World – Legislation and Policy – Identify targets and roles analysis – Attacks and vulnerabilities – Analyze mitigations and protection.

UNIT IV

WLAN Configuration – IEEE 802.11 – Physical layer – media access frame format – systematic exploitation of 802.11b WLAN – WEP – WEP Decryption script – overview of WEP attack – Implementation - Analyses of WEP attacks.

UNIT V

Global Mobile Satellite Systems; case studies of the IRIDIUM and GLOBALSTAR systems. Wireless Enterprise Networks: Introduction to Virtual Networks, Blue tooth technology, Blue tooth Protocols. Server-side programming in Java, Pervasive web application architecture, Device independent example application

REFERENCES

1. Russel Dean Vines, “Wireless Security Essentials: Defending Mobile from Data Piracy”, John Wiley & Sons, 1st Edition, 2002.
2. Cyrus, Peikari and Seth Fogie, “Maximum Wireless Security”, SAMS Publishing 2002.
3. Yi-Bing Lin and Imrich Chlamtac, “Wireless and Mobile Networks Architectures”, John Wiley & Sons, 2001.
4. Raj Pandya, “Mobile and Personal Communication systems and services”, Prentice Hall of India, 2001.
5. Tara M. Swaminathan and Charles R. Eldon, “Wireless Security and Privacy- Best Practices and Design Techniques”, Addison Wesley, 2002.
6. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly Publications, 2002.
7. Burkhardt, “Pervasive Computing”, Pearson Education, India Edition, 2007.
8. J. Schiller, “Mobile Communication”, Pearson Education, India Edition, 2002.

CS972 SECURITY ASSESSMENT AND VERIFICATION

UNIT I

Evolution of information security, information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

UNIT II

Security assessment planning – Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan.
Initial information gathering – Initial preparation, analysis of gathered information.

UNIT III

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

UNIT IV

Security Risk assessment project management, Security risk assessment approaches and methods.

UNIT V

Information security standards, information security Legislation, formal security verification, security verification with SSL.

REFERENCES

1. Sudhanshu Kairab, "A practical guide to security assessments", CRC press, 2005.

2. Douglas J.Landoll, "A Security risk assessment Handbook", Auerbach publications, 2006.

CS973- SECURE SOFTWARE ENGINEERING

UNIT I

Problem, Process, and Product - Problems of software practitioners – approach through software reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability. Implementing Operational Profiles - Developing, identifying, crating, reviewing the operation – concurrence rate – occurrence probabilities- applying operation profiles

UNIT II

Engineering "Just Right" Reliability - Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives -Determining user needs for reliability and availability., overall reliability and availability objectives, common failure intensity objective., developed software failure intensity objectives. - Engineering software reliability strategies. Preparing for Test - Preparing test cases. - Planning number of new test cases for current release. -Allocating new test cases. - Distributing new test cases among new operations - Detailing test cases. - Preparing test procedures

UNIT III

Executing Test - Planning and allocating test time for the current release. - Invoking test-identifying identifying failures - Analyzing test output for deviations. – Determining which deviations are failures. Establishing when failures occurred. Guiding Test - Tracking reliability growth - Estimating failure intensity. - Using failure intensity patterns to guide test - Certifying reliability. Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders. - Executing the deployment - Using a consultant.

UNIT IV

Using UML for Security - UM L diagrams for security requirement -security business process-physical security - security critical interaction - security state. Analyzing Model - Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems - Applying security patterns

UNIT V

Applications - Secure channel - Developing Secure Java program- more case studies. Tool support for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC. Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties.

REFERENCES

1. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
2. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004 (Unit IV and V)

CS974 - SECURED NETWORK PROTOCOLS

UNIT I

OSI:ISO Layer Protocols:-Application Layer Protocols-TCP/IP, HTTP, SHTTP, LDAP, MIME,-POP& POP3-RMON-SNTP-SNMP. Presentation Layer Protocols-Light Weight Presentation Protocol Session layer protocols –RPC protocols-transport layer protocols-ITOT,RDP,RUDP,TALI,TCP/UDP, compressed TCP. Network layer Protocols – routing protocols-border gateway protocol-exterior gateway protocol-internet protocol IPv4- IPv6-Internet Message Control Protocol- IRDP- Transport Layer Security-TSL-SSL-DTLS

UNIT II

Data Link layer Protocol – ARP – InARP – IPCP – IPv6CP – RARP – SLIP .WideArea and Network Protocols- ATM protocols – Broadband Protocols – Point to Point Protocols – Other WAN Protocols- security issues.

UNIT III

Local Area Network and LAN Protocols – ETHERNET Protocols – VLAN protocols – Wireless LAN Protocols – Metropolitan Area Network Protocol – Storage Area Network and SAN Protocols -FDMA, WIFI and WIMAX Protocols- security issues. Mobile IP – Mobile Support Protocol for IPv4 and IPv6 – Resource Reservation Protocol. Multi-casting Protocol – VGMP – IGMP – MSDP.

UNIT IV

Network Security and Technologies and Protocols – AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security architecture for IP – IPSECAH – Authentication Header – ESP – IKE – ISAKMP and Key management Protocol. IEEE 802.11 - Structure of 802.11 MAC – WEP- Problems with WEP – Attacks and Risk- Station security – Access point Security – Gate way Security – Authentication and Encryption.

UNIT V

IEEE 802.15 and Bluetooth – WPAN Communication Protocols – IEEE 802.16- IEEE 802.16A.WCDMA – Services – WCDMA Products – Networks- device addressing – System Addressing – Radio Signaling Protocol – Multimedia Signaling Protocol.

REFERENCES

1. Jawin, “Networks Protocols Handbook”, Jawin Technologies Inc., 2005.
2. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly Publications, 2002.
3. Lawrence Harte, “Introduction to WCDMA”, Althos Publishing, 2004.
4. Ralph Oppliger “SSL and TSL: Theory and Practice”, Arttech House, 2009.
5. Lawrence Harte, “Introduction to CDMA- Network services Technologies and Operations”, Althos Publishing, 2004.
6. Lawrence Harte, “Introduction to WIMAX”, Althos Publishing, 2005.

CS 975 - SECURITY THREATS

UNIT I

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

UNIT II

Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots - IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

UNIT III

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools - Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

UNIT IV

Security Elements: Authorization and Authentication - types, policies and techniques - Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Polices and Procedures, Firewalls, IDS, Log Files, Honey Pots

UNIT V

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies.

REFERENCES

1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005

2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.

3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.

4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

CS976 - STEGANOGRAPHY AND DIGITAL WATERMARKING

UNIT I

Introduction to Information hiding – Brief history and applications of information hiding – Principles of Steganography – Frameworks for secret communication – Security of Steganography systems –Information hiding in noisy data – Adaptive versus non adaptive algorithms – Laplace filtering – Using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications.

UNIT II

Survey of steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and information hiding – Statistical Steganography - Distortion and code generation techniques – Automated generation of English text.

UNIT III

Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information – Watermarking techniques – History – Basic Principles – applications – Requirements of algorithmic design issues – Evaluation and benchmarking of watermarking system.

UNIT IV

Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems

UNIT V

Fingerprints – Examples – Classification – Research history – Schemes – Digital copyright and watermarking – Conflict of copyright laws on the internet.

REFERENCES

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.
2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
3. Steganography, Abbas Cheddad, Vdm Verlag and Dr. Muller, “Digital Image” Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, “Digital Watermarking And Steganography”, Morgan Kaufmann Publishers, Nov 2007.

CS977 - TRUST MANAGEMENT IN E-COMMERCE

UNIT I

Introduction to E-Commerce – Network and E-Commerce – Types of E-Commerce – E-Commerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models – E-Commerce Payment systems: Types of payment system – Credit card E-Commerce transactions – B2C E-Commerce Digital payment systems – B2B payment system.

UNIT II

Security and Encryption: E-Commerce Security Environment – Security threats in E-Commerce environment – Policies, Procedures and Laws.

UNIT III

Inter-organizational trust in E-Commerce: Need – Trading partner trust – Perceived benefits and risks of E-Commerce – Technology trust mechanism in E-Commerce – Perspectives of organizational, economic and political theories of inter-organizational trust – Conceptual model of inter-organizational trust in E-Commerce participation.

UNIT IV

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform

UNIT V

Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

REFERENCES

1. Kenneth C. Laudon and Carol Guercio Trave, "E-Commerce Business Technology Society", Pearson Education, 2005.

4. Pauline Ratnasingam, "Inter-Organizational Trust for Business-to-Business E- Commerce", IRM Press, 2005.

3. Siani Pearson, et al, "Trusted Computing Platforms: TCPA Technology in Context" , Prentice Hall PTR, 2002.

CS 978: BANKING TECHNOLOGY MANAGEMENT

UNIT I

Branch Operation and Core Banking - Introduction and Evolution of Bank Management – Technological Impact in Banking Operations – Total Branch Computerization – Concept of Opportunities – Centralized Banking – Concept, Opportunities, Challenges & Implementation.

UNIT II

Delivery Channels - Overview of delivery channels – Automated Teller Machine (ATM) – Phone Banking – Call centers – Internet Banking – Mobile Banking – Payment Gateways – Card technologies – MICR electronic clearing

UNIT III

Back office Operations - Bank back office management – Inter branch reconciliation – Treasury Management – Forex Operations – Risk Management – Data centre Management – Net work Management – Knowledge Management (MIS/DSS/EIS) – Customer Relationships Management (CRM)

UNIT IV

Interbank Payment System - Interface with Payment system Network – Structured Financial Messaging system – Electronic Fund transfer – RTGSS – Negotiated Dealing Systems & Securities Settlement Systems – Electronic Money – E Cheques

UNIT V

Contemporary Issues in Banking Techniques – Analysis of Rangarajan Committee Reports – E Banking - Budgeting – Banking Software's – Case study: Analysis of Recent Core Banking Software.

References:

1. Jessica Keyes, "Financial Services Information Systems", Auerbach publication; 2nd Edition, 2000.
2. Kaptan S S and Choubey N S., "E-Indian Banking in Electronic Era", Sarup & Sons, New Delhi, 2003.
3. Vasudeva, "E – Banking", Common Wealth Publishers, New Delhi, 2005.
4. Turban Rainer Potter, "Information Technology", John Wiley & Sons Inc., 2005.

CS979 - GAME THEORY

UNIT I

Fundamentals: Conflict, Strategy and Games, Game theory, The Prisoner's Dilemma, Scientific metaphor, Business case, Games in normal and extensive forms – Representation, Examination, Examples.

UNIT II

Non Cooperative Equilibria in Normal Games: Dominant Strategies and Social Dilemmas, Nash Equilibrium, Classical Cases in Game theory, Three person games, Introduction to Probability and Game theory, N-Person games.

UNIT III

Cooperative Solutions: Elements of Cooperative Games- Credible commitment, A Real Estate Development, Solution Set, Some Political Coalitions, Applications of the Core to Economics – The Market Game, The Core of a Two Person Exchange Game, The Core with More than Two Pairs of Traders, The core of Public Goods Contribution Game, Monopoly and Regulation .

UNIT IV

Sequential Games: Strategic Investment to Deter Entry, The Spanish Rebellion, Again, Imbedded Games – Planning Doctoral Study, Centipede Solved, Repeated play- Campers Dilemma, Pressing the shirts, Indefinitely Repeated Play – A Repeated Effort Dilemma, The Discount Factor.

UNIT V

Applications: Voting Games, Games and Experiments, Auctions, Evolution and Boundary Rational Learning.

REFERENCES

1. Roger A. McCain, "Game Theory – A Non-Technical Introduction to the Analysis of Strategy", Thomson South-Western, 2005.
2. Tirole, "Game Theory", Mit press 2005.
3. Osborne, "An Introduction to Game Theory", Oxford Press 2006.
4. E. N. Barron, "Game Theory: An Introduction", Wiley India Pvt Ltd, 2009.

CS980 - DESIGN OF SECURED ARCHITECTURES

UNIT I

Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security-Architecture Review of a System-Security Assessments-Security Architecture Basics-Architecture Patterns in Security.

UNIT II

Low-Level Architecture - Code Review-importance of code review- Buffer Overflow Exploits-Countermeasures Against Buffer Overflow Attacks-patterns applicable- Security and Perl-Bytecode Verification in Java-Good Coding Practices Lead to Secure Code- Cryptography-Trusted Code - Secure Communications

UNIT III

Mid-Level Architecture - Middleware Security- Middleware and Security- The Assumption of Infallibility-The Common Object Request Broker Architecture-The OMG CORBA Security Standard- Vendor Implementations of CORBA Security-CORBA Security Levels-Secure Interoperability- Application-Unaware Security-Application-Aware Security-Application Implications- Web Security - Application and OS Security - Database Security

UNIT IV

High-Level Architecture - Security Components- Secure Single Sign-On- Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories- Kerberos-Distributed Computing Environment-The Secure Shell, or SSH-The Distributed Sandbox-Security and Other Architectural Goals- Metrics for Non-Functional Goals-Force Diagrams around Security- High Availability- Robustness- Reconstruction of Events- Ease of Use-Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance-Portability.

UNIT V

Enterprise Security Architecture - Security as a Process-Security Data- Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the “Stupid Network”-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security

REFERENCES

1. Jay Ramachandran, “Designing Security Architecture Solutions”, Wiley Computer Publishing, 2010.
2. Markus Schumacher, “Security Patterns: Integrating Security and Systems Engineering”, Wiley Software Pattern Series, 2010.

CS981 - MULTICORE ARCHITECTURE AND PARALLEL ALGORITHMS

UNIT I

Fundamentals of SuperScalar Processor Design, Introduction to Multicore Architecture – Chip Multiprocessing, homogeneous Vs heterogeneous design - SMP – Multicore Vs Multithreading. Shared memory architectures– synchronization – Memory organization – Cache Memory – Cache Coherency Protocols - Design of Levels of Caches.

UNIT II

Multicore programming Model – Shared memory model, message passing model, transaction model – OpenMP and MPI Programming. PowerPC architecture – RISC design, PowerPC ISA, PowerPC Memory Management - Power 5 Multicore architecture design, Power 6 Architecture.

UNIT III

Cell Broad band engine architecture, PPE (Power Processor Element), SPE (Synergistic processing element), Cell Software Development Kit, Programming for Multicore architecture.

UNIT IV

PRAM Model – PRAM Algorithms – Parallel Reduction – Prefix Sums – List Ranking – Preorder Tree Traversal – Merging Two Sorted Lists – Graph Coloring – Reducing Number of Processors – NC Class - Classifying MIMD Algorithms – Hypercube SIMD Model – Shuffle Exchange SIMD Model – 2D Mesh SIMD Model – UMA Multiprocessor Model – Broadcase – Prefix Sums - Enumeration Sort – Lower Bound on Parallel Sorting – Odd-Even Transposition Sort –Bitonic Merge – Parallel Quick Sort – Complexity of Parallel Search – Searching on Multiprocessors.

UNIT V

P-Depth Search – Breadth Death Search – Breadth First Search – Connected Components – All pair Shortest Path – Single Source Shortest Path – Minimum Cost Spanning Tree. Matrix Multiplication on 2-D Mesh, Hypercube and Shuffle Exchange SIMD Models – Algorithms for Multiprocessors – Algorithms for Multicomputers – Mapping Data to Processors.

REFERENCES

1. Hennessey & Pateterson, “Computer Architecture A Quantitative Approach”, Harcourt Asia, Morgan Kaufmann, 1999
2. Joseph JaJa, “Introduction to Parallel Algorithms”, Addison-Wesley, 1992.
3. “Power 5, Power 6 and Cell Broadband engine architecture”, IBM Journal, Vol. 2, 1988.
4. Kai Hwang, “Advanced Computer Architecture: Parallelism, Scalability and Programmability”, McGraw-Hill, 1993.
5. Richard Y. Kain, “Advanced Computer Architecture: A System Design Approach”, PHI, 1999.
6. Rohit Chandra, Ramesh Menon, Leo Dagum and David Kohr, “Parallel Programming in OpenMP”, Morgan Kaufmann, 2000.
7. Michael J. Quinn, “Parallel Computing: Theory & Practice”, Tata McGraw Hill Edition, 2003.
8. Ananth Grame, George Karpis, Vipin Kumar and Anshul Gupta, “Introduction to Parallel computing” , 2nd Edition, Addison Wesley, 2003.

CS 982 – ETHICAL HACKING

UNIT I

Casing the Establishment - What is footprinting- Internet Footprinting. -Scanning-Enumeration - basic banner grabbing, Enumerating Common Network services. Case study- Network Security Monitoring

UNIT II

Securing permission - Securing file and folder permission. Using the encrypting file system. Securing registry permissions. Securing service- Managing service permission. Default services in windows 2000 and windows XP. Unix - The Quest for Root. Remote Access vs Local access. Remote access. Local access. After hacking root.

UNIT III

Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.

UNIT IV

Wireless Hacking - Wireless Footprinting. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

UNIT V

Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

REFERENCES:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

CS 983 - OBJECT ORIENTED SOFTWARE ENGINEERING

UNIT I

INTRODUCTION **:** System Concepts – Software Engineering Concepts – Development Activities – Managing Software Development – Unified Modeling Language – Overview – modeling concepts – deeper view into UML - Project Organization – Communication

UNIT II

ANALYSIS **:** Requirements Elicitation – Concepts – Activities – Management – Arena Case Study - Analysis Object Model – Analysis – Concepts – activities - Managing analysis - Case Study

UNIT III

SYSTEM DESIGN**:** Decomposing the system – Overview of System Design – System Design Concepts – System Design Activities – Addressing Design Goals – Managing System Design – Case Study

UNIT IV

OBJECT DESIGN AND IMPLEMENTATION ISSUES **:** Reusing Pattern Solutions – Concepts – Activities – Managing Reuse – Case Study - Specifying Interfaces – Concepts – Activities – Management – Case Study - Mapping Models to Code – Concepts – Activities – Management – Case Study – Testing – Concepts – Activities – Management

UNIT V

MANAGING CHANGE**:** Rationale Management – Concepts – Activities – Management - Configuration Management – Concepts – Activities – Management - Project Management - Concepts – Activities – Management – Software Life Cycle

REFERENCES:

1. Bernd Bruegge and Alan H Dutoit, “Object-Oriented Software Engineering”, 2nd edition, Pearson Education, 2010.

2. Timothy Lethbridge and Robert Laganiere, “Object-oriented Software Engineering: Practical Software Development using UML and Java”, Mc Graw Hill Publication, 2010.

CS 984 - DISTRIBUTED SYSTEMS SECURITY

UNIT – I

Introduction – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues, Common Security Techniques.

UNIT – II

Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities.

UNIT - III

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities -Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile.

UNIT - IV

Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions.

UNIT - V

Service-Level Solutions**:** Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services - SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture - Case Study: Grid - The Financial Application - Security Requirements Analysis. Future Directions - Cloud Computing Security **–** Security Appliances - Usercentric Identity Management - Identity-Based Encryption (IBE) - Virtualization in Host Security.

REFERENCES

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues. Processes and solutions”, Wiley, Ltd., Publication, 2009.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010.

Infrastructure and Faculty requirements for M.Tech(CSE-IS)

Faculty–student ratio: **1:12** (As per AICTE norms for intake of 18: 1 Professor, 1 Associate Professor, 1 Assistant Professors)
Class room Equipment: Multimedia Projector, Black Board

Teacher qualification Specilzation : M.Tech. in Computer Science and Engineering

Class Room: 1 area of 30 sq.m

Laboratory: 1

Resource	**Batch size of 25 students**
Computer System Server	1 No.
Computer systems node	18 No connected in LAN
UPS	Minimum of 5 KVA
Printer	2 No.
User License required for software (proprietary)	Minimum 18 No.
Software	1. Microsoft Server OS/ Linux Server OS/ UNIX Server OS/Any open source server OS / any Proprietary Server OS software[2] 2. Proprietary/ open source clientS 3. Borland C Compiler / Microsoft C compiler/ any open source C compiler/ any Proprietary C compiler 4. Java development Kit (Latest Version) 5. Microsoft Visual Studio With .Net Framework 6. DB2 Server / ORACLE server/ SQL Server/ Open source DBMS server software 7. Network simulator 8. Open MP 9. Firewalls and other information security tools