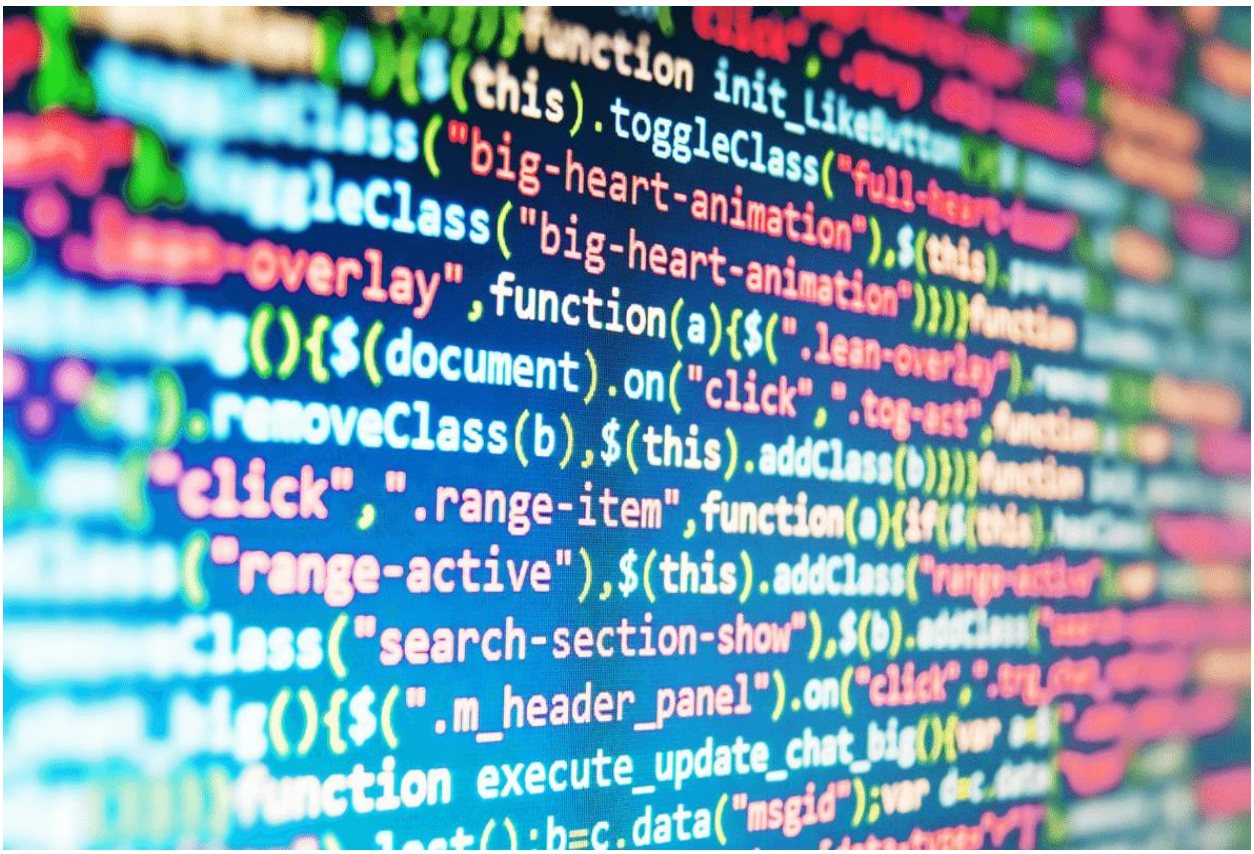



# Detailed Syllabus for Computer Science & Engineering with Specialization in Cyber Security

DEPT. OF COMPUTER SCIENCE & ENGINEERING

UNIVERSITY OF ENGINEERING & MANAGEMENT, JAIPUR

## PREAMBLE

Education plays an enormously significant role in the building of a nation. There are quite a large number of educational institutions, engaged in imparting education in our country. Majority of them have entered recently into semester system to match with international educational pattern. However, our present education system is churning out youth who have to compete locally, regionally, nationally as well as globally. The present alarming situation necessitates transformation and/or redesigning of system, not only by introducing innovations but developing "learner-centric approach.

Majority of Indian higher education institutions have been following marks or percentage-based evaluation system, which obstructs the flexibility for the students to study the subjects/courses of their choice and their mobility to different institutions. There is need to allow the flexibility in education system, so that students depending upon their interests can choose inter-disciplinary, intra-disciplinary and skill-based courses. This can only be possible when choice based credit system (CBCS), an internationally acknowledged system, is adopted. The choice based credit system not only offers opportunities and avenues to learn core subjects but also explore additional avenues of learning beyond the core subjects for holistic development of an individual. The CBCS will undoubtedly facilitate benchmarking of our courses with best international academic practices.

Advantages of the choice based credit system:

•Shift in focus from the teacher-centric to student-centric education.

•Student may undertake as many credits as they can cope with (without repeating all courses in a given semester if they fail in one/more courses).

•CBCS allows students to choose inter-disciplinary, intra-disciplinary courses, skill oriented papers (even from other disciplines according to their learning needs, interests and aptitude) and more flexibility for students.

•CBCS makes education broad-based and at par with global standards. One can take credits by combining unique combinations.

•CBCS offers flexibility for students to study at different times and at different institutions to complete one course (ease mobility of students). Credits earned at one institution can be transferred to another institution.

## CHOICE BASED CREDIT SYSTEM

The Indian Higher Education Institutions have been moving from the conventional annual system to semester system. Currently many of the institutions have already introduced the Choice Based Credit System. The semester system accelerates the teaching-learning process and enables vertical and horizontal mobility in learning. The credit based semester system provides flexibility in designing curriculum and assigning credits based on the course content and hours of teaching. The Choice Based Credit System provides a 'cafeteria' type approach in which the students can take courses of their choice, learn at their own pace, undergo additional courses to acquire more than the required credits and adopt an interdisciplinary approach to learning.

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

It has been a necessity to align higher education with the emerging needs of the economy so as to ensure that the graduates of higher education system have adequate knowledge and skills for employment and entrepreneurship since last few years. The higher education system has to incorporate the requirements of various industries in its curriculum, in an innovative and flexible manner while developing a well-groomed graduate. CSE department aims to encourage research and innovation in the field of Machine Learning, Cyber security, Artificial Intelligence and other allied areas such as Computational Theory, Cloud Computing, Blockchain Technology, Data Science, Big Data Analytics and many more. The objective of the Computer Science & Engineering Programme with Specialization in Cyber Security is to prepare students to undertake careers involving innovative technologies, develop a problem solving capability, or to opt for advanced studies for research oriented careers.

In order to give due importance to practical applications as well as theoretical aspects of CSE, the curriculum for the Computer Science & Engineering Programme with Specialization in Cyber Security covers most of the foundational aspects as well as develops engineering skills for problem solving.

## JOB OPORTUNITIES

Booming IT sector in India has plenty of jobs for fresh computer science graduates. Candidates with a high percentage of mark and good communication skills as well as sound computer knowledge do not face problem in getting a job. Computer engineers can get jobs in non-IT companies like universities, research, private and public industries, government departments, business organizations, commercial organizations and the manufacturing sector, etc. Besides the Computer Engineers have plenty of options to work in IT companies in departments such as design, development, assembly, manufacture, and maintenance, etc. Software Developers: Software developers are professionals who are concerned with facets of the software development process which involves activities such as design and coding, computer programming, project management, etc. Cyber security jobs are expanding rapidly across the nation. The Bureau of Labour Statistics (BLS) projects demand for information security analysts to grow between 2018 and 2028, more than five times the projected growth for all occupations nationwide. With companies increasingly relying on cloud computing, cyber-attacks are happening more often. Organizations across industries are responding by bolstering their cyber defences and opening more cyber security jobs

## PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

**PEO 01:** High Quality Engineering Design and Development Work: Graduates of the program will engage in the effective practice of computer science and engineering to identify and solve important problems in a diverse range of application areas.

**PEO 02:** Real Life Problem Solving: To educate students with proficiency in core areas of Computer science & Engineering and related engineering so as to comprehend engineering trade-offs, analyses, design, and synthesize data and technical concepts to create novel products and solutions for the real life problems.

**PEO 03:** Leadership: Graduates of the program will engage in successful careers in industry, academia and attain positions of importance where they have impact on their business, profession and community.

**PEO 04:** Lifelong Learning: Graduates of the program will adapt to contemporary technologies, tools and methodologies to remain at the frontier of computer science and engineering practice with the ability to respond to the need of a challenging environment.

## PROGRAM OUTCOME (PO)

| PO | Summary | Description |
|---|---|---|
| **PO1** | **Engineering knowledge** | Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. |
| **PO2** | **Problem analysis** | Identify, formulate, research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. |
| **PO3** | **Design /development of solutions** | Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. |
| **PO4** | **Conduct investigations of complex problems** | Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. |
| **PO5** | **Modern tool usage** | Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations. |
| **PO6** | **The engineer and society** | Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities |

| | | |
|---|---|---|
| | | relevant to the professional engineering practice. |
| **PO7** | **Environment and sustainability** | Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. |
| **PO8** | **Ethics** | Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. |
| **PO9** | **Individual and team work** | Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. |
| **PO10** | **Communication** | Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. |
| **PO11** | **Project management and finance** | Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. |
| **PO12** | **Life-Long Learning** | Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change |

## TYPES OF COURSES

1. Courses are the subjects that comprise the Computer Science & Engineering Programme with Specialization in Cyber Forensics & Internet Security.
2. A course may be designed to comprise lectures, tutorials, laboratory work, fieldwork, outreach activities, project work, vocational training, viva, seminars, term papers, assignments, presentations, self-study etc. or a combination of some of these components.
3. The learning outcomes of each course will be defined before the start of a semester.
4. Following are the course types:

   i. **Core Course (CC):** This is a course, which is to be compulsorily studied by a student as a core requirement to complete the requirement of B.Tech in Computer Science & Engineering with Specialization in Cyber Forensics & Internet Security.

   ii. **Elective Course:** An elective course is a course, which can be chosen from a pool of courses. It is intended to support the discipline of study by providing an expanded scope, enabling exposure to another discipline/domain and nurturing a student's proficiency and skill. An elective may be of following types:

   a) **Discipline Elective Courses (DE):** It is an elective course that adds proficiency to the students in the discipline.

   b) **Open Elective Courses (OE):** It is an open elective course taken from other engineering disciplines and enhances the generic proficiency and interdisciplinary perspective of students.

   c) **Specialization Elective Courses (SE):** This is a course, which is to be compulsorily studied by a student as a core requirement to complete the requirement of B.Tech in Computer Science & Engineering with Specialization in Cyber Forensics & Internet Security.

   iii. **Obligatory Courses:**

   a) **Mandatory Courses (MC)**: It can be taken from among a pool of foundation courses, which aim at value-based education. They may provide hands-on training to improve competencies and skills or provide education on human, societal, environmental and national values.

   b) **Internship/Training/Project/Dissertation (PTI):** Course designed to acquire special/advanced knowledge, such as supplement study/support study to a project work, and a candidate studies such a course on his own with an advisory support by a teacher/faculty member is called dissertation/project

   c) **Humanities, Social Sciences & Management (HSM):** It is an elective course taken from non-engineering disciplines (humanities, social sciences and management) that broadens the perspective of an engineering student.

   d) **Basic Science Courses (BSC):** It is based upon content that leads to fundamental knowledge enhancement in sciences, and basic engineering principles.

   e) **Engineering Science Courses (ESC):** It is based upon content that leads to fundamental knowledge enhancement in basic Engineering Principles.

   f) **NPTEL (NPT):** National Programme on Technology Enhanced Learning/Massive Open Online Courses (MOOCs) courses are based on the respective year's offered courses.

g) **General Studies Courses (GSC):** "Essential Studies for Professionals Skill & Skill Development for Professionals" courses designed to encourage and enrich the students for the technical and professional exams.

**h) Mandatory Additional Requirements (MAR):** A student has to do the following things to achieve the MAR points: The student should engage herself / himself in activities outside the curriculum. Join different types of Clubs of NSCBIP, write something for the wall magazine, remain active in outer society, participate in Tech Fests activities, etc.

5. Each credit course contributes certain credits to the programme. A course can be offered either as a full course (4 credits) or as a half course (2 credits). A full course is conducted with 3 hours of lectures and either 1 hour of tutorial or 2 hours of practical work per week. A half course is conducted with 2 hours of lectures. There are also some exceptional electives with 3 credits and 1 credit.

**Definition of Credit:**

| | |
|---|---|
| 1 Hr. Lecture (L) per week | 1 Credit |
| 1 Hr. Tutorial (T) per week | 1 Credit |
| 1 Hr. Practical (P) per week Or 2 Hr. Practical (Lab)/week | 0.5 Credits Or 1 Credit |

6. A project work/dissertation is considered as a special course involving application of the knowledge gained during the course of study in exploring, analyzing and solving complex problems in real life applications. A candidate completes such a course with an advisory support by a faculty member.
7. **Mandatory Courses** may be offered. They do not carry credits but aim at expanding knowledge or bridging deficiency in knowledge or skill.
8. A course may have pre-requisite course(s) that are given in the Semester-wise Course Allocation scheme.
9. A student can opt for a course only if he/she has successfully passed its pre- requisite(s).
10. A student has to register for all courses before the start of a semester.
11. **Program codes:** The codes for various undergraduate programmes are as follows:
    i. Civil Engineering: CE
    ii. Computer Science & Engineering: CS
    (Specialization in Cyber Forensics & Internet Security (CSCFIS))
    iii. Electronics and Communication Engineering: EC
    iv. Electrical Engineering: EE
    v. Mechanical Engineering: ME
12. **Departmental Course Codes:** The codes for departmental core courses and discipline-specific electives are specific to each discipline. The first two characters are derived from departmental codes listed above. The third character is 'C' for core courses and 'D' for discipline-specific courses and 'INT' for Dissertation/Project/Training/Internship. This is followed by a digit sequence number:
    i. CSCyyy: Core Course
    ii. CSDyyy: Discipline-Specific Elective Courses

iii. CFISyy: Specialization Elective Courses

iv. XXXyyy: Open Elective Courses (Depends on the respective Dept.)

v. INTyyy: Project/Training/Internship/ Dissertation

13. **Common Elective Course Codes:** All disciplines will follow a common code as shown below. The 3-digit sequence number 'yyy' is taken from the respective tables of different types of courses.

i. HSMyyy: Humanities, Social Sciences & Management Course

ii. BSCyyy: Basic Science Course

iii. MCyyy: Mandatory Course

iv. GSCyyy: General Studies Courses

v. MARyyy: Mandatory Additional Requirements

Here, yyy will be follow by a sequence of digit.

14. **General Electives:** A student may take a course under the category of General Elective (GE) offered by any other Department of the Institute under the categories of Core Course (CC) and Discipline Specific Electives (DE). However, such options shall be offered to a student as per prescribed guidelines of the Institute.

15. The opting of a course by the student will depend upon the requisites for that course and with the consent of the course advisor.

## PROCESS FOR DESIGNING THE PROGRAM CURRICULUM

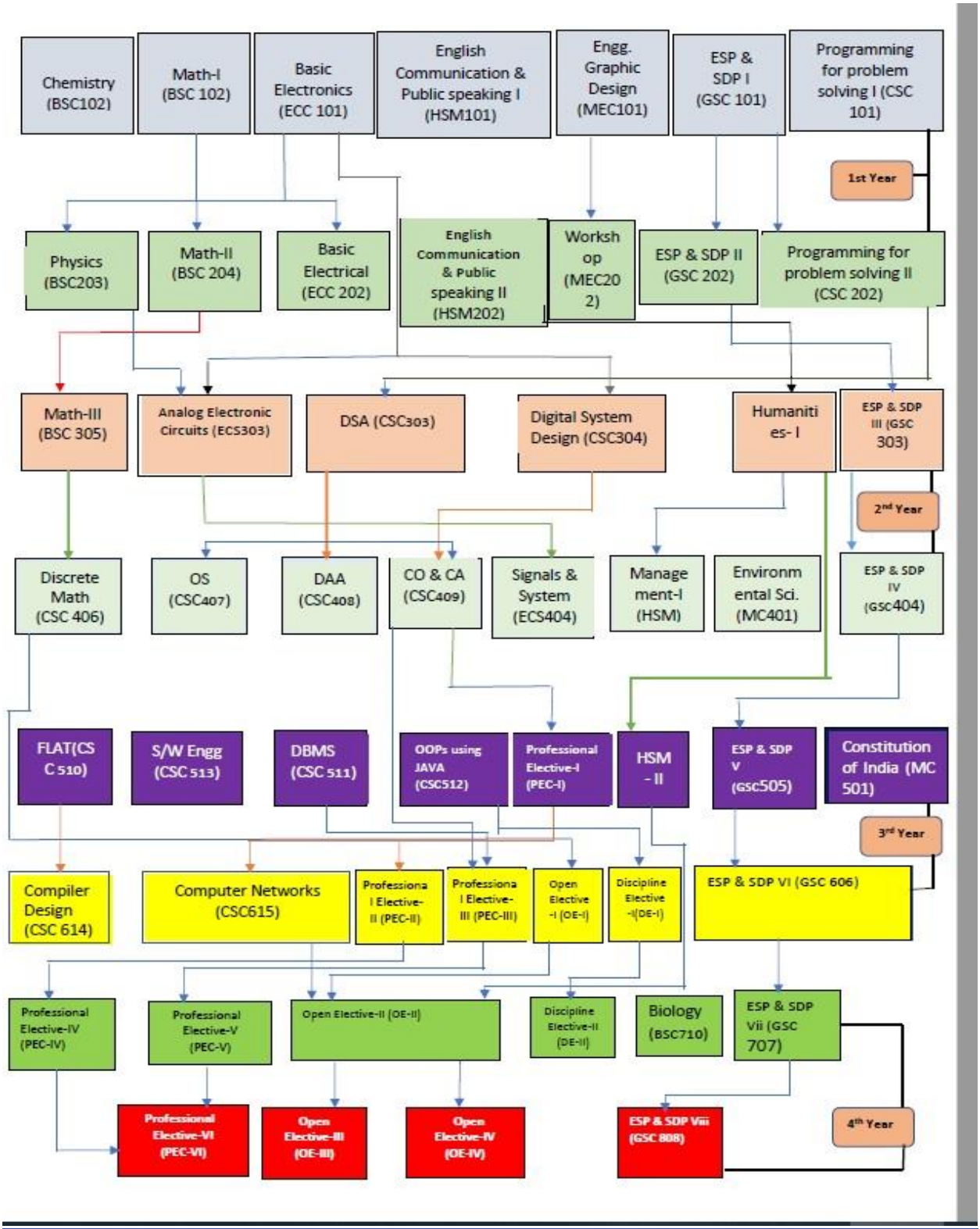
The process for designing the program curriculum involves consideration of the following aspects:

i) Feedback from stakeholders

ii) Institutional and Departmental Vision, Mission and PEOs

iii) Recent trends in industry and research

## PREREQUISITE TREE



## SCHEME – SEMESTER WISE COURSE ALLOCATION

### First Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| **1.** | BSC | BSC101 | Chemistry | 3 | 1 | 3 | 0 | 5.5 |
| **2.** | BSC | BSC102 | Mathematics-I (Calculus & Linear Algebra) | 3 | 1 | 0 | 0 | 4 |
| **3.** | ESC | ECC101 | Basic Electronics Engineering | 2 | 0 | 2 | 0 | 3 |
| **4.** | ESC | MEC101 | Engineering Graphics & Design | 1 | 0 | 2 | 0 | 2 |
| **5.** | ESC | CSC101 | Programming for Problem Solving-I (C) | 2 | 0 | 0 | 2 | 2 |
| **6.** | HSM | HSM101 | English Communication & Public Speaking Skills-I | 0 | 0 | 2 | 0 | 1 |
| **7.** | GSC | GSC101 | ESP & SDP-I | 2 | 0 | 0 | 2 | 2 |
| | | | Total | 13 | 2 | 9 | 4 | 19.5/28 |

#Students will undergo a mandatory Induction Program

### Second Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| **1.** | BSC | BSC203 | Physics (Semi-Conductor Physics) | 3 | 1 | 3 | 0 | 5.5 |
| **2.** | BSC | BSC204 | Mathematics-II(Probability & Statistics) | 3 | 1 | 0 | 0 | 4 |
| **3.** | ESC | EEC202 | Basic Electrical Engineering | 2 | 0 | 2 | 0 | 3 |
| **4.** | ESC | MEC202 | Workshop & Manufacturing Practices | 1 | 0 | 2 | 0 | 2 |
| **5.** | ESC | CSC202 | Programming for Problem Solving-II (Python) | 2 | 0 | 0 | 2 | 2 |
| **6.** | HSM | HSM202 | English Communication & Public Speaking Skills-II | 1 | 0 | 3 | 0 | 2 |
| **7.** | GSC | GSC202 | ESP & SDP-II | 2 | 0 | 0 | 2 | 2 |
| **8.** | NPT | NPT201 | (NPTEL/MOOCs) | - | - | - | - | 2 |
| | | | Total | 15 | 0 | 9 | 4 | 22.5/28 |

#(NPT201)NPTEL/MOOCs are based on the respective year's offered courses.

## Third Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| **1.** | BSC | BSC305 | Mathematics-III (Differential Calculus) | 2 | 0 | 0 | 0 | 2 |
| **2.** | PCC | CSC303 | Data Structure & Algorithms | 3 | 0 | 3 | 0 | 4.5 |
| **3.** | ESC | ECS303 | Analog Electronic Circuits | 2 | 0 | 3 | 0 | 3.5 |
| **4.** | PCC | CSC304 | Digital Electronics | 3 | 0 | 3 | 0 | 4.5 |
| 5. | PCC | CSC305 | IT Workshop (Sci Lab/MATLAB) | 1 | 0 | 4 | 0 | 3 |
| 6. | HSM | HSM--- | Humanities-I | 3 | 0 | 0 | 0 | 3 |
| **7.** | GSC | GSC303 | ESP & SDP-III | 2 | 0 | 0 | 2 | 2 |
| **8.** | MAR | MAR381 | Mandatory Additional Requirements (MAR) | 0 | 0 | 0 | 1 | 0.5 |
| **9.** | NPT | NPT302 | (NPTEL/MOOCs) | - | - | - | - | 2 |
| | | | Total | 17 | 0 | 13 | 3 | 25/33 |

#(NPT302): NPTEL/MOOCs are based on the respective year's offered courses.

## Suggestive Choice Based Subjects

| Sl No | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| **1.** | HSM | **HSM303** | Organizational Behavior | 3 | 0 | 0 | 3 |
| **2.** | **HSM** | **HSM304** | **Values and Ethics in Profession** | 3 | 0 | 0 | 3 |
| **3** | HSM | HSM305 | Industrial Psychology | 3 | 0 | 0 | 3 |

## Fourth Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| **1.** | PCC | CSC406 | Discrete Mathematics | 3 | 0 | 0 | 0 | 3 |
| **2.** | PCC | CSC407 | Operating System | 3 | 0 | 3 | 0 | 4.5 |
| **3.** | PCC | CSC408 | Design & Analysis of Algorithms | 3 | 0 | 3 | 0 | 4.5 |
| **4.** | PCC | CSC409 | Computer Organization & Architecture | 3 | 0 | 3 | 0 | 4.5 |
| **5.** | ESC | ECS404 | Signals & System | 3 | 0 | 0 | 0 | 3 |
| **6.** | HSM | HSM--- | Management-I | 3 | 0 | 0 | 0 | 3 |
| **7.** | GSC | GSC404 | ESP & SDP-IV | 2 | 0 | 0 | 2 | 2 |
| **8.** | MC | MC401/402 | Environmental Sciences/Disaster Management | 0 | 0 | 0 | 2 | 0 |
| **9.** | MAR | MAR484 | Mandatory Additional Requirements (MAR) | 0 | 0 | 0 | 1 | 0.5 |
| **10.** | NPT | NPT403 | (NPTEL/MOOCs) | - | - | - | - | 2 |
| | | | Total | 20 | 0 | 9 | 5 | 27/34 |

#(NPT403): NPTEL/MOOCs are based on the respective year's offered courses.

## Suggestive Choice Based Subjects

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| **1.** | HSM | HSM406 | Human Resource Development and Organizational Behavior | 3 | 0 | 0 | 3 |
| **2.** | HSM | **HSM407** | **Economics & Financial Accounting** | 3 | 0 | 0 | 3 |
| 3. | HSM | HSM408 | Economics for Engineers | 3 | 0 | 0 | 3 |

## Fifth Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| **1.** | PCC | CSC510 | Formal Language & Automata Theory | 3 | 0 | 0 | 0 | 3 |
| **2.** | PCC | CSC511 | Data Base Management System | 3 | 0 | 3 | 0 | 4.5 |
| **3.** | PCC | CSC512 | Object Oriented Programming Using Java | 2 | 0 | 3 | 0 | 3.5 |
| **4.** | PCC | CSC513 | Software Engineering | 2 | 0 | 2 | 0 | 3 |
| **5.** | PEC/SEC | --- | Professional Elective-I | 3 | 0 | 0 | 0 | 3 |
| **6.** | HSM | HSM--- | Humanities-II | 3 | 0 | 0 | 0 | 3 |
| **7.** | MC | MC503 | Constitution of India/Essence of Indian Knowledge Tradition | 0 | 0 | 0 | 0 | 0 |
| **8.** | GSC | GSC505 | ESP & SDP-V | 2 | 0 | 0 | 2 | 2 |
| **9.** | PTI | INT501 | Internship/Project-I | 0 | 0 | 0 | 1 | 1 |
| **10.** | NPT | NPT504 | (NPTEL/MOOCs) | - | - | - | - | 2 |
| | | | Total | 19 | 0 | 6 | 3 | 25/28 |

#(NPT504): NPTEL/MOOCs are based on the respective year's offered courses.

## Suggestive Choice Based Subjects

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1. | PEC* | CSP501 | Embedded Systems | 2 | 0 | 2 | 3 |
| 2. | PEC** | CSP502 | AI & Machine Learning | 2 | 0 | 2 | 3 |
| 3. | HSM | HSM509 | Industrial Psychology | 2 | 0 | 0 | 2 |
| 4. | HSM | **HSM510** | **Principle of Management** | 2 | 0 | 0 | 2 |
| 5. | HSM | HSM511 | Total Quality Management | 2 | 0 | 0 | 2 |

**Note: Students can opt any Professional Track from 5th Sem Onwards/Cyber Security Specialization:**

***Track:** IOT, Cybersecurity & Blockchain Track

****Track:** AI & Machine Learning Track

## Sixth Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | S | Credit Points |
|---|---|---|---|---|---|---|---|---|
| 1 | PCC | CSC614 | Compiler Design | 3 | 0 | 3 | 0 | 4.5 |
| 2 | PCC | CSC615 | Computer Networks | 3 | 0 | 3 | 0 | 4.5 |
| 3 | PEC/SEC | --- | Professional/Specialization Elective -II | 2 | 0 | 2 | 0 | 3 |
| 4 | PEC/SEC | --- | Professional/Specialization Elective -III | 3 | 0 | 0 | 0 | 3 |
| 5 | OE | --- | Open Elective-I | 2 | 0 | 0 | 0 | 3 |
| 6 | DE | CSD--- | Discipline Elective-I | 2 | 0 | 2 | 0 | 3 |
| 7. | GSC | GSC606 | ESP & SDP-VI | 2 | 0 | 0 | 2 | 2 |
| 8. | PTI | INT604 | Internship/Industrial Training/Project-II | 0 | 0 | 0 | 1 | 1 |
| 9. | NPT | NPT605 | (NPTEL/MOOCs) | - | - | - | - | 2 |
| | | | Total | 17 | 0 | 10 | 3 | 26/30 |

#(NPT605): NPTEL/MOOCs are based on the respective year's offered courses.

## Suggestive Choice Based Subjects

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1. | PEC* | CSP5603 | Blockchain Technology | 3 | 0 | 0 | 3 |
| 2. | PEC** | CSP604 | Soft Computing | 3 | 0 | 0 | 3 |
| 3. | PEC* | CSP605 | AI & Machine Learning | 3 | 0 | 2 | 4 |
| 4. | PEC** | CSP606 | Big Data Analytics | 3 | 0 | 2 | 4 |
| 5. | OE | BSC607 | Numerical Methods & Operation Research | 2 | 0 | 2 | 3 |
| 6. | OE | BSC608 | Operations Research | 2 | 0 | 2 | 3 |
| 7. | OE | BSC609 | Statistics for Data Analysis | 2 | 0 | 2 | 3 |
| 8. | OE* | CSD601 | Blockchain Technology | 3 | 0 | 0 | 3 |
| 9. | OE** | CSD602 | Big Data Analytics | 3 | 0 | 2 | 4 |
| 10. | DE | CSD603 | Web Technology | 2 | 0 | 2 | 3 |
| 11. | DE | CSD604 | Computer Graphics | 2 | 0 | 2 | 3 |
| 13. | DE | **CSD605** | **Software Project Management** | 2 | 0 | 2 | 3 |
| 14. | DE | CSD606 | E-Commerce | 2 | 0 | 2 | 3 |

## Seventh Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1 | PEC/SEC | --- | Professional/Specialization Elective -IV | 3 | 0 | 0 | 3 |
| 2 | PEC/SEC | --- | Professional/Specialization Elective -V | 3 | 0 | 0 | 3 |
| 3. | OE | --- | Open Elective-II | 3 | 0 | 0 | 3 |
| 4. | BSC | BSC710 | Biology | 2 | 1 | 0 | 3 |
| 5. | GSC | GSC707 | ESP & SDP-VII | 2 | 0 | 2 | 2 |
| 6. | PTI | INT705 | Internship/Industrial Training/Project-III | 0 | 0 | 8 | 4 |
| | | | Total | 13 | 1 | 8 | 18/21 |

#Students will undergo project/training/internship in the industry / research organization / reputed Institute during the vacation

## Suggestive Choice Based Subjects

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1. | PE* | CSP707 | Blockchain Technology | 3 | 0 | 0 | 3 |
| 2. | PE** | CSP708 | Natural Language Processing | 3 | 0 | 0 | 3 |
| 3. | PEC* | CSP709 | Digital Forensics | 3 | 0 | 0 | 3 |
| 4. | PEC** | CSP710 | Computer Vision | 3 | 0 | 0 | 3 |
| 5. | CSD* | CSD707 | Cyber Law, IPR & Ethics | 3 | 0 | 0 | 3 |
| 6. | CSD** | CSD708 | Natural Language Processing | 3 | 0 | 0 | 3 |
| 7. | OE | CSD709 | Wireless Sensor Network & Network Security | 3 | 0 | 0 | 3 |
| 8. | OE | CSD710 | Neural Network and Application | 3 | 0 | 0 | 3 |
| 9. | OE | CSD711 | Real Time Operating System | 3 | 0 | 0 | 3 |
| 10. | OE | CSD712 | Distributed System | 3 | 0 | 0 | 3 |
| 11. | BSC | BSC711 | Statistics For Data Analytics | 3 | 0 | 0 | 3 |
| 12. | BSC | BSC712 | Statistical Methods For Decision Making | 3 | 0 | 0 | 3 |
| 13. | BSC | BSC713 | Exploratory Data Analysis | 3 | 0 | 0 | 3 |
| 14. | BSC | BSC714 | Graph Theory | 3 | 0 | 0 | 3 |

## Eighth Semester Syllabus

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1. | PEC/SEC | --- | Professional/Specialization Elective-VI | 3 | 0 | 0 | 3 |
| 2. | OE | --- | Open Elective-III | 3 | 0 | 0 | 3 |
| 3. | OE | --- | Open Elective-IV | 3 | 0 | 0 | 3 |
| 4. | GSC | GSC808 | ESP & SDP - VIII | 2 | 0 | 2 | 2 |
| 5. | PTI | INT806 | Internship Industrial Training/Project-IV | 0 | 0 | 12 | 6 |
| 6. | CC | CSC881 | Grand Viva | 0 | 0 | 0 | 2 |
| | | | Total | 11 | 0 | 14 | 19/25 |

#Students will undergo project/training/internship in the industry / research organization / reputed Institute during the vacation.

## Suggestive Choice Based Subjects

| Sl No. | Type | Subject Code | Topic | L | T | P | Credit Points |
|---|---|---|---|---|---|---|---|
| 1. | PEC* | CSP811 | Digital Forensics | 3 | 0 | 0 | 3 |
| 2. | PEC** | CSP812 | Deep Learning | 3 | 0 | 0 | 3 |
| 3. | OE | CSD813 | Data Mining & Data Ware Housing | 3 | 0 | 0 | 3 |
| 4. | OE | CSD814 | Information Theory & Coding | 3 | 0 | 0 | 3 |
| 5. | OE | CSD815 | Advanced Algorithms | 3 | 0 | 0 | 3 |
| 6. | OE | CSD816 | Digital Image Processing | 3 | 0 | 0 | 3 |

## Professional Elective Courses:

| Subject Code | IOT, Cybersecurity & Blockchain Track | Subject Code | AI & Machine Learning Track |
|---|---|---|---|
| CSP501 | Embedded Systems | CSP502 | AI & Machine Learning |
| CSP603 | Blockchain Technology | CSP504 | Soft Computing |
| CSP605 | AI & Machine Learning | CSP606 | Big Data Analytics |
| CSP707 | Cyber Security | CSP608 | Natural Language Processing |
| CSP709 | Cyber Law, IPR & Ethics | CSP710 | Computer Vision |
| CSP811 | Digital Forensics | CSP712 | Deep Learning |

## Specialization Course:

| Subject Code | Cyber Forensics & Internet Security |
|---|---|
| **IS501** | Information Theory for Cyber Security |
| **IS602** | Data Encryption |
| **IS603** | Steganography and Digital Watermarking |
| **IS704** | Security Assessment and Risk Analysis |
| **IS705** | Database Security and Access Control |
| **IS806** | Security Identity & Risk Management |
| **IS807** | Ethical Hacking |
| **IS808** | Applied & Quantum Cryptography |
| **IS809** | Intrusion Detection and Prevention System |

**Note: Refer to Computer Science & Engineering Syllabus for "syllabus of other subject".**

**TITLE OF COURSE: Information Theory for Cyber Security**
**COURSE CODE: IS501**
**L-T-P: 3-0-0**
**CREDITS: 3**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**
The objective of this course is to provide an insight to information coding techniques, error correction mechanism for cyber security.
**Course Outcomes (CO):** After completion of course, students would be able:
**CO1:** To introduce the principles and applications of information theory.
**CO2:** To justify how information is measured in terms of probability and entropy.
**CO3:** To learn coding schemes, including error correcting codes.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |

**Course Contents:**
**Module 1:**
Shannon's foundation of Information theory, Random variables, Probability distribution factors, Uncertainty/entropy information measures, Leakage, Quantifying Leakage and Partitions, Lower bounds on key size: secrecy, authentication and secret sharing. provable security, computationally-secure, symmetric cipher.
**Module 2:**
Secrecy, Authentication, Secret sharing, Optimistic results on perfect secrecy, Secret key agreement, Unconditional Security, Quantum Cryptography, Randomized Ciphers, Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques.
**Module 3:**
Information-theoretic security and cryptograph, basic introduction to Diffie-Hellman, AES, and side-channel attacks.
**Module 4:**
Secrecy metrics: strong, weak, semantic security, partial secrecy, Secure source coding:

rate-distortion theory for secrecy systems, side information at receivers, Differential privacy, Distributed channel synthesis.

**Module 5:**

Digital and network forensics, Public Key Infrastructure, Light weight cryptography, Elliptic Curve Cryptography and applications.

**Text Books**

1. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons.
2. Communication Systems: Analog and digital, Singh and Sapre, Tata McGraw Hill.
3. Fundamentals in information theory and coding, Monica Borda, Springer.
4. Information Theory, Coding and Cryptography R Bose.

**References:**

1. Information Security & Cyber Laws, Gupta & Gupta, Khanna Publishing House.
2. Multi-media System Design, Prabhat K Andleigh and Kiran Thakrar.

## TITLE OF COURSE: Data Encryption

**COURSE CODE: IS602**
**L-T-P: 3-0-2**
**CREDITS: 4**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**

This course will cover the concept of security, types of attack experienced, encryption and authentication for deal with attacks, what is data compression, need and techniques of data compression.

**Course Outcomes (CO):** After completion of course, students would be able:
**CO1:** To introduce the principles and applications of information theory.
**CO2:** To justify how information is measured in terms of probability and entropy.
**CO3:** To learn coding schemes, including error correcting codes.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |

**Course Contents:**

**Module 1**

**Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attacks.

**Encryption Techniques:** Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.

**Module 2**

**Symmetric & Asymmetric Key Cryptography:** Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.

**Module 3**

**Case Studies of Cryptography:** Denial of service attacks, IP spoofing attacks, Conventional Encryption and Message Confidentiality, Conventional Encryption Algorithms, Key Distribution.

**Public Key Cryptography and Message Authentication:** Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management, Firewall.

**Module 4**

**Introduction:** Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification.

**Methods of Data Compression:** Data compression-- Loss less & Lossy.

**Module 5**

**Entropy encoding**-- Repetitive character encoding, Run length encoding, Zero/Blank encoding; Statistical encoding-- Huffman, Arithmetic & Lempel-Ziv coding; Source encoding-- Vector quantization (Simple vector quantization & with error term).

**Module 6**

Recent trends in encryption and data compression techniques.

**Text Books**

1. Cryptography and Network Security, Mohammad Amjad, John Wiley & Sons.
2. Cryptography & Network Security by Atul Kahate, TMH.
3. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons.

**References:**

1. Cryptography and Network Security by B. Forouzan, McGraw-Hill.
2. The Data Compression Book by Nelson, BPB.
3. Cryptography & Network Security, V.K. Jain, Khanna Publishing House.

## TITLE OF COURSE: Steganography and Digital Watermarking

**COURSE CODE: IS603**

**L-T-P: 3-0-0**

**CREDITS: 3**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and

discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**
The objective of course is to provide an insight to steganography techniques. Watermarking techniques along with attacks on data hiding and integrity of data is included in this course.

**Course Outcomes (CO):** After completion of course, students would be able to:
**CO1:** Learn the concept of information hiding.
**CO2:** Survey of current techniques of steganography and learn how to detect and extract hidden information.
**CO3:** Learn watermarking techniques and through examples understand the concept.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |

**Course Contents:**
**Module 1**
**Steganography:** Overview, History, Methods for hiding (text, images, audio, video, speech etc.).
Steganalysis: Active and Malicious Attackers, Active and passive Steganalysis.
**Module 2**
Frameworks for secret communication (pure steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive).
**Module 3**
Steganography techniques: Substitution systems, Spatial Domain, transform domain techniques, Spread spectrum, Statistical steganography.
**Module 4**
Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets.
**Module 5**
**Digital Watermarking**: Introduction, Difference between Watermarking and Steganography, Classification (Characteristics and Applications),
types and techniques (Spatial-domain, Frequency-domain, and Vector quantizationbased watermarking), Watermark security & authentication.
**Module 6**
Recent trends in Steganography and digital watermarking techniques. Case study of LSB Embedding, LSB Steganalysis using primary sets.

**Text Books**
1. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker,

"Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.

**References:**

1. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, Sushil Jajodia.
2. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas.

**Corresponding Online Resources:**

1. Cyber Security, https://swayam.gov.in/nd2_cec20_cs09/preview.
2. Introduction to Cyber Security, https://swayam.gov.in/nd2_nou20_cs01/preview

**TITLE OF COURSE: Security Assessment and Risk Analysis**
**COURSE CODE: IS704**
**L-T-P: 3-0-2**
**CREDITS: 4**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**
Describe the concepts of risk management in information security. Define and differentiate various Contingency Planning components. Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

**Course Outcomes (CO):** After completion of course, students would be able:
**CO1:** To apply contingency strategies including data backup and recovery and alternate site selection for business resumption planning
**CO2:** To Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.
**CO3:** To Design a Disaster Recovery Plan for sustained organizational operations.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |

**Course Contents:**

**Module 1**

SECURITY BASICS: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security countermeasures-education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.

**Module 2**

Threats to and Vulnerabilities of Systems: Threats, major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS).

Countermeasures: assessments (e.g., surveys, inspections).

Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis and implementation of controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information).

33

**Module 3**

Security Planning: directives and procedures for policy mechanism. Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event.

**Module 4**

Personnel Security Practices and Procedures: access authorization/verification (needto-know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel.

Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

**Module 5**

Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link).

**Module 6**

Case study of threat and vulnerability assessment.

**Text Books**

1. Information Systems Security, 2ed: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, John Wiley & Sons.

2. Principles of Incident Response and Disaster Recovery, Whitman & Mattord, Course Technology ISBN: 141883663X.

**Corresponding Online Resources:**

1. Introduction to Cyber Security, https://swayam.gov.in/nd2_nou20_cs01/preview
2. (Web Link) http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

**TITLE OF COURSE: Database Security and Access Control**
**COURSE CODE: IS705**
**L-T-P: 3-0-2**
**CREDITS: 4**

**Pre-requisite:** Good knowledge of communication principles. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**
The objective of the course is to provide fundamentals of database security. Various access control techniques mechanisms were introduced along with application areas of access control techniques.

**Course Outcomes (CO):** After completion of this course, the students will be enable:
**CO1:** To understand and implement classical models and algorithms.
**CO2:** To analyze the data, identify the problems, and choose the relevant models and algorithms to apply.
**CO3:** To assess the strengths and weaknesses of various access control models and to analyze their behavior.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |

**Course Contents:**
**Module 1**
Introduction to Access Control, Purpose and fundamentals of access control.
**Module 2**
Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control (DAC), Non- Discretionary Access Control, Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations.
**Module 3**
Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access Control policy, Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments.
**Module 5**
Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management. PPS Security techniques- user identification, smart card security, quality

assurance and testing, smart card life cycle-5 phases, smart card terminals.

**Module 6**

Cloud Data Security: Recent trends in Database security and access control mechanisms.
Cloud Data Audit: Intro, Audit, Best Practice, Key management, Cloud Key Management Audit.

**Text Books**

1. Role Based Access Control: David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli.

**Corresponding Online Resources:**

1. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf : Smart Card Tutorial.
2. Advanced System Security Topics, https://www.coursera.org/lecture/advancedsystem-security-topics/role-based-access-control-rbac-bYvzS.

**TITLE OF COURSE: SECURITY IDENTITY & RISK MANAGEMENT**
**COURSE CODE: IS806**
**L-T-P: 3-0-0**
**CREDITS: 3**

**Pre-requisite:** Basic concepts in digital network security.

**Introduction:**

This course examines Security Identity & Risk Management. The Topics to be covered (tentatively) include: an introduction to security management, Threats, Risks and SANS 20, Risk modeling and IT risk framework, Forensic and Exam review, Legal and ethical issues in computer security.

**Course Outcomes (CO):**

In this course we will study the basic Security Identity & Risk Management. Students are expected to be capable of understanding the Legal and ethical issues in computer security, their advantages and drawbacks, how to implement them in digital world, how their drawbacks can be overcome and what the applications are and where they can be used. To reach this goal, the following objectives need to be met:

**CO1:** Students would be able to understand the role of Security Management in information technology systems
**CO2:** Student would be able to understanding of the role of firewalls, guards, proxy servers and intrusion detection in networks on a Linux OS with traffic analysis
**CO3:** Student would be able to evaluate the residual risk of a protected network
**CO4:** Student would be able to apply legal and ethical standards in the Information Security context.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | | | ✓ | | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |

**Course Contents:**

**Module-1:** Introduction to security management and to the different cyber security courses taught at Morgan State. cyber risks, basic computer security and network security concepts.

**Module-2:** Threats, Risks and SANS 20 Critical Controls Overview SANS 20 critical control for security management, cyber security concepts: Threats, Vulnerabilities. SANS 20 critical controls for security management vulnerabilities and threats will be presented, key terms.

**Module-3:** Risk modeling and IT risk framework, A novel risk framework, Numerical risk computation. Quantification of risk and costs associated with attacks are explained and determined compare the advantages and disadvantages of various risk assessment methodologies. Balance the defense and control to minimize cost associated with successful breach.

**Module-4:** Risk decisions and IT risk framework analysis. IT risk framework reasonable decisions to minimize the cost of a cyber-attack based on simulation of the risk, evaluate and categorize risk.

**Module-5:** Risk management: NIST 800-30 and 800-39 documents. Assess security risks and costs based on NIST 800-30/39 document and discuss risk assessment from NIST POV. various risk, analysis methodologies and decisions on risk management issues based on the NIST guidelines and Program a risk assessment model to relation between risk and system security policy.

**Module-6:** Forensic and incident response. monitoring, forensics and incident response. security monitoring, identify key concepts in forensic analysis, and make recommendation on incident response given any scenario.

**Module-7:** More on Incident response. we will have a closer look of the NIST SP800-61 document and identify SP800-61 key goals. Also, incident response mechanisms will be explained as well as how to select the best response possible in any given situation.

**Module-8:** Forensic and Exam review. NIST SP800-86 document, network forensics. Cyber forensics will be studied in details, the best forensic analysis in any given situation.

**Module-9:** Forensic SP800-86 document, handle an incident, integrate forensic techniques into incident response, and use data from data files for forensic analysis, use data from operating systems for forensic analysis. Lastly, detect and prevent intrusion.

**Module-10:** Supply Chain Risk Management Practices, NIST SP800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations), identify core components ICT SCRM controls, integrate ICT SCRM into organization wide risk management, and identify ICT supply chain threat events.

**Module-11:** Policy, legal and ethical implications of the security management, data security and its importance. Legal, Ethical and compliance issues regarding data security and identity theft. Identify the risk of identity theft, distinguish different data handling policies, and explain different federal and statewide policies related to cyber security and acts addressing issues of data security such as HIPAA/FERPA.

**Module-12:** Legal and ethical issues in computer security: Evaluating legal, ethical and compliance issues regarding computer security. The key legal terms in computer security such as Patents, copyrights, and IP in Information Concept. Identify different computer crimes, examine a computer fraud case for ethical issues, and comply by the rules of the ethics as dealing with cybercrimes.

**Text Books**

1. Security Awareness—Applying Practical Security in Your World, 4th Ed. Mark Ciampa Copyright © 2014 Course Technology, ISBN-13: 978-1-111-64418-5

**References**

1. Computer Forensics and Cyber Crime, An Introduction, 3rd Ed. Marjie Britz, Copyright © 2013

Pearson/Prentice Hall, ISBN-13: 978-0-13-267771-4

**TITLE OF COURSE: ETHICAL HACKING**
**COURSE CODE: IS807**
**L-T-P: 3-0-0**
**CREDITS: 3**

Pre-requisite: Basic concepts of Networking.

**Introduction:**

This course examines Ethical Hacking and security basics. The Topics to be covered (tentatively) include: an introduction to Ethical Hacking, importance of security, Foot-printing & Port Scanning, Hacking Web Services & Session Hijacking, and Hacking Wireless Networks.

**Course Outcomes (CO):**

In this course we will study the basic components of Ethical Hacking. Students are expected to be capable of understanding the digital foot-print, their advantages and drawbacks, how to implement them in python, how their drawbacks can be overcome and what the applications are and where they can be used. To reach this goal, the following objectives need to be met:

**CO1:** Students would be able to design & implement any digital security properly.

**CO2:** Students would be able to implement System Hacking their own algorithm.

**CO3:** By analyzing the logic of any algorithm, students would be able to Hacking Web Services & Session Hijacking.

**CO4:** To become an efficient network administrator.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | | | ✓ | | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |

**Course Contents:**

**Module-1:** The importance of security, Concept of ethical hacking and essential Terminologies Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking

**Module-2:** Foot printing & Port Scanning: Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS

**Module-3:** System Hacking : Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active

and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing.

**Module-4:** Hacking Web Services & Session Hijacking: Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools

**Module-5:** Hacking Wireless Networks: Introduction to 802.11,Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.

**Text Books**

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
2. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology, 2010

**References**

1. Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt Publishing, 2011
2. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003
3. Rajat Khare, "Network Seuciryt and Ethical Hacking", Luniver Press, 2006

**TITLE OF COURSE: FUNDAMENTAL OF CRYPTOGRAPHY**
**COURSE CODE:**
**L-T-P: 2-0-2**
**CREDITS: 3**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**
Cryptography consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources**.**

**Course Outcomes (CO):**
**CO1:** Have a good understanding of how applications can communicate securely and what tools and protocols exist in order to offer different levels of security
**CO2:** Have detailed knowledge and the ability to critically analyze and design secure networks, applications and systems
**CO3:** Have a fundamental understanding of what makes systems vulnerable and be able to predict new attack methods before they become a reality
**CO4:** Have enough knowledge to evaluate protocols and ability to draw conclusions about the level of security they can offer
**CO5:** Understand what impact the selection of different protocols and security architectures can have to an application or a system

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |

**Course Contents:**
**Module 1:** Introduction and Mathematical Foundation, Introduction to cryptography, Overview on Modern Cryptography, Number Theory, Probability and Information Theory
**Module 2: Classical Cryptosystems**
Cryptanalysis of Classical Cryptosystems, Shannon's Theory: I, Shannon's Theory: II, Shannon's Theory: III
**Module 3:.Symmetric Key Ciphers**

Modern Block Ciphers (DES), Modern Block Cipher (AES), Modern Block Cipher (AES) contd.

**Module 4: Cryptanalysis of Symmetric Key Ciphers**

Linear Cryptanalysis, Differential Cryptanalysis, Other Cryptanalytic Techniques, Overview on S-Box Design Principles, Modes of operation of Block Ciphers

**Module 5: Stream Ciphers and Pseudorandomness**

Stream Ciphers, Pseudorandom functions

**Module 6: Hash Functions and MACs Hash functions:**

The Merkle Damgard Construction, Message Authentication Codes (MACs)

**Module 7:.Asymmetric Key Ciphers:**

Construction and Cryptanalysis, More Number Theoretic Results, The RSA Cryptosystem, Primality Testing, Factoring Algorithms, Other attacks on RSA and Semantic Security of RSA, The Discrete Logarithm Problem (DLP) and the Diffie Hellman Key Exchange algorithm, The ElGamal Encryption Algorithm, Cryptanalysis of DLP

**Module 8: Digital Signatures**

Signature schemes: I, Signature schemes: II

**Text Books**

1. William Stallings: Cryptography and Network Security, seventh edition ISBN 978-1-292-15858-7 or sixth edition ISBN 978-0-273-79335-9.

## TITLE OF COURSE: FUNDAMENTAL OF CRYPTOGRAPHY

**COURSE CODE:**

**L-T-P: 0-0-2**

**CREDITS: 1**

**Pre-requisite:** Good knowledge of communication principles and protocols (TCP, IP, ICMP, ARP, etc.) You must have taken at least one communications course before this course. We also recommend that you have taken the course Computer Security which shows how to think regarding security and discusses security issues in a wider perspective. Other relevant courses are Computer Networks and Cryptography which will make some topics easier to understand.

**Introduction:**

Fundamental of Cryptography consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources**.**

**Course Outcomes (CO):**

**CO1:** Have a good understanding of how applications can communicate securely and what tools and protocols exist in order to offer different levels of security

**CO2:** Have detailed knowledge and the ability to critically analyze and design secure networks, applications and systems

**CO3:** Have a fundamental understanding of what makes systems vulnerable and be able to predict new attack methods before they become a reality

**CO4:** Have enough knowledge to evaluate protocols and ability to draw conclusions about the level of security they can offer

**CO5:** Understand what impact the selection of different protocols and security architectures can have to an application or a system

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |
| CO5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | ✓ |

**Course Contents:**
**Experiment 1:** Network Scanning
**Experiment 2:** iptables, the Linux Firewall
**Experiment 3:** Initial Report & Peer-Review
**Experiment 4:** OpenSSL
**Experiment 5:** Network Intrusion Detection
**Experiment 6:** Cryptanalysis of Symmetric Key Ciphers
**Experiment 7:** Asymmetric Key Ciphers
**Experiment 8:** Digital Signatures
**Experiment 9:** Classical Cryptosystems

**Text Books**
1. William Stallings: Cryptography and Network Security, seventh edition ISBN 978-1-292-15858-7 or sixth edition ISBN 978-0-273-79335-9.

**TITLE OF COURSE: Cyber Law, IPR & Ethics**
**COURSE CODE:**
**L-T-P: 3-0-0**
**CREDITS: 3**

**Pre-requisite:** Knowledge is also assumed of basic concepts of Computer networks, Security algorithms and mobile computing.

**Introduction:**
Information has never been so ubiquitous, valuable, or available. However, with the significant growth in information created, stored, processed and transmitted across Information Technology (IT) systems and networks – often of a sensitive or personal nature – comes the need to protect that information from a range of threats. Similarly the infrastructure that we come to rely on in business, government and society – whether it be for communications, utility, public or business service – must be protected from these threats as it is typically controlled by information that is processed and transmitted across IT systems, IT-enabled control systems and networks. The threats can range from professional criminals making their living from stealing information to well- intentioned employees or individuals making mistakes in the way they use applications or IT, or acts of social protest and terrorism. Protecting information along with the IT systems, control systems, networks and devices

processing that information is now recognized as an industry, a profession and an academic discipline in its own right. However, IT systems, control systems, networks, websites and applications are typically designed or built by people who do not give adequate consideration for this need. As a result, IT systems, control systems, networks, websites and applications typically: contain well-known errors; are deployed with well-known default settings that leave the systems open to exploit; and leave the information and organizations they support vulnerable to compromise. This situation has given rise to an acknowledged and growing prevalence of attack, compromise and loss, fuelling recognition for the need to develop cyber security knowledge and skill within the disciplines responsible for networks and IT systems, including within the academic courses that lead or prepare students to pursue a career in these areas. (ISC)2 , the largest not-for-profit membership body of certified information and software security professionals worldwide, with over 100,000 members and The Council of Professors and Heads of Computing (CPHC), brought together a wide-ranging group of industry and academic experts to identify the key concepts related to cyber security that can be embedded across undergraduate computing science and IT-related (e.g. business information systems and IT management for business) degree courses. This guide is the result of this effort, designed to help enrich those computing courses by providing the key cyber security principles and suggested learning outcomes. The concepts covered here are outlined for five themes: information and risk; threats and attacks; cyber security architecture and operations; secure systems and products; and cyber security management, to satisfy Level 4 requirements as stated in The framework for higher education qualifications in England, Wales and Northern Ireland August 2008. Advanced concepts and further learning outcomes are also provided for each theme, so that academic institutions can develop or enhance their courses to meet Level 5 and 6 requirements of the framework. The descriptors for all three levels (4 – 6) are presented in Annex A. They are developed to support accreditation guidelines used by BCS, The Chartered Institute for IT (BCS) and Institution of Engineering and Technology (IET).

**Course Outcomes (CO):**

**CO1:** Q is an organizational asset that has utility, and a value which may be relative depending on the perspective taken, and therefore can be classified to reflect its importance to an organization or individual Q is vulnerable.

**CO2:** why that protection must occur (for example, legal and regulatory drivers, customer rights or organization objectives)

**CO3:** Student able to understand Downloading/copying/extraction of data or extracts any data, Introduction of computer contaminant, or computer virus, Causing damage either to the computer resource or data residing on it, Disruption, Denial of access, Facilitating access by an unauthorized person, Charging the services availed of by a person to the account of another person, Destruction or diminishing of value of information, Stealing, concealing, destroying or altering source code with an intention.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ |
| CO2 | ✓ | ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ |

**Course Contents:**

**Module 1:**
Introduction of Cybercrime: What is cybercrime? Forgery, Hacking, Software Piracy, Computer Network intrusion

**Module 2:** Category of Cybercrime: how criminals plan attacks, passive attack, Active attacks, cyber stalking.

**Module 3:** Cybercrime Mobile & Wireless devices: Security challenges posted by mobile devices, cryptographic security for mobile devices, Attacks on mobile/cell phones, Theft, Virus, and Hacking. Bluetooth; Different viruses on laptop

**Module 4:** Tools and Methods used in Cybercrime: Proxy servers, password checking, Random checking, Trojan Horses and Backdoors; DOS & DDOS attacks; SQL injection: buffer over flow

**Module 5:** Phishing & Identity Theft: Phising methods, ID Theft; Online identity method.

**Module 6:** Cybercrime & Cyber security: Legal aspects, Indian laws, IT act, Public key certificate.

**Text Books:**

1. Cyber security by Nina Gobole & Sunit Belapune; Pub: Wiley India.

**References:**

1. E-Commerce- The cutting edge of business by Kamlesh K. Bajaj, TMH
2. Cyber Law of Information Technology and Internet by Anirudh Rastogi, First Edition
3. Open Source and the Law by Priti Suri & Associates, First Edition

## TITLE OF COURSE: CYBER SECURITY
## COURSE CODE:
## L-T-P: 2-0-2
## CREDITS: 3

**Pre-requisite:** Basic knowledge of computer science. Ethical values are very much required.

**Introduction:**

Computer security, cyber security or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

**Course Outcomes (CO):**

At the end of this course, students will be expected to be able to:

**CO1:** Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures;

**CO2:** Critique and assess the strengths and weaknesses of general cyber security models, including the CIA triad;

**CO3:** Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people;

**CO4:** Assess how all domains of security interact to achieve effective system-wide security at the enterprise level.

**CO5:** Compare the interrelationships among security roles and responsibilities in a modern information-driven enterprise—to include interrelationships across security domains (IT, physical, classification, personnel, and so on);

**CO6:** Assess the role of strategy and policy in determining the success of information security;
**CO7:** Estimate the possible consequences of misaligning enterprise strategy, security policy, and security plans;

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | | | ✓ | | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO5 | ✓ | ✓ | | ✓ | ✓ | | | | | | | ✓ |
| CO6 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO7 | ✓ | ✓ | | ✓ | ✓ | | | | | | | ✓ |

**Course Contents:**

**Module 1: Introduction to Cyber Security**

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

**Module 2: Cyber Security Vulnerabilities and Cyber Security Safeguards**

Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

**Module 3: Securing Web Application, Services and Servers**

Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

**Module 4: Intrusion Detection and Prevention**

Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

**Module 5: Cyber Forensics**

Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling an Investigation, Conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

**Text Books**

1. Jon Erickson, Hacking: The Art of Exploitation (2nd Ed.)

2. Christopher Hadnagy, Social Engineering: The Science of Human Hacking

**References**

1. Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

**TITLE OF COURSE: CYBER SECURITY LAB**
**COURSE CODE:**
**L-T-P: 0-0-2**
**CREDITS: 1**

**Pre-requisite:**

Basic knowledge of computer science. Ethical values are very much required.

**Introduction:**

Computer security, cyber security or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

**Course Outcomes (CO):**

At the end of this course, students will be expected to be able to:

**CO1:** Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures;
**CO2:** Critique and assess the strengths and weaknesses of general cybersecurity models, including the CIA triad;
**CO3:** Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people;
**CO4:** Assess how all domains of security interact to achieve effective system-wide security at the enterprise level.
**CO5:** Compare the interrelationships among security roles and responsibilities in a modern information-driven enterprise—to include interrelationships across security domains (IT, physical, classification, personnel, and so on);
**CO6:** Assess the role of strategy and policy in determining the success of information security;
**CO7:** Estimate the possible consequences of misaligning enterprise strategy, security policy, and security plans;

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | | | | | | | | | ✓ |
| CO2 | ✓ | ✓ | | | ✓ | | | | | | | ✓ |
| CO3 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO5 | ✓ | ✓ | | ✓ | ✓ | | | | | | | ✓ |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO6 | ✓ | ✓ | | ✓ | | | | | | | | ✓ |
| CO7 | ✓ | ✓ | | ✓ | ✓ | | | | | | | ✓ |

**Course Contents:**
**Experiment 1:** Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
**Experiment 2:** Study the steps to protect a Microsoft Word Document of different version with different operating system.
**Experiment 3:** Study the steps to remove Passwords from Microsoft Word
**Experiment 4:** Study various methods of protecting and securing databases.
**Experiment 5:** Study "How to make strong passwords" and "passwords cracking techniques".
**Experiment 6:** Study the steps to hack a strong password.
**Experiment 7:** Study of the features of firewall in providing network security and to set Firewall Security in windows.
**Experiment 8:** Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
**Experiment 9:** Study of different types of vulnerabilities for hacking a websites / Web Applications.
**Experiment 10:** Analysis the Security Vulnerabilities of E-commerce services.
**Text Books**
1. Jon Erickson, Hacking: The Art of Exploitation (2nd Ed.)
2. Christopher Hadnagy, Social Engineering: The Science of Human Hacking

**References**
1. Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

## TITLE OF COURSE: DIGITAL FORENSICS
## COURSE CODE:
## L-T-P: 3-0-0
## CREDITS: 3

Pre-requisite:
Basics of computer science

**Introduction:**
- Describe digital forensics and relate it to an investigative process.
- Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

**Course Outcomes (CO):**
Upon completion of this course:

**CO1:** Students will explain and properly document the process of digital forensics analysis.
**CO2:** Students will gain an understanding of the tradeoffs and differences between various forensic tools.
**CO3:** Students will be able to describe the representation and organization of data and metadata within modern computer systems.
**CO4:** Students will understand the inner workings of file systems.
**CO5:** Students will be able to create disk images, recover deleted files and extract hidden information.
**CO6:** Students will be introduced to the current research in computer forensics. This will encourage them to define research problems and develop effective solutions.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | ✓ | | | ✓ | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | | | ✓ | | | | | | | ✓ |
| CO5 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO6 | ✓ | | ✓ | ✓ | | ✓ | | | | | | ✓ |

**Course Contents:**
**Module-1:**
Introduction to legal issues, context, and digital forensics.
**Module-2:**
Media Analysis: disk structure, file systems (NTFS, EXT 2/3, HFS), and physical layer issues.
**Module-3:**
Live Collection, Analysis Techniques: keyword searches, timelines, hidden data.
**Module-4:**
Application Analysis, Network Analysis, Midterm, Analysis of Cell phones, PDAs, etc.
**Module-5:**
Binary Code Analysis (Guest lecturer: Alex Berry), Evidence: collection, preservation, testimony Legal Community Panel, Research Challenges.
**Module-6:**
TBD, Project Presentations.

**Text Books**
1. Darren R. Hayes, A Practical Guide to Digital Forensics Investigations)
2. The Best Damn Cybercrime and Digital Forensics Book Period 1st Edition by Jack Wiles, Anthony Reyes, Jesse Varsalone

**References**
1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics 2nd Edition

by John Sammons
2. Cyber Security by Jocelyn O. Padallan

**TITLE OF COURSE: CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS TOOLS**
**COURSE CODE:**
**L-T-P: 3-0-0**
**CREDITS: 3**

**Pre-requisite:** Basic concepts in cyber law or digital forensic.

**Introduction:**
This course examines Cyber Crime Investigation and Digital Forensics basics. The Topics to be covered (tentatively) include: an introduction to Cyber Crime, Cyber Criminology, Information Security, Sociological and Criminological Perspectives, Current Computer Forensics Tools.

**Course Outcomes (CO):**
In this course we will study the basic components of Cyber Crime. Students are expected to be capable of understanding the Cyber Crime Investigation and Digital Forensics basics, their advantages and drawbacks, how their drawbacks can be overcome and what the applications are and where they can be used. To reach this goal, the following objectives need to be met:

**CO1:** Students would be able to know Cyber Crime Investigation properly.
**CO2:** Students would be able to know Digital Forensics basics.
**CO3:** By analyzing the logic of any case, students would be able to define cyber world.
**CO4:** To become an efficient cyber expert.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | | | ✓ | | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |

**Course Contents:**
**Module-1:** Principles and Concepts of Cyber Criminology – Crime, Tort, Misdemeanour, Cyber Space, Cyber Crime, Cyber Criminology, Information Security, Penetration Testing, Incident Response, GRC, etc.- Conventional crimes vs. Cyber Crimes.
**Module-2:** Contemporary Forms of Crimes - White Collar Crimes, Economic Offences, Organized Crimes, Terrorism, Crime and Media and other contemporary forms of crimes.
**Module-3:** Psychology of Cyber Criminals – Types of Cyber Criminals – Modus Operandi of Cyber Criminals – Profiling of Cyber Criminals - Tools and Techniques adopted by Cyber Criminals – Psychological theories relating to cyber criminals.
**Module-4:** Cyber Crime– Sociological and Criminological Perspectives – Causes of Cyber Crimes - Criminological Theories and Cyber Crime – Routine Activity Theory, Social Learning Theory,

Differential Association Theory, Differential Opportunity Theory, Media and Crime and latest theories and other related theories.

**Module-5:** The Role of Criminal Justice Administration and Cyber Crimes

Police Organizational structure of Police in India – Different wings in the States and Districts and their functions - Police & Law Enforcement – F.I.R. cognizable and non-cognizable offences, bailable and non-bailable offences – arrest , search, seizure – Interrogation of suspects and witnesses – charge sheet Cybercrime cells – structure & investigation of cybercrime cases .

Judiciary - Different types of courts – Cyber Appellate Court / Tribunals / Powers Proceedings in the court before trial, after trial, plea of guilty, sentencing.

The Role of N.G.O.s in the Prevention of Cyber Crimes, The Role of Victims of Cyber Crimes in the Criminal Justice Administration Crime Prevention Crime and sense of security - Social control and crime prevention Community and crime prevention Contemporary crime prevention strategies.

**Module-6:** Digital forensic: Computer forensics and investigations as a profession, understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, understanding case laws, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations, Following the legal process, understanding corporate investigations, establishing company policies, Displaying warning Banners.

**Module-7:** Current Computer Forensics Tools: Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Tool Comparisons, Other Considerations for Tools, Computer Forensics Software Tools, Command-Line Forensics Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools, Forensic Workstations, Using a Write-Blocker.

**Module-8:** Identification of data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks ,Router Forensics. Cyber forensics tools and case studies.

**Text Books**

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Fourth Edition, Course Technology.

**References**

1. Angus M.Marshall, “Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008

## TITLE OF COURSE: APPLIED & QUANTUM CRYPTOGRAPHY
## COURSE CODE:
## L-T-P: 3-0-0
## CREDITS: 3

**Pre-requisite:** Basic concepts in Applied & Quantum Cryptography.

**Introduction:**

This course examines Applied & Quantum Cryptography. The Topics to be covered (tentatively)

include: an introduction to Quantum Physics, Qubits, Quantum cryptography, Quantum Logic.

**Course Outcomes (CO):**
In this course we will study the basic components of cryptography. Students are expected to be capable of understanding the quantum cryptography, their advantages and drawbacks, how to implement them in python, how their drawbacks can be overcome and what the applications are and where they can be used. To reach this goal, the following objectives need to be met:

**CO1:** Students would be able to design & implement any cryptography properly.
**CO2:** Students would be able to implement any problem by writing their own algorithm.
**CO3:** By analyzing the logic of any algorithm, students would be able to write efficient program.
**CO4:** To become an efficient programmer.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | | | ✓ | | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |
| CO4 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |

**Course Contents:**
**Module-1:** Quantum Physics: Brief introduction to quantum physics and its importance in the microcosm world. The historical motivation is given and deepens especially in the wave-particle duality. The postulates of quantum physics are introduced, with special emphasis on the Schrödinger equation and the probabilistic nature of the measure. The solution to the Schrödinger equation for a potential well of infinite-dimensional is presented. The example contains all the basic ingredients for understanding the stationary states and also the superposition of states, which will have a prominent role for the description of quantum bits.
**Module-2:** Qubits: Systems of two states: quantum bits (qubits). The basic operations through Kets and bras are introduced, the brackets as scalar products, superpositions of base's states.
**Module-3:** Quantum cryptography. The basic principles of quantum cryptography are outlined. Protocols that use entanglement, such as Eckert's one and others, based on the measure's postulate such as BB84 and B92.
**Module-4:** Quantum Logic. Gates and simple quantum algorithms.
A description is given of:
a) The temporal evolution of the qubits is given in terms of unitary operators and their connection with quantum logic gates.
b) The minimal set of quantum logic gates that allows any computation performed on any system implying an arbitrary number of qubits.
c) Quantum gate diagrams, as a flowchart of the computation.
d) The evaluation of quantum functions, implemented by unitary operators.
e) Simple quantum algorithms of academic interest are worked out: Deutsch, Deutsch-Jozsa and Vazirani.
**Module-5:** Grover algorithm about finding elements of an unstructured database. Unstructured

database, known as Grover's algorithm, which is able to locate it with an efficiency that scales as square root of N, N being the total number of items in the database.

**Module-6:** Shor's factoring algorithm: From the foundations of the classical RSA encryption's algorithm, the Shor's quantum factoring algorithm is introduced. A detailed description is given, distinguishing those parts of the purely classical algorithm, requiring concepts of number theory, modular arithmetic and continuous fractions, from the quantum part, which uses the principle of superposition and quantum Fourier transform to extract the period of a periodic function, from which one can deduce the factors of the number to be factorized.

**Text Books**

1. "Applied Quantum Cryptography", Editors: Kollmitzer, Christian, Pivk, Mario (Eds.)

**References**

1. "Post-Quantum Cryptography" 2009th Edition, by Daniel J. Bernstein (Editor), Johannes Buchmann (Editor), Erik Dahmen

## TITLE OF COURSE: INTRUSION DETECTION AND PREVENTION SYSTEM

**COURSE CODE:**
**L-T-P: 3-0-0**
**CREDITS: 3**

**Pre-requisite:** Basic concepts in Intrusion Detection and Prevention System.

**Introduction:**

This course examines basics Intrusion Detection and Prevention System. The Topics to be covered (tentatively) include: an introduction to History of Intrusion detection, Audit, Network IDs protocol, Snort Installation Scenarios.

**Course Outcomes (CO):**

In this course we will study the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets. Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.

**CO1:** Students would be able to know Intrusion Detection and Prevention System.
**CO2:** Students would be able to implement any Network IDs protocol by their own algorithm.
**CO3:** By analyzing the logic of any algorithm, students would be able to write efficient program.
**CO4:** To become an efficient network administrator.

**Mapping of Course Outcomes (CO) and Program Outcomes (PO):**

| CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |
| CO2 | ✓ | | | ✓ | | | | | | | | ✓ |
| CO3 | ✓ | ✓ | ✓ | | | | | | | | | ✓ |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO4 | ✓ | ✓ | ✓ | | ✓ | | | | | | | ✓ |

**Course Contents:**

**Module-1:** History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

**Module-2:** Intrusion Prevention Systems, Network IDs protocol based IDs, Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

**Module-3:** Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes.

**Module-4:** Working with Snort Rules, Rule Headers, Rule Options, the Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL

**Module-5:** Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

**Text Books**

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003.

**References**

1. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.

2. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.

3. Stephen Northcutt, Judy Novak: "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002.

4. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". 6th Edition, KhannaPublihsers, 2012.