Master of Technology Programme
in
Computer Science and Engg
with specializations
in
Data Sciences
and in
Information Security

Indian Institute of Technology Jammu
and
Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar

Supported by :
R C Bose Center for Cryptology and Information Security,
Indian Statistical Institute, Kolkata
Prelude:

Information-centric digital society needs to exploit data to bring in (i) transparency, (ii) fairness, (iii) accuracy, and (iv) confidentiality in transforming unstructured data to information (and knowledge) for information mining and decision-making. With the increasing volume of data, organizations are getting more and more interested in unravelling the unintuitive trends that lay hidden within the data. These trends can be connected with valuable business insights that are usable in every department, be it marketing or product development or design. Evidence-based decision making has established itself. Various levels in business have to answer different questions as their company evolves, identify common threads across a multitude of similar questions and the right tools for the right question.

Data science is used in business functions such as strategy formation, operational processes, and decision making. It is important to understand that finding patterns within data has to be backed by deep domain knowledge. In other words, insights that are interesting, but do not lead to actionable information, cannot be considered as of any value from the data science perspective. Data scientists help an organization, define the way they collect and treat data. Top companies, such as Google, Facebook, Microsoft, and Baidu are driving research further in this direction with their strong artificial intelligence R&D teams.

A complementary set of areas are knowledge management, data management, data security, and interaction design. As the need to infer insightful inference from the data grows, so is the requirement to share the data across cross-section of the users increases. However, it is equally essential to ensure the security and privacy of the data with increasing sharing. That is, a tradeoff between data availability, usability and its security and privacy needs to be maintained. However, the big challenge today is the low skill adoption rate compared to the growth in technology. In other words, there is a huge shortage of data scientists and information security analysts. Hence, industry and academia need professionals with sound knowledge in data science and information security.

To address the mounting need of high-skilled professionals in these two areas, IIT Jammu and DA-IICT, Gandhinagar with patronage from the RC Bose center, ISI, Kolkata are proud to announce a new postgraduate program - MTech in Computer Science with Specialization in (i) Data Science (CS-DS), and (ii) Information Security (CS-IS). The degree would be conferred by IIT-Jammu while students spend their study semester across the three institutes, depending upon how their research interests align with the research expertise at these three institutes. Specifically, the students are expected to study their first semester at IIT Jammu, the second at DA-IICT, Gandhinagar. Depending on the nature and need of their dissertation or project, the students would continue their third semester and fourth semester either in DA-IICT, or IIT-Jammu, or at RC Bose center of ISI, Kolkata.

The USP of this MTech in CS-DS and CS-IS is that faculties having rich experience and strong research background will teach and mentor the students of the new postgraduate program. The research areas of the faculties of these three institutes span from topics directly associated with data science and information security, such as Bayesian Learning, Estimation, Data Analytics, Natural Language Processing, Information Retrieval, Deep Learning, Statistical Methods, Optimization Techniques, Computer Security and Privacy, Cryptography, Coding Theory, Data Mining, and Bioinformatics.

Current trends in industry and academia:

Prediction analytics on the Cloud: Many leading companies such as IBM, Microsoft, Google, and Amazon, are moving their data and applications to the cloud. This process is
driven by increased collaboration and flexibility, as well as reducing the complexity of administration and configuration of computing resources. In addition, the majority of the top cloud providers developed their own offering of Machine Learning services in a cloud (MLaaS and AIaaS). This step allows organizations to leverage machine learning technology, without massive investments and needs to employ large data science teams. Hence, now we are observing consumerization of predictive analytics technologies, that is supported by those cloud prediction services. Hadoop and Spark big data platforms

The steady growth of Big Data technologies like Hadoop and Spark has made it possible to collect vast amount of data, and then distribute the data to low-cost servers running in parallel. Apache Spark, on the other hand, is one of the fastest growing big data platforms which uses in-memory computation.

**Data Security** The increasing number of cyber-attacks is the reason for rising attention to the question of data security, which became more relevant in recent years. It is expected that security analytics costs will raise up. Thus, it is critical to keep up with new trends in the field of data security. One of the recent trends in security is increased usage of the machine learning algorithm, including deep learning for detection of anomalies and other fields of data science security in various business domains. Another noticeable trend of security data science is the utilization of AI conversational interfaces (a.k.a. bots) for automation of assistance and security responses to emerging threats. Such bots have been already deployed on several platforms like Slack.

Nowadays one of the quickly developing areas is behavioural biometrics. It can be used standalone, but in combination with ML, we should expect faster results that should reduce the costs and improve efficiency. It can be used to identify the persons on the other end and what they’re trying to do as well as distinguish a user from the robot. In future, there may occur new types of attacks, and thus the requirements for cybersecurity are getting more complicated, and security specialists will need to adapt to the new threats.

**Deep Learning** Deep learning gets a lot of attention in recent years, as many noticeable results were achieved by using it for many important applications, such as machine translation and other forms of language processing, Automatic Image Caption Generation, Object Classification and Detection in Images, Facial Recognition and Automatic Game Playing. For data scientists, Deep Learning will be one of the most important approaches for solving machine learning problems. Furthermore, deep learning is becoming widely available now, because of the increased computing power and accessibility of this technology through various open-source frameworks, such as TensorFlow, pyTorch, and Keras.

**Career opportunities**

There can be broadly four types of career options in data science and information security:

**Data Analyst/Data Scientist:** The talents and skills needed for this role are diverse and encompass the entire spectrum of the data science process. Companies like IBM, HP, and others have a huge pool of data analyst jobs and are looking for skilled analysts to do these jobs. As a data scientist, one gets to master a whole new range of skills and talents going from being able to handle the raw data, analyze that data with the help of statistical techniques to sharing the insights with the organization in a compelling way. The data scientist jobs are highly in demand within companies like Google, Microsoft, and Facebook. They differ from data analysts in that while data analysts should have familiarity with data warehousing and business intelligence concepts.
**Business Analyst:** The work of a business analyst is not technically oriented. A business analyst must have a deep understanding of the complex business functions to be successful in their field. A business analyst needs to study the skill of linking actionable business insights to data insights and should be able to use storytelling methods to spread information across the entire company. If you have a good understanding of business and technology then this is the perfect job for you. Companies with the need for business analysts are diverse and active in very different industries. Organizations that have major business analyst positions are Dell, Oracle, and Uber.

**Data Security Analyst:** The responsibilities of a security analyst include analyzing detection alerts. There are multiple operations that involve investigating alerts of potential compromises. Some of the day-to-day analysis that one deals with are, as examples, *what IP addresses did this machine talk to between times A and B?* OR, *How often does this user access this website?*. The duties are to make investigations and alerts faster and more accurate, developing new alerts, improving the fidelity of existing alerts, improving the investigative tools, extending detection to new platforms like cloud, and more. The final end-goal is to come up with extremely high fidelity coverage of every attack vector with zero human effort. Other responsibilities include security assessments, malware analysis, intrusion detection, threat intelligence, forensics and more.

**Program Objectives**

Based on the four types of career options, as detailed in the previous section, the program objectives are aligned as follows:

**M.Tech with specialization in Data Science:** The objective of the Data Science (CS-DS) program is to enable students to apply Machine learning and Data analysis scheme to solve real-life problems. The course will help them develop Statistical Analysis techniques necessary for tackling such problems. Students will be able to analyze the vast amount of data to cater to the efficient utilization of the Industrial data.

**M.Tech with specialization in Information Security:** The objective of the Information Security (CS-IS) program is to train students to become information security professionals who can handle the real-life problems and challenges in cybersecurity in the context of big data. Students will be exposed to various techniques and algorithms related to security analytics, cybersecurity, alert analytics, intrusion detection, malware analytics, and related areas.

**Program Outcomes**

**M.Tech with specialization in Data Science:** At the end of the Data Science (CS-DS) program,

- the students will be able to apply the knowledge of Artificial Intelligence and Machine Learning tools and techniques in the field of Big Data for solving real-world problems.
- the students will learn modelling techniques, key statistical principles, data handling techniques, and will get hands-on experience with large-scale data.
- the students will be able to demonstrate the knowledge and understanding of engineering and management principles in the area of Computer Science and Engineering to manage projects in a multidisciplinary environment.
M.Tech with specialization in Information Security: At the end of the Information Security (CS-IS) program,

- the students will be able to apply the knowledge of security attacks, mechanisms and attributes to understand the importance of information security in real-world applications.

- the students will be able to analyze the security strength of an organization’s information management system, identify the vulnerabilities and suggest solutions to ensure prevention of malicious information access.

- the students will be able to gain knowledge of the functioning of the firewalls and other mitigation mechanisms.

- the students would be able to design security software to prevent malicious information access.

- the students would be able to incorporate security in the software development life cycle to be able to design inherent secure solutions as compared to security solutions designed as an afterthought.
# Semester-wise Credit Distribution

<table>
<thead>
<tr>
<th>Semester</th>
<th>Credits</th>
<th>Hours/week</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>16</td>
<td>19</td>
</tr>
<tr>
<td>II</td>
<td>16</td>
<td>21</td>
</tr>
<tr>
<td>III</td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td>IV</td>
<td>14</td>
<td>42</td>
</tr>
<tr>
<td><strong>Total Credits</strong></td>
<td><strong>58</strong></td>
<td><strong>-</strong></td>
</tr>
</tbody>
</table>
# M.Tech. Program

## Semester-wise Distribution of the Courses

### Convention for Course Coding:
- CSPL 1XX: Institute Core course, theory
- CSPL 2XX: Data Science Specialization Core
- CSPL 3XX: Information Security Specialization Core
- CSPL 41X: Elective I - Data Science
- CSPL 42X: Elective II – Data Science
- CSPL 51X: Elective I – Information Security
- CSPL 52X: Elective II – Information Security
- CSPL 6XX: Elective III – Data Science or Information Security
- CSPP 701: Thematic Seminar
- CSPP 9XX: Project or Dissertation Preliminaries and Preliminaries

## Semester-I : At IIT Jammu

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CSPL 100</td>
<td>Linear Algebra/Abstract Algebra(^1)</td>
<td>(3-1-0)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CSPL 101</td>
<td>Probability and Statistics</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>CSPL 102</td>
<td>Design and Analysis of Algorithms</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>CSPL 201/301</td>
<td>Specialization Core</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Data Organization and Retrieval (DS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IS : Introduction to Computer Systems (IS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CSPP 103</td>
<td>Software Tools</td>
<td>(0-0-1)</td>
<td></td>
</tr>
</tbody>
</table>

Total Credits with 12 hours of lectures, 1 tutorial and 6 hours of lab per week 16

1 lab credit = 2 hours, 1 lecture credit = 1 hour

\(^1\)The students opting for DS specialization must study Linear Algebra and the students opting for IS specialization must study Abstract Algebra.
### Semester-II: At DAIICT, Gandhinagar

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CSPL 202/302</td>
<td>Specialization Core</td>
<td>(3-0-1)/(3-1-0)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DS: Pattern Recognition and Machine Learning (3-0-1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IS: Modern Cryptography (3-1-0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CSPL 203/303</td>
<td>Specialization Core</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DS: Bigdata and Large-Scale computing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IS: Information Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CSPL 41X/51X</td>
<td>Elective-I</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>CSPL 42X/52X</td>
<td>Elective-II</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>CSPL 104</td>
<td>Communication skills and Technical Writing</td>
<td>(1-0-2)</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Credits (13 hours of lectures 1 hour of tutorial and 6/8 hours of lab per week) 20

### Semester-III : IIT Jammu/DA-IICT/ISI Kolkata

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CSPL 6XX</td>
<td>Elective-III</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CSPP 701</td>
<td>Thematic Seminar</td>
<td>(0-0-2)</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>CSPP 911/921</td>
<td>Project/Dissertation Preliminaries</td>
<td>(0-0-6)</td>
<td>6</td>
</tr>
</tbody>
</table>

Total Credits (3 hours of lectures and 27 hours of lab per week) 12

### Semester-III : IIT Jammu/DA-IICT/ISI Kolkata

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CSPP 912/922</td>
<td>Dissertation</td>
<td>(0-0-14)</td>
<td>14</td>
</tr>
</tbody>
</table>

Total Credits (42 hours of lab per week) 14
### Pool of Electives

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Elective I for DS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>CSPL 411</td>
<td>Optimization Techniques</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CSPL 412</td>
<td>Information Visualization</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CSPL 413</td>
<td>Information Retrieval</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Elective II for DS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CSPL 421</td>
<td>Computational Numerical Methods</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>CSPL 422</td>
<td>Brain and Cognitive Sciences</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>CSPL 423</td>
<td>Speech and Audio Processing</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Elective I for IS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>CSPL 511</td>
<td>Computational Number Theory</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CSPL 512</td>
<td>Secure Software Engineering</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>CSPL 513</td>
<td>Distributed Systems</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Elective II for IS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CSPL 521</td>
<td>Blockchain and Cryptocurrencies</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>CSPL 522</td>
<td>Security Protocols</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>CSPL 523</td>
<td>Multimedia Security and Forensics</td>
<td>(3-0-0)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Elective III</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>CSPL 601</td>
<td>Quantum Cryptography</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>CSPL 602</td>
<td>Machine Learning for Security</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>CSPL 603</td>
<td>Social and Legal Aspects of Computer Security</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>CSPL 604</td>
<td>Security in Resource Constrained Environments</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
</tbody>
</table>

*The electives actually offered at any point in time is subject to availability of the appropriate expertise in the faculty members at a particular institute.*
<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Total Credits (L-T-P)</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>CSPL 605</td>
<td>Selected Topics in Security and Privacy</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>CSPL 606</td>
<td>Network Security</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>CSPL 607</td>
<td>Application Security</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>14</td>
<td>CSPL 608</td>
<td>Computer Vision</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>CSPL 609</td>
<td>Deep Learning</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>CSPL 610</td>
<td>Advanced Business Analytics</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>CSPL 611</td>
<td>Natural Language Processing</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>CSPL 612</td>
<td>Human Computer Interaction</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>CSPL 613</td>
<td>Parallel Computing</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>CSPL 614</td>
<td>Recommender Systems</td>
<td>(3-0-1)</td>
<td>4</td>
</tr>
</tbody>
</table>
Courses of Study: Syllabus, Course Abstracts and Course Outcomes

1 Linear Algebra:
This course is about teaching basics of linear algebra including vector spaces, matrix algebra, linear transformations, eigenvalues and eigenvectors, orthogonality, properties of symmetric matrices, positive definite matrices, and SVD. The course is developed with an aim to provide a strong foundation in linear algebra which will be used in the subsequent curriculum by both the specialization of DS and IS students. The course also attempts to increase the mathematical maturity of students by introducing proofs and mathematical rigour.

Indicative Topics of Study:
- Inner products: norms, orthogonal bases and Gram-Schmidt orthogonalization; Matrix Multiplication Problems, Matrix Analysis, Gauss Elimination Technique, LU and LDU Decomposition methods, Diagonalization of a Matrix, Singular value decomposition.
- Linear transformations: Kernel and range, inverse transformations, matrices of linear transformations, change of basis, similarity; Orthogonalizations and Least Squares, Parallel Matrix Computations, Unsymmetrical Eigenvalue problem, Symmetric eigenvalue problem, Iterative methods for linear systems, Lanczos methods.

References:

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Compute the RREF, Inverse, of a matrix, solution in vector form of a linear system (homogeneous or non-homogeneous), Dimension, Complementary subspace of a vector space/subspace, Dimension and basis for the fundamental subspaces of a matrix, Matrix of a given linear transformation/operator, Change of basis matrix and matrix of an operator after change of basis, Determinant and characteristic equation of a given matrix, Eigenvalues and eigenvectors of a matrix/operator (real and complex), Orthogonal basis for a given basis using the Gram-Schmidt process, Orthogonal complement for a given subspace, Diagonalized matrix for a given matrix/operator (including symmetric matrices), SVD decomposition of a given matrix, QR decomposition of a given matrix.
- Test/classify for the given relation, set, subset, vectors, function, matrix.
- Use computational techniques and algebraic skills essential for the study of systems of linear equations, matrix algebra, vector spaces, eigenvalues and eigenvectors, orthogonality and diagonalization.
- Use visualization, spatial reasoning, as well as geometric properties and strategies to model, solve problems, and view solutions, especially in R2 and R3, as well as conceptually extend these results to higher dimensions. (Geometric Skills).
- Critically analyze and construct mathematical arguments that relate to the study of introductory linear algebra. (Proof and Reasoning).
- Use technology, where appropriate, to enhance and facilitate mathematical understanding, as well as an aid in solving problems and presenting solutions (Technological Skills).
Communicate and understand mathematical statements, ideas and results, both verbally and in writing, with the correct use of mathematical definitions, terminology and symbolism (Communication Skills).

2 Abstract Algebra:
It is a well-known fact that algebraic structures play a vital role not only in pure mathematics but also in many areas of computer science such as cryptology and information security etc. This course will introduce the algebraic structures such as groups, rings and fields. The fundamental properties of these structures shall be discussed in a greater detail and some applications of these structures may also be outlined from time to time. Moreover, abstract algebra helps in writing rigorous proofs of mathematical results and enhances problem solving skill.

Indicative Topics of Study: Preliminaries: Sets, functions, equivalence relations and partitions, mathematical induction.
Groups: Elementary properties, subgroups, cosets, Lagrange’s theorem, Euler’s theorem, Fermat’s theorem, normal groups, quotient groups, cyclic groups, finite cyclic groups and their properties, homomorphism and isomorphism, Isomorphism theorem, permutation groups, Sylow’s theorem and application.
Rings and Fields: Rings, units and zero divisors. Ideals and quotients, principal ideals, prime ideals, maximal ideals, integral domain, PID, Euclidean domain, UFD, Euclidean algorithm for GCD, extended Euclidean algorithm, finding modular inverse of an integer, Chinese Remainder Theorem (CRT), Euler’s Phi-function, quadratic residues, fields and field extensions, algebraic extensions, splitting fields.

References:

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:

- Verify (or identify) if a given algebraic structure is a group, ring or field.
- Analyze if the two groups are isomorphic.
- Classify groups up to isomorphism.
- Verify if a group is cyclic.
- Computer generators of finite cyclic groups.
- Analyze if a given ideal in a ring is prime ideal or maximal ideal.
- Verify if a given integral domain is PID or UFD or ED.
- Computer splitting field of a given polynomial of small degree over field of rational numbers.
- Understand various properties of finite fields.
- Construct finite fields.
• Check if a given polynomial is irreducible over a finite field.
• Check if a given polynomial is primitive over a finite field.
• Write down formal mathematical proofs.

3 Probability and Statistics:
This course is about enabling the learner to acquire knowledge required to build algorithms for machine learning, data science and information security. A student must have knowledge about Bayes theorem (conditional probability), random variable, discrete and continuous distribution, Joint distribution function, marginal and conditional distributions, expectation, covariance, law of large numbers, central limit theorem.

Indicative Topics of Study: Introduction to Probability, conditional Probability, Bayes' theorem; Random variables, Analysis of discrete and continuous random variables. Probability distributions, distribution functions, mean and variance of random variables, standard discrete and continuous distributions and their properties. Analysis of Joint Probability Distributions of discrete and continuous random variables, Two or more random variables, joint, marginal and conditional probability distributions, independence of random variables. Covariance and correlation, Linear functions of random variables, several functions of random variables. Point estimation of Parameters and Sampling distributions: Central limit theorem, General concepts of point estimation, Methods of point estimation, method of moments, method of maximum likelihood. Bayesian estimation of parameters, Interval estimation, Confidence interval for the mean and variance of a normal population, large sample confidence interval for population proportions. Hypothesis Testing, general concepts, tests on mean and variance of one and two normal populations, tests on population proportion, testing for goodness of fit and independence; Introduction to nonparametric statistics, sign test, Wilcoxon signed rank test, Wilcoxon rank sum test.

References:

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Acquire the knowledge about the fundamental problems of probability along with problems related to use of random variables and their distribution.
• Learn the modelling and analysis of data using probability distribution
• Analyze the dependence of random variables in the sense of correlation and regression
• Understand data parameter estimation and test of hypotheses.

4 Design and Analysis of Algorithms:
In this course, the students would learn about the design and the analysis of the algorithms. Algorithms are the soul of computing. Algorithmic thinking is akin to creating "recipes" (well defined sequences of computational steps) for getting "things" (computational problems specifying an input-output relation) "successfully" (correctly) "done" (in finite steps and time). This course introduces basic methods for the design and analysis of efficient algorithms emphasizing methods useful in practice. Different algorithms for a given computational task would be
presented and their relative merits evaluated based on performance measures. The following important computational problems will be discussed: sorting, searching, elements of dynamic programming and greedy algorithms, advanced data structures, graph algorithms (shortest path, spanning trees, tree traversals), string matching, elements of computational geometry, NP completeness.


**References:**
1. Cormen, Leiserson, Rivest, Stein:” Introduction to Algorithms”, the MIT Press.
Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:

- Argue the correctness of algorithms using inductive proofs and invariants. Analyze worst-case running times of algorithms using asymptotic analysis.
- Identify the most appropriate algorithm design technique required to solve a given problem. Use either Divide-and-conquer paradigm, Greedy, Dynamic programming, Branch-and-Bound or Backtracking design techniques to design an algorithm.
- Analyze the time complexity and specify them using asymptotic notations. Derive and solve recurrences describing the performance of divide-and-conquer algorithms.
- Analyze randomized algorithms (expected running time, probability of error). Employ indicator random variables and linearity of expectation to perform the analyses. Recite analyses of algorithms that employ this method of analysis. Understand the difference between a randomized algorithm and an algorithm with probabilistic inputs.
- Analyze algorithms using amortized analysis wherever applicable. Describe the different methods of amortized analysis (aggregate analysis, accounting, potential method).
- Understand the limitations of algorithmic computing with respect to bounds on time.
- Understand non-determinism. Design non-deterministic algorithms. Given a problem to solve, analyze whether it can be solved in polynomial time or exponential and how to deal with those that cannot be proven to run in polynomial time. Being able to classify problems.
- Solve those problems that lie beyond the limits of available computational power, using appropriate techniques.

5 Data Organization and Retrieval:
The course explores the issues surrounding the creation, distribution and use of information objects and representations of those objects. Exploration of theoretical issues will center on understanding organization structures, uses and implications for information systems. During this process the students would learn about representation of information using metadata schema and ontologies, Structured, semi-structured and unstructured information storage and retrieval systems. Information Retrieval systems covering different representation and retrieval techniques will be explored.

References:
1. Crestani, Fabio, Mounia Lalmas, Cornelis J. Van Rijsbergen, and Iain Campbell.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- To be familiar with the concepts, issues and methods related to organization and management of physical and digital information.
- To become familiar with the representation and classification of information through cataloguing, metadata creation, indexing and organization.
- To understand the role of information structures and objects in information systems.
- To develop skills for analyzing and processing unstructured data.

6 Introduction to Computer Systems:
The Introduction to Computer Systems course provides a programmer’s view of how computer systems execute programs, store information, and communicate. It enables students to understand better the concept of a stored program, the functions of an operating system and the network protocols that a modern computer system invariably uses. The course is aimed to serve as a foundation for courses on information security, compilers, networks, operating systems, and computer architecture, where a deeper understanding of systems-level issues is required. The course is aimed to make a student become more effective programmer, especially in dealing with issues of performance, portability and robustness. The topics covered include: machine-level code and its generation by optimizing compilers, performance evaluation and optimization, computer arithmetic, memory organization and management, operating system and its functional components, networking technology and protocols, and supporting concurrent computation. The course also introduces students to the basic concepts of Information Security viz. the Security Attributes, Mechanisms and the Attacks as per the ITUT’s X.800 recommendation, the Security Model, the notion of the unconditional vs the computational security and the encryption using the Classical Ciphers.


References:

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Explain common bit-level representations of numeric values (unsigned, twos complement, floating point) and the consequent mathematical properties of arithmetic and bit-level operations on them.
- Recognize the relation between programs expressed in C and in assembly code, including the implementation of expressions, control, procedures, and data structures.
- Demonstrate ability to understand basic intention of a program through its binary representation and apply these skills to debugging programs.
- Investigate the programmers interaction with the underlying system through the different APIs and abstractions, including system support for process and thread control, virtual memory, and networking.
- Demonstrate ability to understand the functional components in a typical TCP/IP network protocol stack.
- Analyze the packets at various layers of the TCP/IP protocol suite, with respect to different fields in the headers at each layer.
- Analyze the consequences of imperfect system usage, such as poor memory and CPU performance, crashes, and security vulnerabilities.
- Apply tools, both standard and self-developed, that will aid program development, including compilers, code analyzers, debuggers, consistency checkers, and profilers.
- Apply these analytic and tool-use abilities to create reliable and efficient programs exercising the different components of a modern computing system.
- Analyze the security attributes required given an application scenario.
- Computer the ciphertext given plaintext and a key using any of the Classical Symmetric Key Encryption ciphers.

7 Software Tools:
This course is about introducing the students on various software tools required for facilitating the research and the development of the software. The indicative tools that students would work hands on with, are as follows: gnuplot, matplotlib, RStudio, MATLAB, Scripting Languages (Python, Linux Shell scripts), and One or more of Continuous Integration/Continuous Development tools like Jenkins, TeamCity, TravisCI, GoCD, Gitlab CI, CircleCI, Codeship.
**Indicative Topics of Study:** Study and Practice of Software Tools e.g. gnuplot, matplotlib, RStudio, MATLAB, Scripting Languages (Python, Linux Shell scripts), and One or more of Continuous Integration/Continuous Development tools like Jenkins, TeamCity, TravisCI, GoCD, Gitlab CI, CircleCI, Codeship.

**References:**
1. As prescribed by the instructor.

**Course Outcomes:** Students who complete the course will have demonstrated the ability to do the following:
- For making graphs from data/results: gnuplot, matplotlib, RStudio, Excel, MATLAB, etc.
- For collaborative documentation, research papers and source codes in addition to version control: e.g. Github and Gitlab
- Use the Scripting Languages Python, Linux Shell scripts.
- Use one or more of Continuous Integration/Continuous Development tools like Jenkins, TeamCity, TravisCI, GoCD, Gitlab CI, CircleCI, Codeship.

**8 Pattern Recognition and Machine Learning:**
Machine learning concerns with designing and developing of algorithms that allow machines, essentially computers, to evolve realistic or human like behavior based on the empirical data available. This course aims to discuss the building blocks of pattern recognition problem and provide an overview of the machine leaning and advance topics. The focus would be to discuss various algorithms for pattern recognition and discuss the tools for pattern recognition too.

References:
1. R.O.Duda, P.E.Hart and D.G.Stork, Pattern Classification, John Wiley.
3. C.M.Bishop, Pattern Recognition and Machine Learning, Springer.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Understand the fundamental problems of pattern recognition and relevant algorithms to deal with real life data such as supervised and unsupervised algorithms
- Understand the modelling and analysis of data using statistical and mathematical models that are fitted to the data
- Study various issues involved in machine learning for categorical and numerical data

9 Modern Cryptography:
The objective of the course is to focus on models and proofs of security for different cryptographic primitives used in various applications. The coverage of this course includes pseudorandom functions, symmetric key encryption, hash functions, message authentication codes, public key encryption, digital signatures, pseudorandom generators, bit commitment schemes, zero-knowledge proofs and secure multiparty computation. The course provides emphasis on provable security notions for building cryptographic primitives. Some advanced topics such as secret sharing, functional encryption, homomorphic encryption, identity-based signatures with real use cases will be covered and discussed through formal presentation/project by students.


References:
14. Roxie Marlinespike Null Prefix Attacks against SSL/TLS Certificates. Published online.
15. Roxie Marlinespike Defeating COPS With the Character ‘3’. Published online.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Visualize security properties, primitives and protocols used in various applications;
- Formulate security problem with computational assumptions;
- Model cryptographic primitives and analyze them; and
- Design and analyze security protocols.
10 Bigdata and Large-Scale Computing:
In today’s era of Big Data Analytics and Mining, where we are constantly faced with high-
velocity and high-volume streaming data, this course is designed to provide an introduction to
some of the most common frameworks, including Hadoop and Spark, that have made big data
analysis easier. The students will be exposed to various categories of data and management
tools. They will become familiar with techniques using real-time and semi-structured data
eamples. The course will also provide techniques to extract value from existing data sources
and discovering new data sources. Using Machine Learning algorithms students would be able
to learn techniques of mining high-velocity and high-volume data. In this regard, students will
be introduced to tools and scalable algorithms.

Indicative Topics of Study: Introduction. Hadoop Fundamentals. Data Logistics, Import-
ing and Exporting Data. Working with Hive and Pig Hadoop Use Cases. Big Data ML with
Mahout: Classification. Big Data ML with Mahout: Clustering and Recommenders. Apache
Spark Fundamentals. Temporal, Geospatial, Text Data Analysis with Spark. Analyzing Net-
works with GraphX. Big Data ML with MLlib. Spark MLlib Use Cases

References:
1. Ron Bekkerman, Mikhail Bilenko, John Langford. Scaling up Machine Learning: Parallel
   and Distributed Approaches, Cambridge University Press
2. Holden Karau, Andy Konwinski, Patrick Wendell, and Matei Zaharia. Hadoop in Practice,
   Manning Publications Co.
3. Alex Holmes. Learning Spark, O'Reilly
4. Sandy Ryza, Uri Laserson, Sean Owen, Josh Wills. Advanced Analytics with Spark,
   O'Reilly
   Publications Co.
   O'Reilly

Course Outcomes: Students who complete the course will have demonstrated the ability to
do the following:
• Describe the Big Data ecosystem and identify real-world big data problems.
• Understand the V’s of Big Data (volume, velocity, variety, veracity, valence, and value)
• Recast big data problems as data science questions.
• Summarize the features and value of core Hadoop stack components (e.g.: YARN resource
  and job management system, the HDFS file system, MapReduce programming model).
• Identify the frequent data operations required for various types of data.
• Select a data model to suit the characteristics of your data.
• Apply techniques to handle streaming data.
• Differentiate between a traditional Database Management System and a Big Data Man-
  agement System.
• Construct models that learn from data using widely available open source tools.
• Analyze big data problems using scalable machine learning algorithms on Spark.
11 Information Security:

In this course, the students would be learn the fundamentals of computer security, communications security, infrastructure security, and operational/organizational security. This course provides students with concepts of computer security, secure protocols, attack detection and other security techniques. Upon the completion of this course, students should be able to understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information.


Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:

- Demonstrate knowledge of security threats
- Create security policies to secure files and print resources
- Demonstrate knowledge of cryptography, access control and authentication
- Design mechanisms to prevent against external attack
- Demonstrate knowledge of operational and organization security

12 Communication Skills and Technical Writing:
Fluent communication and technical writing are functional skills central to science and engineering research. These are highly coveted and sought after talents which continue to be in demand in the academia. The Course Comm. Skills and Tech. Writing will provide the learners with a practical framework and structural orientation toward language used in technical documents. This Course will teach and train students to read, decipher and comprehend complex ideas which are indispensable to technical discourse. Besides preparing the students to construct documents (such as Abstracts, research papers, proposals, memorandums and notes) the course will enable them to edit and proof read their own constructions. The communication aspect of the Course will cater to honing the skills of speaking, expressing and adequately conveying one’s ideas across. This will include teaching the students to successfully carry out powerpoint presentations, interviews, impromptu speeches and discussions/deliberations. The approach and methodology used will be based on auditory-oral-visual tools and aids. The writing aspect will focus on document construction and information processing.


2. Irish, Robert and Peter Weiss. The Engineering Communication Manual, OUP
3. Markel M. Technical Communications, Bedford/St Martin’s
6. Journal of Technical Writing and Communication, SagePub, ISSN: 00472816 – papers as prescribed in class
Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:

- Create and decode complex documents, aimed at increasing their accessibility and readability: communicate complex ideas and issues without resorting to dense technical jargon.
- Practice with the documents ranging from software manuals to creating instructional material: compose material without dumbing down their impact.
- Be able to read and write research reports, briefs, minutes, summary statements etcetera, with the use of plain and appropriate English: read, write and explain confidently with the lay receiver in mind.
- Logically think and express the need for propriety in the world of communication: build a logical skeleton into/out of any document.
- The learners of this Course will be able to find themselves firmly in place to deal with real-time problems which result from an acute failure of the communication chain. The candidates will see themselves fit to troubleshoot situations in the world of information and technology with proper application of their brainstorming skills, the root of which is logical thinking and its parallel expression, written and spoken: become responsible and managerial for not only their own work but errors committed within the chain/system.

Electives

1 Secure Software Engineering:
In this course, the student will be taught how to design secure software and compare this approach with the conventional approach of designing security software to secure applications. The security of the software is to be incorporated in all the stages of the Software Development Life Cycle (SDLC). Hence, the artifacts that come into play at each stage of SDLC and the tools and techniques used to design and build such artifacts will be taught. In addition, a student would be exposed how to model security attacks using formal approaches, design the misuse and ab-use case, as compared to the use cases and then identify the security requirements and the design the software to prevent the attacks. The student would also be exposed to the techniques of writing secure code in C and Java and verify the source code of programs using static analysis. The student would be exposed to Automated static analysis using any of the open-source static analysis (Static Application Security Testing (SAST) Tools), open-source code analyzer tool, Secure Design using UML Sec and/or SecureUML, using Z to analyze security vulnerabilities/design flaws, using Petrinets for finding vulnerabilities in typical distributed applications.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:

- Describe the life cycle for developing secure software systems.
- Demonstrate understanding of the best practices for secure software development, apply formal methods and software testing, issues of privacy and trust for software design, assessment of risk as part of software design.
- Design a range of prevention techniques for web-based attacks.
- Design secure software architecture.
- Identify the code points where security measures are required.
- Select the most appropriate prevention techniques for given scenarios.

\[3\]for electives - the exact topics of study would be decided by the instructor
• Implement security measures in server-side and client-side code, evaluate the outcome of these measures and elicit and specify formally the security requirements thereby uncovering security flaws in designs.

2 Distributed Systems:
This course introduces the principles of distributed systems, how computing is performed across different systems (e.g. Google file systems) differences between local computations versus distributed computations, emphasizing the fundamental issues underlying the design of distributed systems and networks: communication, coordination, synchronization, fault-tolerance, locality, consistency and replication.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Understand the principles and techniques behind the design of distributed systems.
• Understand the core concepts of distributed systems: the way in which several machines orchestrate to correctly solve problems in an efficient, reliable and scalable way
• Analyze how existing systems use the concepts of distributed systems in designing large systems.
• Apply the concepts learnt to design and implement sample systems.
• Understand the concepts of locking, concurrency, caching, prefetching, scheduling, and communication across the network.
• Design practical solutions for the problems typical of real distributed systems and debug the issues, if any.

3 Security Protocols:
Protocols describe how communication between entities takes place. It is commonly believed that a security protocol may fail in three ways: the protocol design may be flawed, the cryptographic primitives used in the protocol may be weak, or the implementation contains bugs. This course aims to covers security properties, threats, vulnerabilities and attacks pertaining to various applications ranging from enterprise applications to electronic cash. The course provides substantial exposure on design and analysis aspects of security protocols such as classical key establishment protocols, electronic voting, multi-party computing, and fair exchange with emphasis on formal security analysis approach.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Understand, practice and learn the fundamental toolboxes for designing and analyzing existing security protocols.
• Be able to analyze, design and implement security mechanisms in organizations so as to minimize the vulnerability of organization ICT infrastructure to malicious attacks.
• Analyze the tradeoff involved in ensuring security attributes vs the available computational power and the capabilities of an adversary.
• Define and Design appropriate security model that simulates the prowess of an attacker.

4 Quantum Cryptography:
This course focuses on the introduction of quantum information, quantum computation and the research trends on quantum cryptography. The course starts with basics of quantum information (operators, measurement, data representation, qubits) and then brings the well-known algorithms (Shor’s algorithm, Grover’s algorithm) into discussion. The course discusses quantum
key exchange, quantum commitment, and the state of the art quantum cryptographic primitives for encryption and decryption schemes.

**Course Outcomes:** Students who complete the course will have demonstrated the ability to do the following:

- Understand quantum key distribution protocols.
- Understand how untrusted quantum devices can be tested.
- Be familiar with modern quantum cryptography – beyond quantum key distribution.
- Identify the role of safe generation and distribution of private keys in cryptography protocols.
- Design security protocols and analyze their security strength given the available computational power.
- Understand the properties of quantum mechanical systems required to build the BB84 & E91 QKD protocols.
- Understand the structure and assumptions of BB84 and E91 QKD protocols.
- Identify the role of QKD protocols in symmetric cryptography.
- Identify and analyze the real-world applications of QKD protocols.

5 Multimedia Security and Forensics:
Multimedia Security plays an important role in modern digital age. The course aims to cover a broad range of topics aimed at detecting and preventing digital assets from forgeries and tampering. Topics include: digital watermarking, transform domain of watermarking techniques, detectors and decoders for watermarking, multimedia data authentication, digital image forensics, framework for digital forensic evidence collection and processing, reconstruction of files and directory structures on the FAT and NTFS, database tampering, anti-forensics, video surveillance techniques and tools.

**Course Outcomes:** Students who complete the course will have demonstrated the ability to do the following:

- Understand and analyse the media representation and fundamentals.
- Understand both the importance and the processes necessary to handle data so as to insure its admissibility in a court of law.
- Understand methods of focusing investigations through analysis of multiple evidence sources.
- Apply and evaluate the media security techniques.
- Devise and implement approaches to perform forensics and counter-forensics.
- Design an investigative process for the digital forensic investigation.
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data and through disk forensics.
- Identify common areas of malicious software activity and characteristics of various types of malicious software files.
- Demonstrate an understanding of visual surveillance.
- Design incident response plan of both victim and suspect systems, including understanding the importance of network reconnaissance and network traffic analysis.
- Execute live response in intrusion investigation scenarios.
6 Social and Legal Aspects of Computer Security:
This course aims to discuss the perspectives of information security for economical, business, technological and social aspects to safeguard personal and corporate information against inadvertent disclosure. Security and privacy concerns for storing data in third-party system, data breaches on individuals and businesses, security and privacy regulations, laws, policies, and procedures will be one of the primary focuses of this course. The course will have discussion on intellectual property, copyrights, ethics, software licensing, import/export laws and information technology Act.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Understand the elements that define cybersecurity
• Understand the legal, social, and political frameworks that affect cybersecurity.
• Identify and define challenges to achieving cybersecurity.
• Identify and explain social, legal, political, and economic impediments to cybersecurity.
• Analyze and prescribe appropriate approaches to ensure secure cybersecurity state and to mitigate the breaches effectively, ethically, and according to law.
• Analyze the tradeoffs between different cybersecurity- vs - availability related interests.

7 Blockchains and Cryptocurrencies:
This course explores the fundamentals of blockchains and cryptocurrencies. The topics covered include blockchain primitives, classical ecash, peer-to-peer ecash, consensus protocols, proof of work and mining, and anonymity. The course will also discuss applications other than cryptocurrencies such as decentralized applications and smart contracts.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Have an understanding of what blockchain technology is.
• Understand what Bitcoin is and how it works.
• Understand and use key vocabulary and concepts commonly used when discussing blockchain and Bitcoin in business situations.
• Understand smart contracts, a core idea and computational model of blockchain that enables automation, autonomy, scalability and transparency.
• Develop a working knowledge of the emerging blockchain technology.
• Design and program smart contracts and decentralized application.
• Design and implement innovative application models, leveraging the blockchain technology.

8 Machine Learning in Cyber Security:
This course will explore how machine learning techniques can help build more secure systems. The primary focus will be on applications of machine learning to problems in computer security, for example, intrusion detection, malware classification and spam detection. The course will also discuss vulnerabilities in machine learning algorithms and countermeasures against attacks on machine learning models.

9 Special Topics in Security and Privacy:
In this course the instructor would decide, selected topics in Security and Privacy to be taught from the state-of-the-art publications, depending upon the research interests of the students as well as that of the instructor teaching the course.

Course Outcomes: - NA as of now -
10 Cognitive and Brain Science:
In recent era Machine learning plays an important role in research areas such as pattern recognition, image processing, natural language processing and computer vision. To make machine more intelligent to perform such tasks it is essential to understand the function of human brain and its direct relation to cognition. A course of cognition will improve the understanding of machine perception including intelligence. The course will include mind-body problem and grow towards sensory attention and memory management in terms of languages.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Learn about the anatomy and physiology of the brain.
- Learn about the working principles of neuroscience and information processing the brain.
- Learn about the analogy or relation between various machine learning techniques and various information processing principles in the brain.
- Understand and appreciate the use of cognitive models in the development of artificial intelligence.
- Be able to analyze the brain signals and its role in developing various brain-computer interfaces.

11 Computer Vision:
In this course, the topics to be taught include discussions on different approaches for 3D depth estimation (third dimension z) using 2D images (f(x,y)) thus solving the ill-posed nature of computer vision. The course will introduce a brief description of image processing and various transformation used for image processing. It will then grow to solve computer vision problems. The course would help the graduate students to understand the basic concepts in computer vision (how the computer can be used to perform the tasks of human vision system).

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Understand the basic concepts in computer vision (how the computer can be used to perform the tasks of human vision system).
- Analyze the images for extracting the 3D coordinates of the object.
- Develop technical presentation skills
- Solve the problems that are of ill-posed nature.

12 Deep Learning:
In this course - one which is a new area of Machine Learning research and a growing field in the area of pattern recognition, natural language processing, speech processing, image processing and vision, the students would be provided a broad introduction to deep learning architectures. The objectives include: 1. Formulate machine learning problems corresponding to different applications and solve using deep learning approaches. 2. Read current research papers and understand the issues raised by current research

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Understand a variety of deep learning architectures,
- Solve problems in object classification, natural language processing, super-resolution, inpainting, speech processing etc.
- Understand and analyze the cutting-edge research — starting from a refresher in basics of neural networks, to recent developments.
13 Information Retrieval:
In last 2 decades information retrieval plays an important role when we are dealing with huge
document data in internet. In this connection, retrieving relevant document is utmost important
for users. Not only that, it has applications in different domain such as medical, legal, social
and so on. In social media, the retrieval of pattern or getting relevant information is the need
of the hour. Keeping this in mind, this course aims to build up the required mathematics of
document representation and its mapping, matching. Many real-life problems as case study will
also be discussed. In case of Indian languages, another dimension is added to the problem of
multilingual issues, this will also be discussed in the course.

Course Outcomes: Students who complete the course will have demonstrated the ability to
do the following:

- Understand the complexity of a Natural Language Text processing system
- Be familiar with the concepts, issues and methods related to Unstructured Information
  Access.
- Perform quantitative evaluation of an Information access systems
- Be industry ready to undertake similar projects.

14 Numerical Methods for Data Sciences:
The objective of this course is to make the student learned some numerical techniques to find the
more appropriate solution to their problems in Data Science, and also to analyze their solution in
various circumstances. The course contains discussion of numerical methods particularly some
iterative methods for linear algebra and optimization in the context of machine learning and
data analysis problem. It will focus on sparsity problems, rank structure, special behavior of
underlying linear algebra problems, convergence analysis of numerical algorithms, regularization
via iteration, comparison between numerical methods for data analysis and large scale numerical
methods used in other areas of science and engineering.

Course Outcomes: Students who complete the course will have demonstrated the ability to
do the following:

- Acquire sufficient knowledge how to solve a problem numerically if the analytic solution is
  not available.
- Analyze the solution, analyze the sensitivity of the solution under various circumstances.
- Use the skills of Linear algebra and Numerical methods to apply them in Machine learning
  and data analysis problems.

15 Optimization Techniques:
The main purpose of this course is to provide the students the working knowledge of several
optimization techniques and numerical approaches to solve optimization problems in Data Sci-
ence. The course contents the linear and nonlinear convex optimization problems, and their
analytical solution methods. It also discusses some numerical optimization techniques in partic-
ular, gradient method, gradient descent method, steepest descent methods, Newton’s method,
proximal methods etc. that are useful to solve optimization problems aroused from Data science
and Machine learning. It also discusses the analysis of these methods and sensitivity of these
methods towards variation of data and parameters.

Course Outcomes: Students who complete the course will have demonstrated the ability to
do the following:

- Acquire sufficient knowledge to solve optimization problems analytically and numerically
  if the analytic solution is not available.
• analyze the solution, analyze the sensitivity of the solution under various circumstances.
• Apply the skills of analyzing optimizing problems and design solutions to problems in Machine learning and data analysis problems.

16 Speech Processing:
Speech processing plays a key role in design of conversational interfaces. Innovation in voice-based technologies has been derived by surge in use of smart phones across the world. In addition, it can be time consuming and in fact, frustrating to interact with computers using keyboard whereas speech is so natural to produce and it carries multiple levels of information, such as, linguistic message, speaker’s identity, health condition, acoustic environment in which it is recorded, emotion, cognition, attitude, gender, language, etc. The major objective of this course is to understand the potential of various speech technologies, such as, speech, speaker and language recognition, voice conversion, text-to-speech (TTS) synthesis, audio search, query-by-humming (QBH).

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Understand the speech signal and its formation process
• Be able to model the speech signal for better understanding
• Be familiar with the algorithms for speaker identification, speech recognition, language identification and so on
• Be exposed to various applications of speech processing

17 Network Security:
In this course, at the beginning, the student is exposed to different attacks and threats in computer networks, including network mapping, port scanning, sniffing, DoS, DDoS, reflection attacks, attacks on DNS and leveraging P2P deployments for attacks. The course continues with cryptography topics most relevant to secure networking protocols. First a review of the concepts of block ciphers, stream ciphers, public key cryptography, RSA, Diffie Hellman, certification authorities, digital signatures and message integrity is covered. After surveying basic cryptographic techniques, the course examines several secure networking protocols, including PGP, SSL, IPsec and wireless security protocols. The course examines operational security, including firewalls and intrusion-detection systems. Students would be expected to read recent research papers on network security and participate in an important lab component that includes packet sniffing, network mapping, firewalls, SSL and IPsec.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
• Evaluate and recognize a problem as being a possible network security threat.
• Analyze the network traffic to identify different types of Denial of Service attacks.
• Design a firewall for a typical network setup, including specifying the rules for filtering traffic.
• Design an intrusion detection system.
• Analyze the security strength of a typical installation using the TLS and/or IPSec protocols.
• Design a security protocol that works at either the Application layer, Transport layer or the Network layer.
• Analyze the security issues in Network operating systems, Web applications and the Web browsers.
18 Security and Privacy Issues in Resource Constrained Environments:
This course is concerned with study of the security issues in the resources constrained environments viz. the Wireless Sensor Networks, RFID Systems, Mobile Adhoc Networks and the Internet of Things. While topics such as cryptography, networking, network protocols are touched upon, this is not a course on those topics. Instead, this course is on understanding the characteristics of the Wireless Sensor Networks, the RFID Systems, and the Internet of Things; identification of potential threats and vulnerabilities in such environments and techniques for mitigating such threats. The emphasis in this course is on the design of the security protocols to ensure protection against the security attacks, and ways to avoid security holes in Wireless Sensor Networks, RFID Systems, and the Internet of Things. There are programming assignments based on the simulation using open source simulation/programming tools (C/C++, nesC, TinyOS, TOSSIM, Contiki/Cooja) to make students practice and experience secure software design and development.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Understand the importance of the Security Issues in Resource Constrained Environments, Embedded Devices & Systems.
- Understand the architecture of Wireless Sensor Networks, the typical configurations of the constituent components viz. sensor motes, typical applications, operating environments, programming languages, simulators through theoretical description as well as hands on experimentations.
- Design a hop-by-hop link layer security architecture and end-to-end security architecture for the Wireless Sensor Networks and the Internet of Things systems.
- Design a security protocol using Homomorphic Encryption Ciphers and of Attribute Based Cryptography for the embedded systems.
- Understand the design of existing ciphers for resource constrained devices and for embedded systems.
- Understand the security provisions in the typical operating systems for embedded systems.
- Analyze the security protocol stack of a typical Internet of Things architecture.

19 Application Security:
In this course the learner will be taught the design and implementation of secure applications. The emphasis would be exposing the learner to the techniques of writing software programs that make it difficult for intruders to exploit security holes. The students would be able to learn the fundamental technical skills required to identify and prevent application vulnerabilities. The course emphasizes writing secure programs in C and secure distributed programs in object oriented Java. The security ramifications of class, field and method visibility are emphasized as applicable.

Course Outcomes: Students who complete the course will have demonstrated the ability to do the following:
- Learn about the tools they will need to understand and assess software security.
- Learn how to apply the theory and practice of code auditing.
- Analyze/dissect an application, discover security vulnerabilities, and assess the danger each vulnerability presents.
- Understand and apply issues of secure programming principles i.e. different variable naming styles, code review processes, managing security bug bounties, unit testing philosophy, and how to write effective documentation.
• Design and implement various live projects, including a 6 week project where students would take an existing large code base and write a substantial new piece of functionality that integrates with it.
• Design and develop of secure applications, covering fundamental application development practices and the software security lifecycle.
• Analyze the source code and design testing methodologies for a set of projects, including web applications, C code, and mobile applications.
• Manage how to maximize their productivity, focusing on the most security-relevant elements of an application and prioritize efforts to help identify the most critical vulnerabilities first.
• Carry out a comprehensive security assessment of an application.

Offering of these and other probable Elective Courses  Depending on the availability of the faculty expertise, the following courses would be offered as Electives, as per the category shown:

1. Computational Number Theory – Elective I
2. Optimization Techniques – Elective I
3. Information Visualization – Elective I
4. Information Retrieval – Elective I
5. Distributed Systems – Elective I
7. Computational Numerical Methods - – Elective II
8. Brain and Cognitive Sciences – Elective II
10. Applications Security - Elective II
11. Blockchain and Cryptocurrencies – Elective II
12. Speech and Audio Processing – Elective II
13. Computer Vision – Elective III
15. Advanced Business Analytics – Elective III
16. Quantum Cryptography – Elective III
19. Selected Topics in Security and Privacy – Elective III

****
***
*
Additional Notes and Implementation Guidelines

1. The scheme of the program, the courses of study and the detailed curriculum were arrived in a series of meetings held at DA-IICT faculty. The minutes of each of these meetings are attached in the Appendices.

2. The M Tech program would be governed by the rules and regulations applicable to the MTech programs of study at IIT Jammu as duly approved by the IIT Jammu Senate.

3. For each semester there will be a Program advisor, who shall advise each student on the courses to study. The program advisor, by default, shall be at the place where the student is pursuing the studies in that semester.

4. However, for every semester, there will be a Program advisor (independent or joint, as applicable) from IIT Jammu. The Program advisor from IIT Jammu shall be final signatory for the scholarships of the students each month, for certifying the attendance and satisfactory duty of assigned work.

5. A course Project/Dissertation Preliminaries may be offered as either Dissertation Preliminaries OR as a Project in consultation with the Program advisor. In case it is offered as a Project, it is assumed that this course may be allowed to have no linkages with the dissertation to be done in the Semester 4. This would allow a student to carry out optional internship (in summer break), project (in 3rd semester) and Dissertation (in 4th semester) independently with no correlation amongst each other. However, in either cases, a student will have to select one Supervisor from IIT Jammu, along with other joint Supervisors.

6. Alternatively, a student may carry out (optional) Summer internship in summer break, the Dissertation Preliminaries (in the 3rd semester) and the Dissertation (in the 4th semester) on the same theme/problem domain, either internally (i.e. in any of the institutes) or in any industry (linked to the placement). Again, in either cases too as before, a student will have to select one Supervisor from IIT Jammu, along with other joint Supervisors, if need be and as appropriate.

7. The Electives I and II are aimed to impart depth and are aimed to decide the eventual specialization of a student. The Elective IV can occur at either of the three venues.

8. The evaluation scheme of IIT Jammu will be followed in the proposed program with two Minor examinations (in-semester examinations) and one Major examination (End-semester examination) in every semester, along with some weightage for the continuous evaluation in the form of Class quizzes, Surprise tests, and other components. The Weightage of these evaluations shall be as per the discretion of the Course Coordinator but announced in the first class or before that.

9. A student would register for the placement at either IIT Jammu or at DA-IICT, Gandhinagar as per their choice. A separate meeting of the T & P coordinators shall be scheduled to further decide the modalities at a subsequent date after due approvals.
10. At the commencement of every course, the Course Coordinator shall be responsible jointly with the Course Instructors to announce and publish a detailed Syllabus for the course, the exact list of references, the evaluation criteria and distribution amongst various components of examinations, and a Course plan spanning topics intended to be covered in all the lectures for the course throughout the semester. The same would be widely circulated across all the three institutes for noting.

11. The fees structure applicable shall be the same as the one approved at IIT Jammu.

12. This detailed curriculum shall be for internal use, after it is vetted in the statutory bodies of each institute (viz. the Senate and the Academic Council). The detailed curriculum shall not be displayed on the web-sites. Instead for the public distribution, two pamphlets shall be prepared as follows:

   a. **Brochure 1**: A program brochure containing brief description of the program, the aims and the objectives, the deliverables, broad structure, the places of study, the fees structure, the eligibility criteria etc shall be prepared. This brochure shall be used for media campaigns too.

   b. **Brochure 2**: A program brochure containing an abstract of each course in the program with its Course outcomes shall be prepared. This brochure shall be uploaded on the Institute’s web-sites.

*****

***

*