CO1 To be able to describe various security issues.
CO2 To be able to implement a symmetric and asymmetric cryptographic methods.
CO3 To be able to describe the role and implementation of digital signatures.
CO4 To be able to describe security mechanisms like intrusion detection, auditing and logging.

Syllabus:

Overview of Security: Protection versus security; aspects of security– confidentiality, data integrity, availability, privacy; user authentication, access controls, Orange Book Standard.

Security Threats: Program threats, worms, viruses, Trojan horse, trap door, stack and buffer overflow; system threats- intruders; communication threats- tapping and piracy.

Computer Security Models: BLP Model, BIBA Model, HRU Model.

Cryptography: Substitution, transposition ciphers, symmetric-key algorithms: Data Encryption Standard, Advanced Encryption Standard, IDEA, Block cipher Operation, Stream Ciphers: RC-4. Public key encryption: RSA, ElGamal. Diffie-Hellman key exchange. Elliptic Curve, EC cryptography, Message Authentication code (MAC), Cryptographic hash function.

Digital signatures: ElGamal digital signature scheme , Elliptic Curve digital signature scheme, NISTdigital signature scheme.

Key Management and Distribution : Symmetric Key Distribution, X.509 Certificate public key infrastructures.

Intrusion detection and prevention.

Readings:

1. W. Stalling, **Cryptography and Network Security Principles and Practices** (7th ed.), Pearson of India, 2018.
2. A.J. Elbirt, Understanding and Applying Cryptography and Data Security, CRC Press, Taylor Francis Group, New York, 2015.
3. C. Pfleeger and SL Pfleeger, Jonathan Margulies, **Security in Computing** (5th ed.), Prentice-Hall of India, 2015
4. M. Merkow and J. Breithaupt, **Information Security: Principles and Practices**, Pearson Education, 2006.

MCSC104: MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE [3-0-1]

Course Objectives:
This course will discuss fundamental concepts and tools in discrete mathematics with emphasis on their applications to computer science. The objectives of this course comprise of providing students knowledge of logic and boolean circuits, sets, functions, relations, deterministic and randomized algorithms. Furthermore, the students will learn analysis techniques based on counting methods, recurrence relations, trees and graphs.

Course Learning Outcomes :

At the end of the course, the student will be able to

CO1: perform operations on vectors; represent vectors geometrically; apply vector algebra to solve problems in sub-disciplines of computer science.
CO2: perform operations on matrices and sparse matrices; compute the determinant, rank and eigenvalues of a matrix; apply matrix algebra to solve problems in sub-disciplines of computer science.
CO3: perform data analysis in probabilistic framework
CO4: visualise and model the given problem using mathematical concepts covered in the course

Syllabus:

Vectors: Definition of Vectors, Vector Addition, Dot and Cross Products, Span, Norm of vectors, Orthogonality, geometry of vectors, Application of vectors in document analysis

Matrix Algebra
Matrices as vectors; Matrix-vector ,vector-matrix and matrix-matrix multiplications; Inner and outer products, triangular matrix, diagonal matrix, systems of linear equations, linear independence, determinant, rank of matrix, Eigen values and Eigen vectors, matrix transformations, geometry of transformations, Applications of matrix algebra in image representation and transformations.

Basic Probability Theory
Sample Space and Events, Probability axioms, Conditional Probability, Bayes' law

Basic Statistics
Introduction to Descriptive and Inferential Statistics, Describing Data Sets as Frequency tables, Relative frequency tables and graphs, Scatter diagram, Grouped data, Histograms, Ogives; Percentiles, Box Plot, Coefficient of variation, Skewness, Kurtosis;,

Distributions: Continuous and Discrete random variables, probability density function, probability mass function, distribution function and their properties, mathematical expectation, conditional expectation, Uniform (continuous and discrete), Binomial, Poisson, Exponential, Normal, $\chi 2$ distributions, weak Law of Large Numbers, Central Limit Theorem, Chebyshev's inequality.

Stochastic Processes
Introduction to stochastic process, Markov Chain, Transition probabilities, Birth-Death process

Readings:

1. Kishor S. Trivedi, Probability and Statistics with Reliability, Queuing and Computer Science Applications, John Wiely, 2016.
2. Sheldon M. Ross, Probability Models for Computer Science, Academic Press, 2001.
3. Linear Algebra and Probability for Computer Science Applications, Ernest Davis, CRC Press 2012. https://cs.nyu.edu/davise/MathTechniques/index.html

4. From Algorithms to Z-Scores: Probabilistic and Statistical Modeling in Computer Science Norm Matloff, University of California, Davis (Creative Common Licence) http://heather.cs.ucdavis.edu/~matloff/132/PLN/probstatbook/ProbStatBook.pdf

MCSC105: DATA MINING [3-0-1]

Course Objectives: In this course, the objective is to introduce the KDD process. The course should enable students to translate real-world problems into predictive and descriptive tasks. The course also covers data cleaning and visualization, supervised and unsupervised mining techniques.

Course Learning Outcomes : At the end of the course, the student will be able to

CO1: distinguish between the process of knowledge discovery and Data Mining.
CO2: play with basic data exploration methods to develop understanding of given data
CO3: identify suitable pre-processing method for give problem.
CO4: describe different data mining tasks and algorithms.
CO5: use programming tools (e.g. Weka/Python/R etc) for solving data mining tasks.
CO6: follow formal notations and understand the mathematical concepts underlying data mining algorithms

Syllabus:

Overview: The process of knowledge discovery in databases, predictive and descriptive data mining techniques, and unsupervised learning techniques.

Data preprocessing : Data cleaning, Data transformation, Data reduction, Discretization

Classification: Supervised learning/mining tasks , Decision trees, Decision rules, Statistical (Bayesian) classification, Instance-based methods (nearest neighbor), Evaluation and Validation methods.

Clustering : Basic issues in clustering, Partitioning methods (k-means, expectation maximization), Hierarchical methods for clustering, Density-based methods, Cluster Validation methods and metrics

Association Rule Mining: Frequent item set, Maximal and Closed itemsets, Apriori property, Apriori algorithm.

Readings:

1. J Zaki Mohammed and Wagner Meira, **Data Mining and Analysis: Fundamental Concepts and Algorithms,** Cambridge University Press, 2014.
2. P. Tan, M. Steinbach and V. Kumar, **Introduction to Data Mining**, Addison Wesley, 2006.
3. Jiawei Han and Micheline Kamber, **Data Mining: Concepts and Techniques** (3nd ed.), Morgan Kaufmann, 2011.
4. Charu C Agrawal, Data Mining: The Textbook, Springer, 2015