Elective I (**Credits: 3**)

Any 1 elective from …

Cryptography

Quantitative Techniques in Finance

Image Processing

Business & Data Analytics

CRYPTOGRAPHY

Course Syllabus
June 2014

Prerequisites: NONE **Course Credits: 4**

UNIT - I: OVERVIEW, HISTORY AND CLASSICAL CIPHERS

Cryptography, steganography and cryptanalysis; History and development of cryptography; Classical cryptosystems: shift, substitution and Vigen´ere ciphers; Attacks on shift, substitution and Vigen´ere ciphers; Enigma cryptosystem and Role of WW-II; Designing a provably secure system, One-Time pads.

UNIT - II: SYMMETRIC KEY CRYPTOSYSTEMS AND GSM SECURITY

Basics of number theory and algebra; Introduction to information theory, Shannon's axioms; DES and AES; Encryption in GSM communications, A5 family of algorithms.

UNIT - III: ASYMMETRIC KEY CRYPTOSYSTEMS AND DIGITAL SIGNATURES

Prime numbers, factorisation and discrete logarithms; RSA and El Gamal cryptosystems; Signa-ture schemes, hash functions and secret sharing schemes.

UNIT - IV: INTRODUCTION TO CRYPTANALYSIS

Known plaintext, known ciphertext, chosen plaintext and chosen ciphertext attacks, man-in-the-middle attacks; Attacks on DES and AES, differential cryptanalysis; Attacks on RSA; Attacks on El Gamal; Attacks on A5 family.

UNIT - V: ADVANCED TOPICS

Zero knowledge proofs; Pseudo-random number generators; Industry standards and practices.

TEXTBOOKS:

Recommended:

Douglas Stinson. *Cryptography: Theory and Practice*, Third Edition or higher, Chap-man & Hall/CRC (Indian Edition) 2011.

Alfred Menezes, Paul C. van Oorschot and Scott A. Vanstone. *Handbook of Applied Cryptography*, CRC Press (2001).

Free download in PDF available from http://cacr.uwaterloo.ca/hac/

References:

Johannes Buchmann. *Introduction to Cryptography*, Springer Pubs., 2nd Edition (2004)

Lawrence C. Washington. *Elliptic Curves, Number Theory and Cryptography*, Chapman & Hall/CRC 2nd Edition (2008).

Simon Singh. *The Code Book*, 4th Estate Pubs. (2002)

Quantitative Techniques in Finance

Credit: 3

Prerequisite : Mathematics and Statistics

Brief description :

The course on Quantitative Techniques in Finance (QTF) deals with fundamental concepts and models of quantitative measures required for scientific decision making with specific examples and case studies relevant to the Banking and Financial Sector. It covers topics of statistics, probability, numerical techniques and operations research models to develop necessary skills to understand, formulate, analyze and handle important real-life financial problems through examples, exercises and case studies. Analytical tools such as MS-EXCEL, MATLAB and R would be used for the analysis and solution of formulated problems.

Course Contents :

Module-A : Valuation Techniques :

Bond Characteristics and valuation, Cash flows, Simple and Compound Interest, Discounting, Present and Future value for single and multiple periods, EMI, Yield to Maturity, Duration, Modified Duration, Financial Markets, Yield Curve, balance sheet analysis, Profit and Loss Account Analysis, Financial Ratios, Statutory Liquidity Ratio, Cash Reserve Ratio, Prime Lending Rate, Base Rate, Repo Rate, Reverse Repo Rate, Forex Rate and analysis, Risks in Banks, Asset Liability Management, Interest Rate Risk and Liquidity Risk computation using Gap and Duration Gap Models.

Module-B : Forecasting Techniques

Statistical measures, Continuous and Discrete Probability distributions, Linear and Non-linear Interpolation, Regression, Time series, Least square and Maximum Likelihood estimation, Random Number Generation, Simulation and its applications, Variance and Co-variance Computation, Variance reduction, Volatility Models (ARCH, GARCH), Credit Risk Measures, Credit Rating, Value at Risk Computation, CAPM, Transfer pricing Models.

Module-C: Linear and Non-Linear Programming Techniques

LPP and NLPP Formulation and Solution, Application to various financial decision problems, Network optimization problems, Multi-Stage Financial Decisions, Dynamic Programming, Supply Chain Management and Currency Flows.

Module-D: Multiple Objective and Dynamic Optimization Techniques

Pareto Optimality, Multiple Objective Decision Making models, Scalarization methods, Weighting method, Ranking Methods, Goal Programming Formulation, Analytical Hierarchy Process, Data Envelopment Analysis, Optimal Control Problem, Stochastic Programming Problems.

Module-E: Financial Applications:

Optimization Models of Asset Liability Management with Single and Multiple Objectives, Stochastic Programming Models of Asset Liability Management using Single and Multiple Objectives, Investment decisions in Stock Markets, Single and Multiple Objective Portfolio Optimization Problems, Financial derivatives, Binomial Tree, Black Scholes Model, Financial Games.

Text Books & Reference Books:

1. An Introduction to Computational Finance, Ugur, Omer, Imperial College Press, 2009.

2. Quantitative Finance, Epps. T.W., Wiley, 2009.

3. Methods for business analysis and forecasting: text and cases, Tryfos, Peter, John Wiley & Sons, 1998.

4. Financial Engineering and Computation, Yuh-Dauh Lyuu, Cambridge University Press, 2002.

5. Quantitative Analysis for Management, Barry Render, Ralph M., Stair Jr., Michael, Pearson Education Inc., Delhi, 2003.

6. Quantitative business methods using Excel, Whigham, David, Oxford University Press, 1998.

7. Operations research: An Introduction, Taha, Hamdy A., Prentice Hall of India, New Delhi, 2001.

8. Principles of operations research with application to managerial decisions, Wagner, Harvey M., Prentice-Hall of India, New Delhi, 1996.

9. Decision Making and Information System Analysis, Krishna Chandra, Sarup & Sons Publ., New Delhi, 2002.

10. Introduction to Management Science, Prentice Hall, Taylor, B. W. , 2002.

11. Mathematical modeling: case studies from industry, Cumberbatch, Ellis; Fitt, Alistair, Cambridge University Press, 2001.

12. Valuation of Financial Assets, A.S.Ramasastri, Response Books, New Delhi, 2000.

13. Operations Research, Kanti Swaroop, P.K.Gupta and Man Mohan, Wiley, 2000.

14. Quantitative models for supply chain management, Tayur, Sridhar; Ganeshan, Ram;, Magazine, Michael, Kluwer Academic Publishers, 1999.

15. Monte Carlo Methods in Finance, Jaeckel, Peter, John Wiley & Sons, 2002.

16. Monte Carlo Methods in Financial Engineering, Glasserman, Paul, Springer-Verlag, 2003.

17. Financial Engineering, John F.Marshall and Vipul K.Bansal, Prentice Hall of India, New Delhi, 1996.

Suggested Assignments:

(i) Analysis of Banks Annual reports including balance sheet and Structural Liquidity.

(ii) Solution of Problems using MS-Excel, R and Matlab Optimization tools.

(iii) Writing Programs of computation techniques in Java

(iv) Preparing case study of various financial applications.

(v) Simulating various financial scenarios.

Business & Data Analytics

Credits: 3 Credits

Pre-requisites: Knowledge of basic linear algebra, statistics, database management systems is desirable

Course Objectives and Scope

The main objective of the course is to provide students a good overview of the ideas, the techniques, recent developments in Analytics in all its forms viz., descriptive, predictive and prescriptive analytics. In the last one decade, analytics has emerged as a catch-all phrase subsuming and connoting various modeling techniques for data-driven analysis such as statistical techniques/models such as multiple linear regression, logistic regression, k-means clustering, machine learning models including k-nearest neighbor technique, neural networks, decision trees, case-based reasoning, support vector machine, association rule mining, optimization, OLAP etc. Visual analytics, with ample coverage of visualization techniques shall be discussed. Feature selection and dimension reduction techniques shall also be covered. The relationship between analytics and data mining shall be discussed. Also, it aims to formulate data-driven problems as data mining or predictive analytics problems. Numerous case studies from banking, insurance, finance, manufacturing, bioinformatics shall be discussed. This approach gives the students an ample opportunity to learn the intricate concepts in the most appropriate way and lets them develop skills to solve real-life problems using data mining. Further, the ubiquitous presence of unstructured data in many fields shall be discussed with specific reference to text mining and web mining with applications in cyber fraud detection in banking etc. This completes the whole gamut of analytics at the PG level. Concepts of data warehousing and Online Analytical Processing (OLAP), in terms of data models, conceptual design methodologies, meta data and project implementation strategies shall also be discussed. Finally, Big data analytics shall also be introduced. A salient feature of the course is students shall be tasked to work on two mini-projects on real-life problems in order to enable them to learn first and how to conduct an analytics related project using open source tools.

Contents:

Module-A: Introduction to Analytics

Introduction to Analytics; its various forms viz., descriptive, predictive and prescriptive. Introduction to Data Warehousing and its concepts, Data Mining (DM), DM concepts, DM Process; CRISP-DM Methodology, Data Preparation/Preprocessing techniques – Feature Selection methodologies, dimension reduction techniques such as PCA and Transformations. Data Visualization Techniques, Data Balancing Techniques etc.

Module-B: Descriptive and Predictive Analytical techniques

Association Rule Mining and its Algorithms & Applications; Clustering, Hierarchical and Partition clustering – Techniques and applications; Forecasting- Simple Linear Regression, Multiple Linear Regression; Classification – Logistic Regression, Decision Trees, k-NN, Neural Networks, Case Based Reasoning etc.

Module-C: Practical Considerations in Analytics Projects

Determination of best analytical/data mining technique, MSE, NRMSE, MAPE, Confusion Matrix, ROC, AUC, Lift, Comprehensibility etc.

Module-D: Applications and Case Studies

Analytical CRM applications such as bankruptcy prediction, churn prediction, default prediction, customer segmentation, market basket analysis, credit scoring, Financial Fraud detection; Manufacturing in Hardware industry; Bioinformatics applications for cancer prediction etc.

Module- E: Advanced Analytics and Case Studies

Unstructured data mining, Text Analytics, Web Mining etc., Cyber Fraud Detection including Phishing/Spam/Malware detection; Overview of prescriptive analytics and application in time series data mining with a case study from banking operations. Introduction to Big Data and applications

Suggested Assignments: Two mini projects dealing with data mining applications to finance shall be assigned to students

References:

1. Data Mining: Practical machine learning tools and techniques by IH Witten, E Frank, Morgan Kaufmann, 2005.

2. Data warehouse lifecycle toolkit: expert methods for designing, developing, and deploying data warehouses - Kimball, Ralph; Reeves, Laura et al, John Wiley & Sons, 1998

3. Data Mining for Business Intelligence: Concepts, Techniques, and Applications in Microsoft Office Excel with XLMiner, by Galit Shmueli and Nitin R. Patel, Peter Bruce, 2010, John Wiley

4. Practical Text Mining and Statistical Analysis for Non-structured Text Data Applications by Gary Miner, John Elder, Andrew Fast, Thomas Hill, Robert Nisbet, Dursun Delen, Andrew Fast, Academic Press, 2012.

5. Data Mining Techniques – A. K. Pujari, University Press, 2001

6. Data mining: concepts and techniques - Han, Jiawei; Kamber, Micheline, J. Pei, Morgan Kaufmann Publishers, 2011.

7. M. N. Murty and V. S. Devi, Pattern Recognition: An Algorithmic Approach, Springer, 2013

8. L. Bellatreche, K. Karlapalem and M. Mohania, Some Issues in Design of Data Warehousing Systems, Chapter VI, In book Developing Quality Complex Database Systems: Practices, Techniques and Technologies – Shirley A. Becker, IDEA GROUP PUBLISHING, 2001.

9. C. Bishop, Pattern Recognition and Machine Learning, Springer, 2011

10. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, 2003