



Minutes of Meetings (MoM) of Board of Studies (BoS)

Academic Year : 2021-22

School : School of Mathematical And Computational Science

Department : Computer Science and Information

Date and Time : Nov 2nd, 2021- 11.30 AM

Venue : CSIT Department

The Board of Studies (BoS) of Department of Computer Science and Information, School of Studies of Mathematical and Computational Science, Guru Ghasidas Vishwavidyalaya, Bilaspur was held to design and discuss the introduction of new courses.

The following members were present in the meeting:

1. Prof. R. S. Jadon (External Expert Member BoS)
2. Prof. A. K. Saxsena (BOS Chairman, Dept. of Computer Science and Information, GGU Bilaspur)
3. Dr. Rajwant Singh Rao (Asst. Prof., Dept. of Computer Science and Information, GGU Bilaspur)

Following new courses are introduced in BSc(CS), MSc(CS) and MCA(2 Years Course)

1. Programming Methodology
2. Information Security
3. Research Methodology
4. Data Mining and Data Warehousing
5. Network Security

Kavens
**HEAD
DEPT OF CSIT
G.G.V. BILASPUR (C.G.)**



Minutes of Meetings (MoM) of Board of Studies (BoS)



Guru Ghasidas Vishwavidyalaya
Koni, Bilaspur - 495009 (C.G.)

(A Central University established by the Central Universities Act, 2009 No. 25 of 2009)
Department of Computer Science & Information Technology

No.233/CSIT/2021

Bilaspur, Dated: 02.11.2021

Minutes of the Meeting of BOS

The meeting of the Board of studies (BOS) of Computer Science and Information Technology Department was conducted on 01-11-2021 in the online mode. The external and internal faculty members attended this meeting online. Following agenda items were discussed and resolved.

Agenda items discussed in the meeting

01. Online discussion on curriculum design of M.Sc. (CS), CBCS based course to finalize the scheme and syllabus to be implemented from the session 2021-22).

The Scheme and Syllabus for MSc (CS) CBCS based were discussed among the members, the suggestions were given by the External member.

Resolution, Scheme and Syllabus for CBCS based MSc (CS) were approved to be implemented from 2021-22.

02. Online discussion on curriculum design of Pre Ph.D. Course work to finalize the syllabus to be implemented from the session 2021-22).

The syllabi for Pre Ph.D. Course work with syllabus of the first compulsory paper, optional papers were discussed among the members.

Resolution, Pre Ph.D. course work, compulsory, optional papers and syllabus were approved to be implemented from 2021-22.

03. Online discussion on curriculum design of B.Sc.(CS) Honours, LOCF based course to finalize the scheme and syllabus to be implemented from the session 2021-22).

The syllabus for B.Sc.(CS) Honours LOCF based was discussed among the members, the suggestions were given by the External member.

Aravind
**HEAD
DEPT OF CSIT
G.G.V. BILASPUR (C.G.)**



List of New Course(s) Introduced

Department : Computer Science and Information Technology

Programme Name : B.Sc(CS)

Academic Year : 2021-22

List of New Course(s) Introduced

Sr. No.	Course Code	Name of the Course
	B.Sc(101)	Programming Methodology
	BSC-504(1)	Information Security

Agarwal
HEAD
DEPT OF CSIT
G.G.V. BILASPUR (C.G.)

SYLLABUS FOR MCA COURSE UNDER CHOICE BASED CREDIT SYSTEM (CBCS) *

Session 2021-22 BSc(CS)

Note: The decision of the GG Vishwavidyalaya for implementing CBCS system on this course shall be final, rest will remain the same.

SEMESTER-I

S. No.	Subject Code	Title	Credits	Marks		Total
				Internal/	External	
1	BSC-101 (CIUATT1) (CORE - 1)	Programming Methodology	3 (3Th)	30	70	100
2	BSC-102 (CIUATT2) (CORE - 2)	Computer System Architecture	5 (4Th+1Tu)	30	70	100
3	BSC-103 (CIUATG1) (GE - I)	(GE - I)	5 (3Th+2P)	30	70	100
4	BSC-104 (CIUATL1) (SEC - I)	(SEC - I)	2 (2Th)	30	70	100
5	BSC-105 (CIUATA1) (AEC - I)	(AEC - I)	2(2Th)	30	70	100
6	BSC-106 (CIUALT1) (Practical Core-1)	Programming using C++	2 (2P)	30	70	100
		Total	19			600

List of GE Courses (5 credit)

1. Object Oriented Programming Concept
2. Introduction to DBMS

List of AEC Courses (2 credit)

1. Information Communication Technology
2. Internet Technology

List of SEC Courses (2 credit)

1. HTML and Introduction to JAVA Script
2. Introduction to WEB Technology

SEMESTER-II

S. No.	Subject Code	Title	Credits	Marks		Total
				Internal	External /	
1	(CIUBTT1) (CORE - 3)	Data Structure	3 (3Th)	30	70	100
2	(CIUBTT2) (CORE - 4)	Discrete Structures	5 (4Th+1Tu)	30	70	100
3	(CIUBTG1) (GE-II)	(GE-II)	5 (3Th + 2 P)	30	70	100
4	(CIUBTA1) (AEC - 2)	(AEC - 2)	2 (2Th)	30	70	100
5	(CIUBTL1) (SEC - I)	(SEC - I)	2(2Th)	30	70	100
6	(CIUBLT1) (Practical – 2)	Lab: Data Structure	2 (2P)	30	70	100
		Total	19			600

List of GE Courses (5 credit)

1. Introduction to Programming in C
2. Introduction to LINUX Operating System

List of AEC Courses (2 credit)

1. Introduction to JAVA
2. Introduction to Data Communication

List of SEC Courses (2 credit)

1. Introduction to IoT
2. Introduction to Logics of Computer

Semester-III

S.No.	Subject Code	Title	Credits	Marks *		Total *
				Internal /	External	
1	BSC-301 (CIUCTT1) (CORE - 5)	Operating System	5	30	70	100
2	BSC-302 (CIUCTT2) (CORE - 6)	Introduction to Algorithms Design	3	30	70	100
3	BSC-303 (CIUCTT3) (CORE - 7)	Computer Networks	5	30	70	100
4	BSC-304 (CIUCTG1) (GE - III)	(GE - III)	5	30	70	100
5	BSC-305 (CIUCTL2) (Practical -3)	(Lab:- Introduction to Algorithms Design)	2			100
6	BSC-306 (CIUCTA1) (AEC - III)	AEC – III	2			100
		Total	22			600

List of GE Courses (5 credit)

1. Introduction to microprocessor.
2. Introduction to Management Information Systems

List of AEC Courses (2 credit)

1. E-Commerce
2. PC Package

Semester-IV

S.No.	Subject Code	Title	Credits	Marks *		Total *
				Internal/	External	
1	BSC-401 (CIUDTT1) (CORE - 8)	Software Engineering	5	30	70	100
2	BSC-402 (CIUDTT2) (CORE - 9)	DBMS	5	30	70	100
	BSC-403 (CIUDTT3) (CORE - 10)	Object Oriented Programming using JAVA	3	30	70	100
3	BSC-403 (CIUDTG1) (GE-IV)	(GE - IV)	5	30	70	100
4	BSC-404 (CIUDTA1) (AEC-IV)	AEC IV	2	30	70	100
5	BSC-405 (CIUDLT3) (Practical -4)	Programming Lab in JAVA	2			100
		Total	22			600

List of GE Courses (5 credit)

1. System Software
2. Operating Systems

List of AEC Courses (2 credit)

1. Ethics and Cyber-awareness
2. Introduction to Business Analytics

Semester-V

S.No.	Subject Code	Title	Credits	Marks *		Total *
				Internal /	External	
1	BSC-501 (CIUETT1) (CORE - 11)	Internet Technologies	5	30	70	100
2	BSC-502 (CIUETT2) (CORE - 12)	Introduction to Artificial Intelligence	5	30	70	100
3	BSC-503 (CIUETD1) (DSE – I)	Image Processing / Soft Computing	3	30	70	100
4	BSC-504 (CIUETD2) (DSE-II)	Information Security / Data analytics	5	30	70	100
5	BSC-404 (CIUDTA1) (AEC- V)	AEC V	2			100
6	BSC-505 (CIUEL D1) (Practical DSE - I)	(Practical based on Image Processing / Soft Computing (DSE - I)	2			100
		Total	22			600

List of AEC Courses (2 credit)

1. Multimedia Technology
2. Operation Research & Optimization Techniques

Semester-VI

S.No.	Subject Code	Title	Credits	Marks *		Total *
				Internal /	External	
1	BSC-601 (CIUFTT1) (CORE - 13)	Computer Graphics	5	30	70	100
2	BSC-602 (CIUFTT2) (CORE - 14)	Machine Learning	5	30	70	100
3	BSC-603 (CIUFTD1) (DSE – III)	Data Mining / Internet of Things	3	30	70	100
4	BSC-604 (CIUFTD2) (DSE-IV)	Theory of Computation / Cloud Computing	5	30	70	100
5	BSC-605 (CIUFLD1) (Practical – 3)	(Practical based on Data Mining / Internet of Things (DSE - III)	2			100
6	BSC-606 (CIUFLF1)	Project	2			100
		Total	22			600

* As per University (GGV) Provisions



BSc(CS)-101

Programming Methodology

COURSE OBJECTIVES:

- To understand how C++ improves C with object-oriented features.
- To learn how to write functions for efficiency and performance.
- To learn the syntax and semantics of the C++ programming language.
- To learn how to design C++ classes for code reuse.

1. Introduction to C and C++

History of C and C++, Overview of Procedural Programming and Object-Oriented Programming, Using main() function, Compiling and Executing Simple Programs in C++.

2. Data Types, Variables, Constants, Operators and Basic I/O

Declaring, Defining and Initializing Variables, Scope of Variables, Using Named Constants, Keywords, Data Types, Casting of Data Types, Operators (Arithmetic, Logical and Bitwise), Using Comments in programs, Formatted and Console I/O (printf(), scanf(), cin, cout), Using Basic Header Files (stdio.h, iostream.h, conio.hetc).

3. Expressions, Conditional Statements and Iterative Statements

Simple Expressions in C++ (including Unary Operator Expressions, Binary Operator Expressions), Understanding Operators Precedence in Expressions, Conditional Statements, Understanding syntax and utility of Iterative Statements (while, do-while, and for loops), Use of break and continue in Loops, Using Nested Statements.

4. Functions and Arrays

Utility of functions, Call by Value, Call by Reference, Functions returning value, Inline Functions, Return data type of functions, Functions parameters, Differentiating between Declaration and Definition of Functions, Command Line Arguments.



Creating and Using One Dimensional Arrays (Declaring and Defining an Array, Initializing an Array), Two- dimensional Arrays, Introduction to Multi-dimensional arrays.

5. Pointers and References in C++

Understanding a Pointer Variable, Simple use of Pointers, Pointers to Pointers, Pointers to structures, Problems with Pointers, Passing pointers as function arguments, Returning a pointer from a function, Using references as function arguments and function return values.

6. Using Classes in C++

Principles of Object-Oriented Programming, Defining & Using Classes, Class Constructors, Constructor Overloading, Function overloading in classes, Class Variables & Functions, Objects as parameters, specifying the Protected and Private Access, Copy Constructors.

7. Overview of Function Overloading and Operator Overloading

Need of Overloading functions and operators, Overloading functions by number and type of arguments, looking at an operator as a function call, Overloading Operators (including assignment operators, unary operators).

8. Inheritance, Polymorphism and Exception Handling

Introduction to Inheritance (Multi-Level Inheritance, Multiple Inheritance), Polymorphism (Virtual Functions, Pure Virtual Functions), Basics Exceptional Handling (using catch and throw, multiple catch statements).

COURSE OUTCOMES:

After completion of this course students should able to understand -

- The fundamental programming concepts and methodologies which are essential to building good C/C++ programs.
- To practice the fundamental programming methodologies in the C/C++ programming



language via laboratory experiences.

To code, document, test, and implement a well- structured, robust computer program using the C/C++ programming language.

Reference Books

1. HerbtzSchildt, "C++: The Complete Reference", Fourth Edition, McGraw Hill.2003
2. BjarneStroustrup, "The C++ Programming Language", 4th Edition, Addison-Wesley , 2013.
3. BjarneStroustrup, "Programming -- Principles and Practice using C++", 2nd Edition, Addison-Wesley 2014.
4. E Balaguruswamy, "Object Oriented Programming with C++", Tata McGraw-Hill Education, 2008.
5. Paul Deitel, Harvey Deitel, "C++ How to Program", 8th Edition, Prentice Hall, 2011.
5. John R. Hubbard, "Programming with C++", Schaum's Series, 2nd Edition, 2000.
6. Andrew Koeni, Barbara, E. Moo, "Accelerated C++", Published by Addison-Wesley , 2000.
7. Scott Meyers, "Effective C++", 3rd Edition, Published by Addison-Wesley, 2005.
8. Harry, H. Chaudhary, "Head First C++ Programming: The Definitive Beginner's Guide", First Create space Inc, O-D Publishing, LLC USA.2014
9. Walter Savitch, "Problem Solving with C++", Pearson Education, 2007.
10. Stanley B. Lippman, JoseeLajoie, Barbara E. Moo, "C++ Primer", Published by Addison- Wesley, 5th Edition, 2012



Information Security

Computer Security: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, A Security Architecture for Open Systems, Computer Security Trends, Computer Security Strategy.

Cryptography: Substitution, transposition ciphers, symmetric-key algorithms-Data Encryption Standard, advanced encryption standards, public key encryption – RSA; Diffie-Hellman key exchange, ECC cryptography, Message Authentication- MAC, hash functions.

User Authentication and Access Control:

User Authentication: Means of Authentication, Password-Based Authentication, Token-Based Authentication, Biometric Authentication, Remote User Authentication, Security Issues for User Authentication Access Control: , Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control Example: UNIX File Access Control, Role-Based Access Control

Database Security: The Need for Database Security, Database Management Systems, Relational Databases, Database Access Control, Inference, Statistical Databases, Database Encryption, Cloud Security

Malicious Software's and Denial of Service Attacks:

Section-C Malicious Software: Types of Malicious Software (Malware), Propagation–Infected Content–Viruses, Propagation–Vulnerability Exploit–Worms, Propagation–Social Engineering– SPAM E-mail, Trojans, Payload–System Corruption, Payload–Attack Agent–Zombie, Bots, Payload–Information Theft– Keyloggers, Phishing, Spyware, Payload–Stealth–Backdoors, Rootkits

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial- ofService Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack

Operating System Security: Introduction to Operating System Security, System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/Unix Security, Windows Security, Virtualization Security

Textbook W. Stallings, -Computer Security: Principles and Practice,|| 2nd Edition, Prentice Hall, ISBN: 0132775069, 2011.

Recommended Books

1. M. Stamp, -Information Security: Principles and Practice,|| 2nd Edition, Wiley, ISBN: 0470626399, 2011.
2. M. E. Whitman and H. J. Mattord, -Principles of Information Security,|| 4th Edition, Course Technology, ISBN: 1111138214, 2011.
3. M. Bishop, -Computer Security: Art and Science,|| Addison Wesley, ISBN: 0-201- 44099-7, 2002.
4. G. McGraw, -Software Security: Building Security In,|| Addison Wesley, ISBN: 0321356705, 2006.



List of New Course(s) Introduced

Department : Computer Science and Information Technology

Programme Name : M.Sc(CS)

Academic Year : 2021-22

List of New Course(s) Introduced

Sr. No.	Course Code	Name of the Course
	MSC-205	Research Methodology
	MSC-303	Data Mining and Data Warehousing
	MSC-304	Network Security

Handwritten signature in blue ink.

**HEAD
DEPT OF CSIT
G.G.V. BILASPUR (C.G.)**



Semester-III

S.No.	Subject Code	Title	Credits	Marks		Total
				Internal	External	
1	MSC-301 (CORE - 7)	Computer Graphics and Multimedia	5	40	60	100
2	MSC-302 (CORE - 8)	Compiler Design	5	40	60	100
3	MSC-303 (DSE - 3)	Data Mining and Data Warehousing	5	40	60	100
4	MSC-304 (DSE - 4)	Network Security	5	40	60	100
5	MSC-305 (OE - 1)	Open Elective*	5	40	60	100
6	MSC-306 (Practical - 3)	Programming Lab in Data Mining	5			100
		Total	30			600

* Open Elective will be decided after the information of availability of courses from other departments

Semester-IV

S.No.	Subject Code	Title	Credits	Total
1	MSC-401 Dissertation/Field Work/Internship/Project/Industry Visit	Major Project	18	500

GRAND TOTAL	100	2200
--------------------	------------	-------------



Department of Computer Science & Information Technology (CSIT)

Guru Ghasidas Vishwavidyalaya, Bilaspur (C.G.)

(A Central University established by the Central Universities Act 2009 No. 25 of 2009)

SYLLABUS FOR M.Sc.(CS) CBCS based

Session 2021-22

Semester-I

S.No.	Subject Code	Title	Credits	Marks		Total
				Internal	External	
1	MSC-101 (CORE- 1)	Design of Operating System	5	40	60	100
2	MSC-102 (CORE -2)	Artificial Intelligence	5	40	60	100
3	MSC-103 (CORE- 3)	Relational Data Base Management Systems	5	40	60	100
4	MSC-104 (CORE-4)	Advanced JAVA Programming	5	40	60	100
5	MSC-105 (Practical-1)	Programming Lab in JAVA	5			100
		Total	25			500

Semester-II

S.No.	Subject Code	Title	Credits	Marks		Total
				Internal	External	
1	MSC-201 (CORE - 5)	Design and Analysis of Algorithm	5	40	60	100
2	MSC-202 (CORE - 6)	Machine Learning	5	40	60	100
3	MSC-203 (DSE - 1)	Neural Networks and Deep Learning	5	40	60	100
4	MSC-204 (DSE - 2)	Web Technology	5	40	60	100
5	MSC-205 (RM - 1)	Research Methodology	2	40	60	100
6	MSC-206 (Practical - 2)	Programming Lab in Web Technology	5			100
		Total	27			600



MSc(CS)-205

Research Methodology

COURSE OBJECTIVE:

This course is designed to enable students to:

- Identify and discuss the role and importance of research in the field of sciences.
- Identify and discuss the issues and concepts salient to the research process.
- Identify and discuss the complex issues inherent in selecting a research problem, selecting an appropriate research design, and implementing a research project.
- Identify and discuss the concepts and procedures of sampling, data collection, analysis and reporting.

UNIT I –RESEARCH FORMULATION AND DESIGN: Motivation and objectives – Research methods vs. Methodology. Types of research – Descriptive, Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, Conceptual vs. Empirical, concept of applied and basic research process, criteria of good research. Defining and formulating the research problem, selecting the problem, necessity of defining the problem, importance of literature review in defining a problem, literature review-primary and secondary sources, reviews, monograph, patents, research databases, web as a source, searching the web, critical literature review, identifying gap areas from literature and research database, development of working hypothesis.

UNIT II – DATA COLLECTION AND ANALYSIS: Accepts of method validation, observation and collection of data, methods of data collection, sampling methods, data processing and analysis strategies and tools, data analysis with statically package (Sigma STAT, SPSS for student t-test, ANOVA, etc.), hypothesis testing.

UNIT III –RESEARCH ETHICS, IPR AND SCHOLARY PUBLISHING: Ethics-ethical issues, ethical committees (human & animal); IPR- intellectual property rights and patent law, commercialization, copy right, royalty, trade related aspects of intellectual property rights (TRIPS); scholarly publishing- IMRAD concept and design of research paper, citation and acknowledgement, plagiarism, reproducibility and accountability.

UNIT IV –INTERPRETATION AND REPORT WRITING: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types



of reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports, Conclusions.

References:

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.
2. Kothari, C.R., 1990. Research Methodology: Methods and Techniques. New Age International. 418p.
3. Sinha, S.C. and Dhiman, A.K., 2002. Research Methodology, EssEssublications. 2 volumes.
4. Trochim, W.M.K., 2005. Research Methods: the concise knowledge base, Atomic Dog Publishing. 270p.

COURSE OUTCOME:

Students who successfully complete this course will be able to:

- Explain key research concepts and issues
- Read, comprehend, and explain research articles in their academic discipline.
- Demonstrate the ability to choose methods appropriate to research aims and objectives
- Understand the limitations of particular research methods
- Develop skills in qualitative and quantitative data analysis and presentation
- Develop advanced critical thinking skills
- Demonstrate enhanced writing skills
- Describe the appropriate statistical methods required for a particular research design
- Choose the appropriate research design and develop appropriate research hypothesis for a research project
- Develop an appropriate framework for research studies



MSc(CS)-303

Data Mining and Data Warehousing

COURSE OBJECTIVE:

- To introduce students to basic applications, concepts, and techniques of data mining.
- Understand and implement classical models and algorithms in data warehouses and data mining
- Characterize the kinds of patterns that can be discovered by association rule mining, classification and clustering
- Master data mining techniques in various applications like social, scientific and environmental context
- Develop skill in selecting the appropriate data mining algorithm for solving practical problems.
- To gain experience doing independent study and research.

1. **Data Mining:** Meaning, necessity, steps, Normal searching Vs. knowledge extraction

2. **Data Mining on different types of databases:** Relational, Data Warehouses, Transactional, Objectoriented, Object relational, Spatial, Temporal and time series, Text and multimedia, Heterogeneous and legacy.

3. **Data Warehouse:** Meaning, definition, OLTP vs. OLAP, Data cube, star schema, snow flakeschema, fact constellations, basic concepts in writing of DMQL, Three Tier Architecture of data warehouse, data mart, Indexing.

4. **Data Preprocessing:** Data cleaning, Data integration, Chi-square test, Data transformation, Data reduction, Dimensionality reduction: Principal component analysis (PCA), factor analysis (FA), Data compression: discrete Fourier Transform (DFT), discrete cosine transform (DCT), discrete Wavelet transform (DWT).

5. **Classification, Clustering and Prediction:** Meaning, k-nearest neighbourhood (k-NN), neural network based classification, Support vector machine (SVM) classifier, Naïve Bayes classifier and Decision tree. Performance measures of classification : confusion matrix, accuracy, F1 score, specificity, sensitivity, ROC and AUC. Clustering: types of variables, distance measures, types of Clustering, Partitioning Method: k-means, k-medoid clustering, unsupervised: Hierarchical clustering, DBSCAN, Prediction using Regression, nonlinear regression and Neural Network. Performance Measures for prediction. Types of training: holdout method, cross validation, leave-one-out method.

6. **Association rule mining:** Market basket analysis, support, confidence, Apriori algorithm with an example.

Readings:

1. Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber, Morgan Kaufmann Publishers (Elsevier, 2nd edition), 2006
2. Data Mining Methods for Knowledge Discovery, Cios, Pedrycz, Swiniarski, Kluwer Academic Publishers, London - 1998.

COURSE OUTCOME:

After successfully completing the course students will be able to

- Understand the functionality of the various data mining and data warehousing component
- Appreciate the strengths and limitations of various data mining and data warehousing models
- Explain the analyzing techniques of various data
- Describe different methodologies used in data mining and data warehousing.
- Compare different approaches of data warehousing and data mining with various technologies.



MSc(CS)-304

Network Security

COURSE OBJECTIVE:

- The main goal of this course is to enable the students to develop the necessary skills for developing robust & high performance scalable network applications.
- To learn about raw sockets and socket programming.
- To understand simple network management protocols and basics of TCP & UDP sockets.
- To understand the principles and practices of cryptography and network security
- To understand the practical applications that have been implemented and are in use to provide network Security

1. **Foundations of Cryptography and security:** Security trends, The OSI Security architecture, Security attack, services and mechanism, Ciphers and secret messages, Mathematical tools for cryptography: substitution techniques, modular arithmetic, Euclid's algorithm, finite fields, polynomial arithmetic.

2. **Symmetric Cipher:** Symmetric cipher model, Design Principles of Block Ciphers, Theory of Block Cipher Design, Feistel cipher network structure, Data Encryption Standard (DES), Strength of DES, Triple DES, Modes of operation, Advance encryption Standard (AES)- Evaluation criteria of AES, AES cipher, key distribution.

3. **Public Key cryptography and Hash function:** Prime numbers and testing for primality, factoring large numbers, Principles of public key cryptosystem, RSA algorithm. Key management: Diffie-Helman, Key exchange, Hash and Message authentication Code (MAC), Hash and MAC algorithms, Digital signature.

4. **IP and Web security protocols:** Authentication application: Kerberos, Public key infrastructure. E-mail: Pretty Good Privacy (PGP), S/MIME. IP security, Web Security: Secure Socket layer (SSL) and Transport layer security, Secure Electronic Transaction (SET).

5. **System Security:** Firewall, and Intrusion Detection system (IDS), Malicious Software.

Readings

1. Cryptography and Network Security By William Stallings, 4th Edition Pearson Publication
2. Applied cryptography - protocols and algorithm By Bruce Schneier, Springer Verlag 2003



3. Cryptography and Network Security By AtulKahate , TMH Publication.
4. Cryptography and Network Security By Behrouz A. Forouzan, First Edition, TMH Publication.
5. Network Security:Private Communication in Public World By Charlie Kaufman,RadiaPerlmanand Mike Speciner ,PHI Publication.

COURSE OUTCOME:

After successful completion of the course, students will be

- Familiar with protocols, network interfaces, and Design/performance issues in local area networks and wide area networks.
- Familiar with basics of Socket and Socket programming.
- Familiar with contemporary issues in networking technologies.
- Familiar with network tools and network programming.
- Familiar with client server programming, Conventional encryption algorithms for confidentiality and their design principles, Public key encryption algorithms and their design principles
- Able to use of message authentication codes, hash functions , digital signature and public key certificates

Handwritten signature: K. K. K.

**HEAD
DEPT OF CSIT
G.G.V. BILASPUR (C.G.)**