MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-I

Name of the Course: B.Sc. in Information Technology (**Cryptography and Network Security**) **Subject:** Programming for Problem Solving **and** Programming for Problem Solving Lab			
Course Code: BITCNS101 and BITCNS191		**Semester: 1**	
Duration: 36 Hrs.		**Maximum Marks: 100+100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance : 5**	
Practical: 4 hrs./week		**Continuous Assessment: 25**	
Credit: 3 + 2		**Practical Sessional internal continuous evaluation: 40**	
		Practical Sessional external examination: 60	
Aim:			
Sl. No.			
1.	Implement your algorithms to build programs in the C programming language		
2.	Use data structures like arrays, linked lists, and stacks to solve various problems		
3.	Understand and use file handling in the C programming language		
Objective:			
Sl. No.			
1.	To write efficient algorithms to solve various problems		
2.	To understand and use various constructs of the programming language		
3.	To apply such as conditionals, iteration, and recursion in programming		
Pre-Requisite:			
Sl. No.			
1.	**Basic Knowledge of Computer System**		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction to Computers** Computer Systems, Computing Environments, Computer Languages, Creating and Running Programs, Software Development, Flow charts. Number Systems: Binary, Octal, Decimal, Hexadecimal Introduction to C Language - Background, C Programs, Identifiers, Data Types, Variables,	**6**	**10**

	Constants, Input / Output Statements Arithmetic Operators and Expressions: Evaluating Expressions, Precedence and Associativity of Operators, Type Conversions.		
02	**Conditional Control Statements** Bitwise Operators, Relational and Logical Operators, If, If- Else, Switch-Statement and Examples. Loop Control Statements: For, While, DoWhile and Examples. Continue, Break and Goto statements Functions: Function Basics, User-defined Functions, Inter Function Communication, Standard Functions, Methods of Parameter Passing. Recursion- Recursive Functions.. Storage Classes: Auto, Register, Static, Extern, Scope Rules, and Type Qualifiers.	**8**	**10**
03	**Pre-processors and Arrays** Pre-processor Commands Arrays - Concepts, Using Arrays in C, Inter-Function Communication, Array Applications, Two-Dimensional Arrays, Multidimensional Arrays, Linear and Binary Search, Selection and Bubble Sort.	**8**	**16**
04	**Pointers** Pointers for Inter-Function Communication, Pointers to Pointers, Compatibility, Lvalue and Rvalue, Arrays and Pointers, Pointer Arithmetic and Arrays, Passing an Array to a Function, Memory Allocation Functions, Array of Pointers, Programming Applications, Pointers to void, Pointers to Functions, Command Line Arguments. Strings - Concepts, C Strings, String Input/ Output Functions, Arrays of Strings, String Manipulation Functions.	**8**	**16**
05	**Structures and File** Definition and Initialization of Structures, Accessing Structures, Nested Structures, Arrays of Structures, Structures and Functions, Pointers to Structures, Self-Referential Structures, Unions, Type Definition (typedef), Enumerated Types. Input and Output: Introduction to Files, Modes of Files, Streams, Standard Library Input/ Output Functions, Character Input/ Output Functions.	**6**	**18**
	Sub Total:	**36**	**70**

	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. The ability to learn concepts and apply them to other problems. ...
2. Basic mathematical skills.
3. A passion for problem solving.
4. Confidence around a computer programming Language.

List of Practical: Sl. No. 1 to 10 compulsory & at least three from the rest)

1. Write a c program to display the word "welcome".
2. Write a c program to take a variable int and input the value from the user and display it.
3. Write a c program to add 2 numbers entered by the user and display the result.
4. Write a c program to calculate the area and perimeter of a circle.
5. Write a C program to find maximum between two numbers.
6. Write a C program to check whether a number is divisible by 5 and 11 or not.
7. Write a C program to input angles of a triangle and check whether triangle is valid or not.
8. Write a C program to check whether a year is leap year or not.
9. Write a C program to input basic salary of an employee and calculate its Gross salary according to following:
   Basic Salary <= 10000 : HRA = 20%, DA = 80%
   Basic Salary <= 20000 : HRA = 25%, DA = 90%
   Basic Salary > 20000 : HRA = 30%, DA = 95%
10. Write a c program to print “welcome” 10 times.
11. Write a c program to print first n natural numbers using while loop.
12. Write a c program to print all the odd numbers in a given range.
13. Write a c program to add first n numbers using while loop.
14. Write a c program to print all numbers divisible by 3 or 5 in a given range.
15. Write a c program to add even numbers in a given range.
16. Write a c program to find the factorial of a given number.
17. Write a c program to find whether a number is prime or not.
18. Write a c program to print the reverse of a number.
19. Write a c program to add the digits of a number.
20. Write a c program to print the Fibonacci series in a given range using recursion.
21. Write a c program to check whether a number is an Armstrong number or not.
22. Write a c program to find g.c.d. and l.c.m. of two numbers using function.

Assignments:

Based on theory lectures.

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Yashavant Kanetkar,	Let us C	13th Edition	BPB Publication
E. Balaguruswamy	Programming in ANSI C		Tata McGraw-Hill
Gary J. Bronson	A First Book of ANSI C	4th Edition	ACM
Reference Books:			
Byron Gottfried	Schaum's Outline of Programming with C		McGraw-Hill
Kenneth A. Reek	Pointers on C		Pearson
Brian W. Kernighan and Dennis M. Ritchie	The C Programming Language		Prentice Hall of India

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions (MCQ only with the correct answer)		Subjective Questions			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	1,2,3,4,5	10	10				
B	3, 4, 5			5	3	5	60
C	1,2,3,4,5			5	3	15	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each	Question to be	Question to be

		question	set	answered
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3
Examination Scheme for Practical Sessional examination:				
Practical Internal Sessional Continuous Evaluation				
Internal Examination:				
Continuous evaluation				**40**
External Examination: Examiner-				
Signed Lab Assignments			**10**	
On Spot Experiment			**40**	
Viva voce			**10**	**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Mathematics for Computer Science**			
Course Code: BITCNS102		**Semester: 1**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	To develop formal reasoning.		
2.	Create habit of raising questions		
3.	Knowledge regarding the use of Mathematics in Computer Science		
4.	Ability to communicate knowledge, capabilities and skills related to the computer engineer profession		
Objective: **Throughout the course, students will be expected to demonstrate their understanding of Mathematics by being able to do each of the following**			
Sl. No.			
1.	To understand and solve mathematical problems		
2.	To impart knowledge regarding relevant topics.		
3.	To familiarize students with linear Algebra, differential and integral calculus, numerical methods and statistics.		
Pre-Requisite:			
Sl. No.			
1.	**Knowledge of basic algebra, trigonometry and calculus.**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Modern algebra** Set, Relation, Mapping, Binary Operation, Addition Modulo n, Multiplication modulo n, semi group, properties of groups, subgroup.	**3**	**5**
02	**Trigonometry**	**3**	**5**

	Radian or circular Measure, Trigonometric Functions, Trigonometric ratios of angle θ when θ is acute, trigonometric ratios of certain standard angles, allied angles, compound angles, multiple and sub- multiple angles.		
03	**Limits and Continuity** The real number system, The concept of limit, concept of continuity.	**2**	**5**
04	**Differentiation** Differentiation of powers of x, Differentiation of ex and log x, differentiation of trigonometric functions, Rules for finding derivatives, Different types of differentiation, logarithmic differentiation, differentiation by substitution, differentiation of implicit functions, differentiation from parametric equation. Differentiation from first principles.	**4**	**10**
05	**Integrations** Integration of standard Functions, rules of Integration, More formulas in integration, Definite integrals.	**4**	**10**
06	**Differential equations** First order differential equations, practical approach to Differential equations, first order and first degree differential equations, homogeneous equations. Linear equations, Bernoulli's equation, Exact Differential Equations.	**4**	**5**
07	**Complex Numbers** Complex Numbers, Conjugate of a complex number, modulus of a complex Number, geometrical representation of complex number, De Moivre's theorem, n^{th} roots of a complex number.	**3**	**5**
08	**Matrices and Determinants** Definition of a matrix, Operations on matrices, Square Matrix and its inverse, determinants, properties of determinants, the inverse of a matrix, solution of equations using matrices and determinants, solving equations using determinants.	**4**	**10**
09	**Infinite Series** Convergence and divergence, series of positive terms, binomial series, exponential series,logarithmic series.	**3**	**5**
10	**Probability**	**3**	**5**

	Concept of probability, sample space and events, three approaches of probability, kolmogorov's axiomatic approach to probability, conditional probability and independence of events, bay's theorem.		
11	**Introduction to Statistics** Measures of central Tendency, Standard Deviation, Discrete series. Methods, Deviation taken from assumed mean, continuous series, combined standard deviation, coefficient of variation, variance.	**3**	**5**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
S. K. Mapa	Higher Algebra		Levant Books
Chakravorty and Ghosh	Advanced Higher Algebra		U N Dhar Pvt. Ltd
Reference Books:			
Das and Mukherjee	Integral Calculus		U N Dhar Pvt. Ltd
Das and Mukherjee	Differential Calculus		U N Dhar Pvt. Ltd

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 11**	**10**	**10**				
B	**1 to 11**			**5**	**3**	**5**	**60**

C	**1 to 11**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Introduction to Financial Technology			
Course Code: BITCNS103		**Semester: 1**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	Providing a comprehensive skill set to build professional skill and apply new technologies to innovate and streamline financial systems.		
Objective:			
Sl. No. 1.	Providing a comprehensive idea about different technology issue and latest trends in Information technology that are highly applicable to today's competitive technology-driven world.		
2.	To impart knowledge regarding Artificial Intelligence, office automation, Distributed data processing.		
3.	To familiarize students with ERP, IS strategy and effects, Knowledge engineering and data warehouse.		
Pre-Requisite:			
Sl. No.	**None**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
1	Use of computers for managerial applications, Technology issues and data processing in organisations, Introduction to Information Systems, shift in Information system thinking, latest trends in Information Technology.	**9**	**15**
2	Computer Based Information Systems- office automation systems. Decision making and MIS, transaction processing systems. Decision support system, Group Decision Support,	**9**	**20**

	Executive Information systems, DSS generator		
3	Introduction to:Artificial Intelligence Based Systems, End user computing, Distributed data processing. Deciding on IS architecture, IT leadership & IS strategic planning.	**9**	**15**
4	Introduction to:IS strategy and effects of IT on competition. Introduction to: ERP, re-engineering work processes for IT applications, Business Process Redesign Knowledge engineering and data warehouse.	**9**	**20**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
O'Brien	Management Information System		**TMH**
Kelkar	Management Information System: A Concise Study		PHI
Reference Books:			
Janaki Raman	Decision support Systems		PHI
M.M. Oka	Business Application of Computers		EPH

End Semester Examination Scheme. **Maximum Marks-70.** **Time allotted-3hrs.**

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of	Total	No of	To	Marks	Total Marks

		question to be set	Marks	question to be set	answer	per question	
A	**1 to 4**	**10**	**10**				
B	**1 to 4**			**5**	**3**	**5**	**60**
C	**1 to 4**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (**Cryptography and Network Security**) **Subject:** e-Commerce security **and** e-Commerce security Lab	
Course Code: BITCNS104 and BITCNS194	**Semester: 1**
Duration: 36 Hrs.	**Maximum Marks: 100+100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 4 hrs./week	**Continuous Assessment: 25**
Credit: 3 + 2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60

Aim:	
Sl. No.	
1.	Learn about web application security threats and how to mitigate them.

Objective:	
Sl. No.	
1.	To understand what e-Commerce is.
2.	Learn how e-commerce security works.
3.	Learn to develop secure website

Pre-Requisite:	
Sl. No.	**None**

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
1	**Introduction** Ecommerce, doing business on the internet, the scope of ecommerce, using the web to reach customers, benefits of ecommerce market, Ecommerce technology, the internet environment. E-business models and markets, business models, e business market, traditional buy build approach and vendors, online sales channels, the advantages of outsourcing and infrastructure of TCP.	**9**	**20**

2	**Ecommerce Website Creation** Ecommerce website creation: the elements of ecommerce, website server, developing a ecommerce website, requirements for your site, building the site, implementation. Building shopping base systems, a shopping cart scenario, a customer servlet, real world application model, loose coupling.	**9**	**20**
3	**Mobile Commerce [9L]** Mobile commerce: wireless industry standard, wireless communication, platforms based of commerce, wireless wan, facilities for wireless-s environment. Concerns for mobile enterprise.	**9**	**15**
4	**Security** Security issues, security solution, symmetric and asymmetric cryptosystems, RSA, DES platforms, Protocols for secure messaging, secure electronic transaction protocol, electronic cash over the internet, internet security. Electronic payment system, issues, smart cards, digital currencies.	**9**	**15**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Learn and apply different security aspects
2. Develop programming skills

List of Practical: Sl. No. 1 to 10 compulsory & at least three from the rest)

1. Configuration of IIS server.
2. Study of Scripting language
3. Static Web Page Designing
4. Dynamic Web Page designing

Assignments:

Based on theory lectures.

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Pete loshin and vecca	Electronic commerce		
Janice Reynolds	The complete e-commerce book	**2nd**	**CRC Press**

Reference Books:

Carol Guercio Traver and Kenneth C. Laudon	E-commerce: Business, Technology, Society	**2nd**	**Pearson**
Daniel D'Apollonio	E-commerce A Beginners Guide To E-commerce	**1542810213, 9781542810210**	

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer with moderate configuration and Network connection

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions (MCQ only with the correct answer)		Subjective Questions			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	1 to 4	10	10				
B	1 to 4			5	3	5	60
C	1 to 4			5	3	15	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Examination Scheme for end semester examination:				
Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3
Examination Scheme for Practical Sessional examination:				
Practical Internal Sessional Continuous Evaluation				
Internal Examination:				
Continuous evaluation				**40**
External Examination: Examiner-				
Signed Lab Assignments		**10**		
On Spot Experiment		**40**		
Viva voce		**10**		**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Soft Skills and Soft Skills Lab			
Course Code: BITCNS105 and BITCNS195		**Semester: 1**	
Duration: 36 Hrs.		**Maximum Marks: 100+100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance: 5**	
Practical: 4 hrs./week		**Continuous Assessment: 25**	
Credit: 3 + 2		**Practical Sessional internal continuous evaluation: 40**	
		Practical Sessional external examination: 60	
Aim:			
Sl. No.			
1.	Ability to read English with ability to read English with understanding and decipher paragraph patterns, writer techniques and conclusions		
2.	Skill to develop the ability to write English correctly and master the mechanics of writing the use of correct punctuation marks and capital letter		
3.	Ability to understand English when it is spoken in various contexts.		
Objective:			
Sl. No.			
1.	To enable the learner to communicate effectively and appropriately in real life situation		
2.	Touse English effectively for study purpose across the curriculum		
3.	To use R,W,L,S and integrate the use of four language skills, Reading, writing , listening and speaking.		
4.	To revise and reinforce structures already learnt.		
Pre-Requisite:			
Sl. No.			
1.	Basic knowledge of English Language.		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Grammar** Correction of sentence, Vocabulary/word formation, Single word for a group of words, Fill in the blank, transformation of sentences, Structure of sentences – Active / Passive Voice – Direct / Indirect Narration.	**6**	**15**
02	**Essay Writing** Descriptive – Comparative – Argumentative – Thesis statement- Structure of opening / concluding paragraphs – Body of the essay.	**5**	**5**
03	**Reading Comprehension**	**5**	**10**

	Global – Contextual – Inferential – Select passages from recommended text.		
04	**Business Correspondence** Letter Writing – Formal. Drafting. Bio data - Resume'- Curriculum Vitae.	**5**	**8**
05	**Report Writing** Structure, Types of report – Practice Writing.	**5**	**5**
06	**Communication skills** Public Speaking skills, Features of effective speech, verbal-nonverbal.	**5**	**15**
07	**Group discussion** Group discussion – principle – practice	**5**	**12**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Skill of Grammar
2. Various writing skills
3. Skill of reading English text
4. Skill of effective written communication

Motor Skills:

1. Skill of using Correct body language while giving a presentation
2. Various non-verbal communication skills
3. Skill of using correct gestures and expressions while speaking publicly
4. Essential approach and attitude in Group Discussion or Viva

List of Practical:

1. Honing 'Listening Skill' and its sub skills through Language Lab Audio device.
2. Honing 'Speaking Skill' and its sub skills.
3. Helping them master Linguistic/Paralinguistic features (Pronunciation/Phonetics/Voice modulation/ Stress/ Intonation/ Pitch & Accent) of connected speech.
4. Honing 'Conversation Skill' using Language Lab Audio –Visual input, Conversational Practice Sessions (Face to Face / via Telephone, Mobile phone & Role Play Mode).
5. Introducing 'Group Discussion' through audio –Visual input and acquainting them with key strategies for success.
6. GD Practice Sessions for helping them internalize basic Principles (turn- taking, creative intervention, by using correct body language, courtesies & other soft skills) of GD.

7. Honing 'Reading Skills' and its sub skills using Visual / Graphics/Diagrams /Chart Display/Technical/Non Technical Passages, Learning Global / Contextual / Inferential Comprehension.
8. Honing 'Writing Skill' and its sub skills by using Language Lab Audio –Visual input, Practice Sessions

Assignments:
Based on theory lectures.

List of Books
Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
R.C. Sharma and K.Mohan	Business Correspondence and Report Writing		Tata McGraw Hill , New Delhi , 1994
.Gartside	Model Business Letters		Pitman , London , 1992
Reference Books:			
Mark MaCormack	Communication		
John Metchell	How to write reports		
S R Inthira&amp, V Saraswathi	Enrich your English – a) Communication skills b) Academic skills		CIEFL &amp, OUP
Longman	Longman Dictionary of Contemporary English/Oxford Advanced Learner's Dictionary of Current English		OUP , 1998
Maxwell Nurnberg and Rosenblum Morris	All About Words		General Book Depot, New Delhi , 1995
	A Text Book for English for Engineers &amp, Technologists		
List of equipment/apparatus for laboratory experiments:			
Sl. No.			

1.	Computer
2.	Audio Devices
3.	Visual Devices
4.	Language lab Devices and the dedicated software

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	1 to 7	10	10				
B	1 to 7			5	3	5	60
C	1 to 7			5	3	15	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Assignments	**10**	
On Spot Experiment	**40**	
Viva voce	**10**	**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-II

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Data Structure and Algorithm with Python and Data Structure and Algorithm with Python Lab**	
Course Code: BITCNS201 and BITCNS291	**Semester: 2**
Duration: 36 Hrs.	**Maximum Marks:**100+100
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	End Semester Exam:70
Tutorial: 0	Attendance: 5
Practical: 4 hrs./week	Continuous Assessment: 25
Credit: 3+2	Practical Sessional internal continuous evaluation: 40
	Practical Sessional external examination: 60

Aim:	
Sl. No.	
1.	The point of this course is to give you a vibe for algorithms and data structures as a focal area of what it is to be a computer science student.
2.	You ought to know about the way that there are regularly a few calculations for some issue, and one calculation might be superior to another, or one calculation better in certain conditions and another better in others.
3.	You should have some idea of how to work out the efficiency of an algorithm.
4.	You will be able to use and design linked data structures
5.	You will learn why it is good programming style to hide the details of a data structure within an abstract data type.
6.	You should have some idea of how to implement various algorithm using python programming.
Objective:	
Sl. No.	
1.	To impart the basic concepts of data structures and algorithms.
2.	To understand concepts about searching and sorting techniques.
3.	To understand basic concepts about stacks, queues, lists, trees and graphs.
4.	To understanding about writing algorithms and step by step approach in solving problems with the help of fundamental data structures
Pre-Requisite:	
Sl. No.	

1.	Basics of programming language.		
2.	Logic building skills.		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction to Data Structure** Abstract Data Type.	**1**	**2**
02	**Arrays** 1D, 2D and Multi-dimensional Arrays, Sparse Matrices. Polynomial representation.	**3**	**4**
03	**Linked Lists** Singly, Doubly and Circular Lists, Normal and Circular representation of Self Organizing Lists, Skip Lists, Polynomial representation.	**4**	**7**
04	**Stacks** Implementing single / multiple stack/s in an Array, Prefix, Infix and Postfix expressions, Utility and conversion of these expressions from one to another, Applications of stack, Limitations of Array representation of stack.	**4**	**10**
05	**Queues** Array and Linked representation of Queue, Circular Queue, De-queue, Priority Queues.	**4**	**7**
06	**Recursion** Developing Recursive Definition of Simple Problems and their implementation, Advantages and Limitations of Recursion, Understanding what goes behind Recursion (Internal Stack Implementation)	**4**	**5**
07	**Trees** Introduction to Tree as a data structure, Binary Trees (Insertion, Deletion, Recursive and Iterative Traversals of Binary Search Trees), Threaded Binary Trees (Insertion, Deletion, Traversals), Height-Balanced Trees (Various operations on AVL Trees).	**5**	**15**
08	**Searching and Sorting** Linear Search, Binary Search, Comparison of Linear and	**6**	**15**

	Binary Search, Selection Sort, Insertion Sort, Merge Sort, Quick sort, Shell Sort, Comparison of Sorting Techniques		
09	**Hashing** Introduction to Hashing, Deleting from Hash Table, Efficiency of Rehash Methods, Hash Table Reordering, Resolving collision by Open Addressing, Coalesced Hashing, Separate Chaining, Dynamic and Extendible Hashing, Choosing a Hash Function, Perfect Hashing Function.	**5**	**5**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Skill to analyze algorithms and to determine algorithm correctness and their time efficiency.
2. Knowledge of advanced abstract data type (ADT) and data structures and their implementations.
3. Ability to implement algorithms to perform various operations on data structures.

List of Practical:

1. Implementation of array operations.
2. Stacks and Queues: adding, deleting elements.
3. Circular Queue: Adding & deleting elements
4. Merging Problem : Evaluation of expressions operations on Multiple stacks & queues
5. Implementation of linked lists: inserting, deleting, and inverting a linked list.
6. Implementation of stacks & queues using linked lists:
7. Polynomial addition, Polynomial multiplication
8. Sparse Matrices: Multiplication, addition.
9. Recursive and Non Recursive traversal of Trees Threaded binary tree traversal. AVL tree implementation Application of Trees.
10. Application of sorting and searching algorithms Hash tables' implementation: searching, inserting and deleting, searching & sorting techniques.

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Michael H. Goldwasser, Michael T. Goodrich, and Roberto Tamassia	Data Structures and Algorithms in Python	1118476735, 9781118476734	John Wiley & Sons
Rance D Necaise	Data Structures and Algorithms Using Python	9788126562169	John Wiley & Sons

Reference Books:

Sartaj Sahni	DataStructures, Algorithms and applications in C++	Second Edition	Universities Press

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer with moderate configuration
2.	Python 2.7 or higher and other softwares as required.

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 9**	**10**	**10**				
				5	**3**	**5**	**60**
B	**1 to 9**						
				5	**3**	**15**	

C	**1 to 9**						

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Note Book	**10**	
On Spot Experiment	**40**	
Viva voce	**10**	**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Computation Number Theory and Computation Number Theory Lab**			
Course Code: BITCNS202 and BITCNS292		**Semester: 2**	
Duration: 36 Hrs.		**Maximum Marks:**100+100	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam:70	
Tutorial: 0		Attendance: 5	
Practical: 4 hrs./week		Continuous Assessment: 25	
Credit: 3+2		Practical Sessional internal continuous evaluation: 40	
		Practical Sessional external examination: 60	
Aim:			
Sl. No.			
1.	Define and interpret the concepts of Computation Number Theory		
Objective:			
Sl. No.			
1.	Learn methods and techniques used in number theory		
2.	Learn to apply knowledge in cryptography and related applied subjects		
3.	Provide a comprehensive hands on experience to write programs/functions to compute number theoretic functions.		
Pre-Requisite:			
Sl. No.			
1.	Strong mathematical background and knowledge of programming.		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
1	**Algorithms for integer arithmetic** Divisibility, gcd, modular arithmetic, modular exponentiation, Montgomery arithmetic, congruence, Chinese remainder theorem, Hensel lifting, orders and primitive roots, quadratic residues, integer and modular square roots, prime number theorem, continued fractions and rational approximations.	6	10
2	**Representation of finite fields** Prime and extension fields, representation of extension fields, polynomial basis, primitive elements, normal basis,	5	10

	optimal normal basis, irreducible polynomials.		
3	**Algorithms for polynomials** Root-finding and factorization, Lenstra-Lenstra-Lovasz algorithm, polynomials over finite fields.	4	5
4	**Elliptic curves** The elliptic curve group, elliptic curves over finite fields, Schoof's point counting algorithm.	4	5
5	**Primality testing algorithms** Fermat test, Miller-Rabin test, Solovay-Strassen test, AKS test.	4	10
6	**Integer factoring algorithms** Trial division, Pollard rho method, p-1 method, CFRAC method, quadratic sieve method, elliptic curve method.	4	10
7	**Computing discrete logarithms over finite fields** Baby-step-giant-step method, Pollard rho method, Pohlig-Hellman method, index calculus methods, linear sieve method, Coppersmith's algorithm.	5	10
8	**Applications** Algebraic coding theory, cryptography .	4	10
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

List of Practical:

Based on test environment.

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
V. Shoup	A computational introduction		Cambridge

	to number theory and algebra		University Press
M. Mignotte	Mathematics for computer algebra		Springer-Verlag
Reference Books:			
I. Niven, H. S. Zuckerman and H. L. Montgomery	An introduction to the theory of numbers		John Wiley
List of equipment/apparatus for laboratory experiments:			
Sl. No.	Computer with moderate configuration and internet connection.		

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	1 to 8	**10**	**10**				
				5	**3**	**5**	**60**
B	1 to 8						
				5	**3**	**15**	
C	1 to 8						

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	All	1	10	10

B	All	5	5	3
C	All	15	5	3
Examination Scheme for Practical Sessional examination:				
Practical Internal Sessional Continuous Evaluation				
Internal Examination:				
Continuous evaluation			**40**	
External Examination: Examiner-				
Signed Lab Note Book	**10**			
On Spot Experiment	**40**			
Viva voce	**10**		**60**	

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Operation Research and Game theory**			
Course Code: BITCNS203		**Semester: 2**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	Understand the mathematical tools that are needed to solve optimisation problems.		
Objective:			
Sl. No.			
1.	To impart knowledge in concepts and tools of Operations Research		
2.	To understand mathematical models used in Operations Research		
3.	To apply these techniques constructively to make effective decission.		
Pre-Requisite:			
Sl. No.			
1.	Basic concept linear algebra.		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
1	**Basics of Operational Research** Origin & Development of Operational Research, Definition and Meaning of Operational Research, Different Phases of an Operational Research Study, Scope and Limitations of Operational Research, Mathematical Modeling of Real Life Problems.	**12**	**15**
2	**Linear Programming** Introduction to Linear algebra. Solution of a system of Linear Equations, Linear independence and dependence of vectors, Concept of Basis, Basic Feasible solution, Convex sets. Extreme points, Hyperplanes and Halfspaces, Convex cones,	**12**	**30**

	Polyhedral sets and cones. Linear Programming Problem Formulation, solution by Graphical Method, Theory of Simplex Method, Simplex Algorithm, Two phase Method, Charnes-M Method, Degeneracy, Theory of Duality, Dual-simplex method.		
3	**Theory of Games** Introduction to Game theory, Formulation of two- person zero- sum rectangular game Solution of rectangular games with saddle points; dominance principle rectangular games without a saddle point – mixed strategy, Graphical, algebraic and linear programming solution of m x n games.	**12**	**25**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Hamdy A. Taha	Operations Research - An Introduction	9th Edition	Prentice Hall
P. R. Thie, G. E. Keough	An Introduction to Linear Programming and Game Theory	3rd edition	Wiley

Reference Books:

F.S. Hillier and G.J. Lieberman	Introduction to operation research	9 th edition	Tata Mcgrawhill

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 3**	**10**	**10**				

B **C**	**1 to 3** **1 to 3**			**5** **5**	**3** **3**	**5** **15**	**60**

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Discrete Mathematics**			
Course Code: BITCNS204		**Semester: 2**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	The aim of this course is to introduce you with a new branch of mathematics which is discrete mathematics, the backbone of Computer Science.		
2.	In order to be able to formulate what a computer system is supposed to do, or to prove that it does meet its specification, or to reason about its efficiency, one needs the precision of mathematical notation and techniques. The Discrete Mathematics course aims to provide this mathematical background.		
Objective: Throughout the course, students will be expected to demonstrate their understanding of Discrete Mathematics by being able to do each of the following			
Sl. No.			
1.	Use mathematically correct terminology and notation.		
2.	Construct correct direct and indirect proofs.		
3.	Use division into cases in a proof.		
4.	Use counterexamples.		
5.	Apply logical reasoning to solve a variety of problems.		
Pre-Requisite:			
Sl. No.			
1.	**Knowledge of basic algebra**		
2.	**Ability to follow logical arguments.**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Set Theory** Definition of Sets, Venn Diagrams, complements, Cartesian products, power sets, counting principle, cardinality and	**7**	**14**

	countability (Countable and Uncountable sets), proofs of some general identities on sets, pigeonhole principle. Relation: Definition, types of relation, composition of relations, domain and range of a relation, pictorial representation of relation, properties of relation, partial ordering relation. Function: Definition and types of function, composition of functions, recursively defined functions.		
02	**Propositional logic** Proposition logic, basic logic, logical connectives, truth tables, tautologies, contradictions, normal forms (conjunctive and disjunctive), modus ponens and modus tollens, validity, predicate logic, universal and existential quantification. Notion of proof: proof by implication, converse, inverse, contrapositive, negation, and contradiction, direct proof, proof by using truth table, proof by counter example.	**8**	**14**
03	**Combinatorics** Mathematical induction, recursive mathematical definitions, basics of counting, permutations, combinations, inclusion-exclusion, recurrence relations (nth order recurrence relation with constant coefficients, Homogeneous recurrence relations, Inhomogeneous recurrence relation), generating function (closed form expression, properties of G.F., solution of recurrence relation using G.F, solution of combinatorial problem using G.F.)	**7**	**14**
04	**Algebraic Structure** Binary composition and its properties definition of algebraic structure, Groyas Semi group, Monoid Groups, Abelian Group, properties of groups, Permutation Groups, Sub Group, Cyclic Group, Rings and Fields (definition and standard results).	**6**	**10**
05	**Graphs** Graph terminology, types of graph connected graphs, components of graph, Euler graph, Hamiltonian path and circuits, Graph coloring, Chromatic number. Tree: Definition, types of tree(rooted, binary), properties of trees, binary search tree, tree traversing (preorder, inorder, post order). Finite	**8**	**18**

	Automata: Basic concepts of Automation theory, Deterministic finite Automation (DFA), transition function, transition table, Non Deterministic Finite Automata (NDFA), Mealy and Moore Machine, Minimization of finite Automation.		
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Kenneth H. Rosen	Discrete Mathematics and its Applications		Tata Mc.Graw Hill
seymour Lipschutz, M.Lipson	Discrete Mathematics		Tata Mc.Graw Hill

Reference Books:

V. Krishnamurthy	Combinatorics:Theory and Applications		East-West Press
Kolman, Busby Ross	Discrete Mathematical Structures		Prentice Hall International

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**

C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Environmental Science**			
Course Code: BITCNS205		**Semester: 2**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 1 hr./week		End Semester Exam: 70	
Tutorial: 0		Attendance: 5	
Practical: 0		Continuous Assessment: 25	
Credit: 1		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	To enable critical thinking in relation to environmental affairs.		
2.	Understanding about interdisciplinary nature of environmental issues		
3.	**Independent research regarding environmental problems in form of project report**		
Objective:			
Sl. No.			
1.	To create awareness about environmental issues.		
2.	To nurture the curiosity of students particularly in relation to natural environment.		
3.	To develop an attitude among students to actively participate in all the activities regarding environment protection		
4.	To develop an attitude among students to actively participate in all the activities regarding environment protection		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Basic ideas of environment, basic concepts, man, society &amp, environment, their interrelationship. Mathematics of population growth and associated problems, Importance of population study in environmental engineering, definition of resource, types of resource, renewable, non- renewable, potentially renewable, effect of excessive use vis-à-vis population growth, Sustainable Development. Materials balance: Steady state conservation system, steady state system with non-conservative pollutants, step function.	**3**	**5**

	Environmental degradation: Natural environmental Hazards like Flood, earthquake, Landslide-causes, effects and control/management, Anthropogenic degradation like Acid rain-cause, effects and control. Nature and scope of Environmental Science and Engineering.		
02	**Ecology** Elements of ecology: System, open system, closed system, definition of ecology, species, population, community, definition of ecosystem- components types and function. Structure and function of the following ecosystem: Forest ecosystem, Grassland ecosystem, Desert ecosystem, Aquatic ecosystems, Mangrove ecosystem (special reference to Sundar ban), Food chain [definition and one example of each food chain], Food web. Biogeochemical Cycle- definition, significance, flow chart of different cycles with only elementary reaction [Oxygen, carbon, Nitrogen, Phosphate, Sulphur]. Biodiversity- types, importance, Endemic species, Biodiversity Hot-spot, Threats to biodiversity, Conservation of biodiversity.	**7**	**10**
03	**Air pollution and control** Atmospheric Composition: Troposphere, Stratosphere, Mesosphere, Thermosphere,Tropopause and Mesopause. Energy balance:Conductive and Convective heat transfer, radiation heat transfer, simple global temperature model [Earth as a black body, earth as albedo], Problems.Green house effects: Definition, impact of greenhouse gases on the global climate and consequently on sea water level, agriculture and marine food.Global warming and its consequence, Control of Global warming. Earth's heat budget. Lapse rate: Ambient lapse rate Adiabatic lapse rate, atmospheric stability, temperature inversion (radiation inversion). Atmospheric dispersion: Maximum mixing depth, ventilation coefficient, effective stack height, smokestack plumes and Gaussian plume model. Definition of pollutants and contaminants, Primary and secondary pollutants: emission standard, criteria pollutant. Sources and effect of different air pollutants- Suspended particulate matter, oxides of carbon, oxides of nitrogen, oxides of sulphur, particulate, PAN. Smog, Photochemical smog and London smog. Depletion Ozone layer: CFC, destruction of ozone layer by CFC, impact of other green house gases, effect of ozone modification. Standards and control measures: Industrial,	**6**	**10**

	commercial and residential air quality standard, control measure (ESP. cyclone separator, bag house, catalytic converter, scrubber (ventury), Statement with brief reference).		
04	**Water Pollution and Control** Hydrosphere, Hydrological cycle and Natural water. Pollutants of water, their origin and effects: Oxygen demanding wastes, pathogens, nutrients, Salts, thermal application, heavy metals, pesticides, volatile organic compounds. River/Lake/ground water pollution: River: DO, 5 day BOD test, Seeded BOD test, BOD reaction rate constants, Effect of oxygen demanding wastes on river[deoxygenation, reaeration], COD, Oil, Greases, pH. Lake: Eutrophication [Definition, source and effect]. Ground water: Aquifers, hydraulic gradient, ground water flow (Definition only) Standard and control: Waste water standard [BOD, COD, Oil, Grease], Water Treatment system [coagulation and flocculation, sedimentation and filtration, disinfection, hardness and alkalinity, softening] Wastewater treatment system, primary and secondary treatments [Trickling filters, rotating biological contractor, Activated sludge, sludge treatment, oxidation ponds] tertiary treatment definition. Water pollution due to the toxic elements and their biochemical effects: Lead, Mercury, Cadmium, and Arsenic.	**6**	**15**
05	**Land Pollution** Lithosphere, Internal structure of earth, rock and soil 1L Solid Waste: Municipal, industrial, commercial, agricultural, domestic, pathological and hazardous solid wastes, Recovery and disposal method- Open dumping, Land filling, incineration, composting, recycling. Solid waste management and control (hazardous and biomedical waste).	**4**	**10**
06	**Noise Pollution** Definition of noise, effect of noise pollution, noise classification [Transport noise, occupational noise, neighbourhood noise] Definition of noise frequency, noise pressure, noise intensity, noise threshold limit value, equivalent noise level,(18hr Index), Ldn. Noise pollution control.	**5**	**10**
07	**Environmental Management**	**5**	**10**

	Environmental impact assessment, Environmental Audit, Environmental laws and protection act of India, Different international environmental treaty/ agreement/ protocol.		
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
G. M.Masters,	Introduction to Environmental Engineering and Science		Prentice-Hall of India Pvt. Ltd., 1991
Reference Books:			
A. K. De	Environmental Chemistry		New Age International

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 7**	**10**	**10**				
B	**1 to 7**			**5**	**3**	**5**	**60**
C	**1 to 7**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Project I**	
Course Code: BITCNS281	**Semester: 2**
Duration: 36 Hrs	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: 100
Tutorial: 0	Attendance:
Practical: 2 hrs./week	Continuous Assessment:
Credit: 1	Practical Sessional internal continuous evaluation: 40
	Practical Sessional external examination: 60
Contents	
Students will do projects on application areas of latest technologies and current topics of societal relevance.	

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-III

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Computer Networks and Computer Networks**			
Course Code: BITCNS301 + BITCNS391		**Semester: 3**	
Duration: 36 Hrs.		**Maximum Marks: 100 + 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance : 5**	
Practical: 4 hrs./week		**Continuous Assessment: 25**	
Credit: 3 + 2		**Practical Sessional internal continuous evaluation: 40**	
		Practical Sessional external examination: 60	
Aim:			
Sl. No.			
●	To gain knowledge of computer networks.		
●	To gain knowledge of several layers and network architectures		
●	To gain knowledge of communication through networks, protocols and alghorithms.		
Objective:			
Sl. No.			
1.	Understand the division of network functionalities into layers.		
2.	Be familiar with the components required to build different types of networks Be exposed to the required functionality at each layer		
3.	Learn the flow control and congestion control algorithms		
Pre-Requisite:			
Sl. No.			
●	Understanding of algorithms		
●	Understanding of basic computer architecture		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**FUNDAMENTALS & LINK LAYER** Building a network – Requirements – Layering and protocols – Internet Architecture – Network software – Performance ; Link layer Services – Framing – Error Detection – Flow control	**7**	**14**
02	**MEDIA ACCESS & INTERNETWORKING** Media access control – Ethernet (802.3) – Wireless LANs – 802.11 – Bluetooth – Switching and bridging – Basic Internetworking (IP, CIDR, ARP, DHCP,ICMP)	**7**	**14**
03	**ROUTING**	**7**	**14**

	Routing (RIP, OSPF, metrics) – Switch basics – Global Internet (Areas, BGP, IPv6), Multicast – addresses – multicast routing (DVMRP, PIM)		
04	**TRANSPORT LAYER** Overview of Transport layer – UDP – Reliable byte stream (TCP) – Connection management – Flow control – Retransmission – TCP Congestion control – Congestion avoidance (DECbit, RED) – QoS – Application requirements	**8**	**14**
05	**APPLICATION LAYER** Traditional applications -Electronic Mail (SMTP, POP3, IMAP, MIME) – HTTP – Web Services – DNS – SNMP	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Identify the components required to build different types of networks
2. Choose the required functionality at each layer for given application
3. Identify solution for each functionality at each layer
4. Trace the flow of information from one node to another node in the network

List of Practical: Based on theory lectures.

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Larry L. Peterson, Bruce S. Davie	Computer Networks: A Systems Approach	Fifth	Morgan Kaufmann Publishers
Behrouz A. Forouzan	Data Communication and Networking	Fourth	Tata McGraw – Hill
James F. Kurose, Keith W. Ross	Computer Networking – A Top-Down Approach Featuring the Internet	Fifth	Pearson Education

Reference Books:

Nader. F. Mir	Computer and Communication Networks		Pearson Prentice Hall Publishers
Ying-Dar Lin, Ren-Hung Hwang, Fred Baker	Computer Networks: An Open Source Approach		McGraw Hill Publisher

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer with Internet Connection

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Assignments	**10**	

On Spot Experiment	**40**	
Viva voce	**10**	**60**

Name of the Course: B.Sc. in Information Technology **(Cryptography and Network Security)**	
Subject: Operating Systems and Operating Systems Lab	
Course Code: BITCNS302 + BITCNS392	**Semester: 3**
Duration: 36 Hrs.	**Maximum Marks: 100 + 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 4 hrs./week	**Continuous Assessment: 25**
Credit: 3 + 2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60

Aim:

Sl. No.	
1.	General understanding of structure of modern computers
2.	Purpose, structure and functions of operating systems
3.	Illustration of key OS aspects by example

Objective:

Sl. No.	
1.	To learn the fundamentals of Operating Systems.
2.	To learn the mechanisms of OS to handle processes and threads and their communication
3.	To learn the mechanisms involved in memory management in contemporary OS
4.	To gain knowledge on distributed operating system concepts that includes architecture, Mutual exclusion algorithms, deadlock detection algorithms and agreement protocols

5.	To know the components and management aspects of concurrency management
6.	To learn programmatically to implement simple OS mechanisms

Pre-Requisite:

Sl. No.	
1.	Strong programming skills (Knowledge of C)
2.	Computer architecture
3.	Elementary data structures and algorithms

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Concept of Operating Systems, Generations of Operating systems, Types of Operating Systems, OS Services, System Calls, Structure of an OS - Layered, Monolithic, Microkernel Operating Systems, Concept of Virtual Machine. Case study on UNIX and WINDOWS Operating System.	**3**	**5**
02	**Processes** Definition, Process Relationship, Different states of a Process, Process State transitions, Process Control Block (PCB), Context switching Thread: Definition, Various states, Benefits of threads, Types of threads, Concept of multithreads, Process Scheduling: Foundation and Scheduling objectives, Types of Schedulers, Scheduling criteria: CPU utilization, Throughput, Turnaround Time, Waiting Time, Response Time; Scheduling algorithms: Pre-emptive and Non pre-emptive, FCFS, SJF, RR; Multiprocessor scheduling: Real Time scheduling: RM and EDF.	**8**	**20**

03	**Inter-process Communication:** Critical Section, Race Conditions, Mutual Exclusion, Hardware Solution, Strict Alternation, Peterson's Solution, The Producer\ Consumer Problem, Semaphores, Event Counters, Monitors, Message Passing, Classical IPC Problems: Reader's & Writer Problem, Dinning Philosopher Problem etc.	**4**	**5**
04	**Deadlocks** Definition, Necessary and sufficient conditions for Deadlock, Deadlock Prevention, Deadlock Avoidance: Banker's algorithm, Deadlock detection and Recovery.	**4**	**10**
05	**Memory Management** Basic concept, Logical and Physical address map, Memory allocation: Contiguous Memory allocation – Fixed and variable partition– Internal and External fragmentation and Compaction; Paging: Principle of operation – Page allocation – Hardware support for paging, Protection and sharing, Disadvantages of paging. Virtual Memory: Basics of Virtual Memory – Hardware and control structures – Locality of reference, Page fault , Working Set , Dirty page/Dirty bit – Demand paging, Page Replacement algorithms: Optimal, First in First Out (FIFO), Second Chance (SC), Not recently used (NRU) and Least Recently used (LRU).	**8**	**10**
06	**I/O Hardware** I/O devices, Device controllers, Direct memory access Principles of I/O Software: Goals of Interrupt handlers, Device drivers, Device independent I/O software, Secondary-Storage Structure: Disk structure, Disk scheduling algorithms File Management: Concept of File, Access methods, File types, File operation, Directory structure, File System structure, Allocation methods (contiguous, linked, indexed), Free-space management (bit vector, linked list, grouping), directory implementation (linear list, hash table), efficiency and performance.	**6**	**10**

07	**Disk Management** Disk structure, Disk scheduling - FCFS, SSTF, SCAN, C-SCAN, Disk reliability, Disk formatting, Boot-block, Bad blocks.	**3**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Can be able to Identify the purpose of the analysis.
2. Can be considered a reliable source of information.
3. Can able to use a variety of techniques to extend the original idea.

List of Practical:

1. Basics of UNIX commands.

2. Shell programming

3. Implementation of CPU scheduling. a) Round Robin b) SJF c) FCFS d) Priority

4. Implement all file allocation strategies

5. Implement Semaphores

6. Implement Bankers algorithm for Dead Lock Avoidance

7. Implement an Algorithm for Dead Lock Detection

9. Implement the all page replacement algorithms a) FIFO b) LRU c) LFU 10. Implement Shared memory and IPC

10. Implement Paging Technique f memory management.

11. Implement Threading & Synchronization Applications

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
AviSilberschatz, Peter Galvin, Greg Gagne, Wiley Asia	Operating System Concepts Essentials	978-1-119-32091-3	
William Stallings	Operating Systems: Internals and Design Principles	5th Edition	Prentice Hall of India

Reference Books:

Charles Crowley	Operating System: A Design-oriented Approach	1st Edition	Irwin Publishing
J. Nutt, Addison-Wesley	Operating Systems: A Modern Perspective	2nd Edition	
Maurice Bach	Design of the Unix Operating Systems	8th Edition	Prentice-Hall of India
Daniel P. Bovet, Marco Cesati	Understanding the Linux Kernel	3rd Edition	O'Reilly and Associates

List of equipment/apparatus for laboratory experiments:

Sl. No.	

•	**Computer**
•	**Linux/Ubantu operating system**

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 7**	**10**	**10**				**60**
B	**1 to 7**			**5**	**3**	**5**	
C	**1 to 7**			**5**	**3**	**15**	

1. Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**3**	**3**

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:			
Continuous evaluation			**40**
External Examination: Examiner-			
Signed Lab Note Book		**10**	
On Spot Experiment		**40**	
Viva voce		**10**	**60**

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Probability & Statistics**			
Course Code:BITCNS303		**Semester: 3**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	**The aim of this course is to equip the students with standard concepts and tools at an intermediate to advanced level that will serve them well towards tackling various problems in the discipline.**		
2.	**The objective of this course is to familiarize the students with statistical techniques.**		
Objective: Throughout the course, students will be expected to demonstrate their understanding of probability & statistics by being able to learn each of the following			
Sl. No.			
1.	**The ideas of probability and random variables and various discrete and continuous probability distributions and their properties.**		
2.	**The basic ideas of statistics including measures of central tendency, correlation and regression.**		
3.	**The statistical methods of studying data samples.**		
Pre-Requisite:			
Sl. No.			
1.	**Knowledge of basic algebra, calculus.**		
2.	**Ability to learn and solve mathematical model.**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Definition of Partial Differential Equations, First order partial differential equations, solutions of first order linear PDEs; Solution to homogenous and nonhomogeneous linear partial differential equations of second order by complimentary function and particular integral method. Second-order linear equations and their classification, Initial and boundary conditions, D'Alembert's solution of the wave equation; Duhamel's principle for one dimensional wave equation. Heat diffusion and vibration problems, Separation of	**12**	**20**

	variables method to simple problems in Cartesian coordinates. The Laplacian in plane, cylindrical and spherical polar coordinates, solutions with Bessel functions and Legendre functions. One dimensional diffusion equation and its solution by separation of variables.		
02	Probability spaces, conditional probability, independence; Discrete random variables, Independent random variables, the multinomial distribution, Poisson approximation to the binomial distribution, infinite sequences of Bernoulli trials, sums of independent random variables; Expectation of Discrete Random Variables, Moments, Variance of a sum, Correlation coefficient, Chebyshev's Inequality. Continuous random variables and their properties, distribution functions and densities, normal, exponential and gamma densities.Bivariate distributions and their properties, distribution of sums and quotients, conditional densities, Bayes' rule.	**12**	**25**
03	Basic Statistics, Measures of Central tendency: Moments, skewness and Kurtosis - Probability distributions: Binomial, Poisson and Normal - evaluation of statistical parameters for these three distributions, Correlation and regression – Rank correlation. Curve fitting by the method of least squares- fitting of straight lines, second degree parabolas and more general curves. Test of significance: Large sample test for single proportion, difference of proportions, Tests for single mean, difference of means, and difference of standard deviations. Test for ratio of variances - Chi-square test for goodness of fit and independence of attributes.	**12**	**25**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:
Based on the curriculum as covered by subject teacher.

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Erwin Kreyszig	Advanced Engineering Mathematics	9 th Edition	John Wiley & Sons
N. G. Das	Statistical Methods	0070083274, 9780070083271	Tata Mc.Graw Hill
Reference Books:			
P. G. Hoel, S. C. Port and C. J. Stone	Introduction to Probability Theory		Universal Book Stall
W. Feller	An Introduction to Probability Theory and	3rd Ed.	Wiley

		its Applications					
End Semester Examination Scheme.			**Maximum Marks-70.**			**Time allotted-3hrs.**	
Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A **B** **C**	**1 to 3** **1 to 3** **1 to 3**	**10**	**10**	 **5** **5**	 **3** **3**	 **5** **15**	 **60**

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Cryptography			
Course Code:BITCNS305		**Semester: 3**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1	**Enable the students to learn fundamental concepts of cryptography and utilize these techniques in computing systems and also introduce them with network security using various cryptographic algorithms.**		
Objective:			
Sl. No.			
1	**Understand the most common type of cryptographic algorithm.**		
2	**Understand the Public-Key Infrastructure**		
3	**Understand security protocols for protecting data on networks**		
4	**Be able to configure simple firewall architectures**		
Pre-Requisite:			
Sl. No.			
1.	**Basic concept on linear algebra, number theory and computer programming.**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Attacks on Computers & Computer Security -Introduction, Need for Security, Security approaches, Principles of Security, Types of attack	**5**	**10**
02	Cryptography: Concepts & Techniques- Introduction, Plaintext & Cipher text, Substitution Techniques, Transposition Techniques, Encryption & Decryption, Symmetric & Asymmetric key Cryptography, Key Range & Key Size	**7**	**15**
03	Symmetric Key Algorithm - Introduction, Algorithm types & Modes,	**8**	**10**

	Overview of Symmetric Key Cryptography, DES(Data Encryption Standard) algorithm, IDEA(International Data Encryption Algorithm) algorithm, RC5(Rivest Cipher 5) algorithm.		
04	Asymmetric Key Algorithm, Digital Signature and RSA - Introduction, Overview of Asymmetric key Cryptography, RSA algorithm, Symmetric & Asymmetric key Cryptography together, Digital Signature, Basic concepts of Message Digest and Hash Function (Algorithms on Message Digest and Hash function not required).	**5**	**15**
05	Internet Security Protocols, User Authentication - Basic Concepts, SSL protocol, Authentication Basics, Password, Authentication Token, Certificate based Authentication, Biometric Authentication.	**5**	**10**
06	Electronic Mail Security - Basics of mail security, Pretty Good Privacy, S/MIME.Firewall - Introduction, Types of firewall, Firewall Configurations, DMZ Network	**6**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:
Based on the curriculum as covered by subject teacher.

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
William Stallings	Cryptography and Network security	4th	Pearson
Christof Paar and Jan Pelzl	Understanding Cryptography: A Textbook for Students and Practitioners		Springer
Reference Books:			
Bruce Schneier	Applied Cryptography	**2nd**	Wiley India Edition

End Semester Examination Scheme. **Maximum Marks-70.** **Time allotted-3hrs.**

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 6**	**10**	**10**				
B	**1 to 6**			**5**	**3**	**5**	**60**
C	**1 to 6**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.

- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Web security			
Course Code:BITCNS304		**Semester: 3**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1	**Understanding the fundamental security principles of the web. The course provides an overview of the most common attacks, and illustrates fundamental countermeasures that every web application should implement.**		
Objective:			
Sl. No.			
1	**To understand security principles of the web**		
2	**To learn concrete threats against web applications**		
3	**Be able to learn common web attacks and countermeasures.**		
Pre-Requisite:			
Sl. No.			
1.	**Basic concepts behind web applications, including HTTP, HTML, and JavaScript**		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Introduction to the web security landscape, and an overview of the most relevant threats. Understanding the security model of the web, and the recent evolution towards client-centric security.	**7**	**14**
02	Understanding the dangers of an insecure communication channel. Practical advice on deploying HTTPS, and dealing with the impact on your application. Insights into the latest evolutions for HTTPS deployments.	**7**	**14**
03	Understanding the interplay between authentication, authorization and session management. Practical ways to secure the authentication process, prevent authorization bypasses and harden session management mechanisms.	**8**	**14**
04	Investigation of injection attacks over time. Understanding the cause	**7**	**14**

	behind both server-side and client-side injection attacks. Execution of common injection attacks, and implementation of various defenses.		
05	Overview of current best practices for building secure web applications.	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:
Based on the curriculum as covered by subject teacher.

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Gene Spafford and Simson Garfinkel	Web Security, Privacy & Commerce	2nd	O'Reilly

Reference Books:

Ben Walther and Paco Hope	Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast		O'Reilly

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-IV

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject :Introduction to Information Security**			
Course Code: BITCN401		**Semester: 4**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 1 hr./week		**Attendance : 5**	
Practical: 0		**Continuous Assessment: 25**	
Credit: 4		**Practical Sessional internal continuous evaluation: NA**	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	This introductory course is aimed at giving basic understanding about system security.		
2.	This entry-level course covers a broad spectrum of security topics and is based on real-life examples to create system security interest in the students		
3.	A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.		
Objective:			
Sl. No.			
1.	Develop an understanding of information assurance as practiced in computer operating systems, distributed systems, networks and representative applications.		
2.	Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.		
3.	Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.		
4.	Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges		
Pre-Requisite:			
Sl. No.			
●	Not Required		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Information and Network Security fundamentals** Overview of Networking Concepts Basics of Communication Systems, Transmission Media,	**16**	**20**

	Topology and Types of Networks, TCP/IP Protocol, Wireless Networks, The Internet Information Security Concepts Information Security Overview: Background and Current Scenario, Types of Attacks, Goals for Security, E-commerce Security Security Threats and Vulnerabilities Overview of Security threats, Weak / Strong Passwords and Password Cracking, Insecure Network connections, Malicious Code Cybercrime and Cyber terrorism Cryptography Introduction to Cryptography, Digital Signatures, Public Key infrastructure, Applications of Cryptography, Tools and techniques of Cryptography		
02	**Security Management** Security Management Practices Overview of Security Management, Security Policy, Risk Management, Ethics and Best Practices Security Laws and Standards Security Assurance, Security Laws, International Standards, Security Audit	**8**	**10**
03	**Information and Network Security** Server Management and Firewalls User Management, Overview of Firewalls, Types of Firewalls, DMZ and firewall features Security for VPN and Next Generation Technologies VPN Security, Security in Multimedia Networks, Various Computing Platforms: HPC, Cluster and Computing Grids, Virtualization and Cloud Technology and Security	**6**	**20**
04	**System and Application Security** Security Architectures and Models Designing Secure Operating Systems, Controls to enforce security services, Information Security Models System Security Desktop Security, Email security, Database Security	**6**	**20**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

List of Books
Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
B. A. Forouzan	Data Communications and Networking	3rd Ed	TMH
A. S. Tanenbaum	Computer Networks	4th Ed	Pearson Education/PHI
Reference Books:			
W. Stallings	Data and Computer Communications	5th Ed	PHI/ Pearson Education
Atul Kahate	Cryptography & Network Security		TMH

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions (MCQ only with the correct answer)		Subjective Questions			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	1 to 4	10	10				
B	1 to 4			5	3	5	60
C	1 to 4			5	3	15	

5. Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
6. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Object-Oriented Programming with Java and Object-Oriented Programming with Java Lab	
Course Code: BITCNS402 & BITCNS492	**Semester: 4**
Duration: 36	**Maximum Marks: 100+100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical:4 hrs./week	**Continuous Assessment:25**
Credit: 3+2	**Practical Sessional internal continuous evaluation:40**
	Practical Sessional external examination:60

Aim:

Sl. No.	
1.	To understand Basic concepts of OOPs
2.	To Learn programming by class and object model
3.	Get knowledge Java programming

Objective:

Sl. No.	
1.	To learn the fundamentals of Java programming such as data types, variables and arrays.
2.	To study the syntax and necessity of decision making and iterative statements.
3.	To create a class and invoke the methods.
4.	To instigate programming in overloading of methods.
5.	To emphasize the concept of packages.
6.	To learn the exception handling routines.

Pre-Requisite:

Sl. No.	
1.	The fundamental point in learning programming
2.	Basic knowledge of algorithms and procedural programming

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction:**	**12**	**20**

	Why object orientation, History and development of object oriented programming language, concepts of object oriented programming language. Difference between OOP and other conventional programming – advantages and disadvantages. Data types, variables. Array, operators. String, I/O. Control statements. Object oriented design: Major and minor elements, class fundamentals. Declaring objects, instantiation of class, introducing methods. Constructing objects using constructor. Static variable, constants. Visibility modifiers.		
02	**Object Properties:** Introduction to basic features of a class (encapsulation, polymorphism etc) Data field encapsulation. Passing objects to methods. Array of objects, 'This' keyword Relationships among objects: aggregation, composition, dependency, links. Relationship among classes: association, aggregation. Meta class, meta object. Grouping constructs.	**12**	**25**
03	**Basic concepts of object oriented programming using Java:** Using objects as parameters, closure look at argument passing, returning objects. Introducing access control, Final keyword, garbage collection, Nested and inner classes. Class abstraction and encapsulation, Overloading of methods (overloading of constructor). Super class, subclasses, super keyword, inheritance, types, member access. Multilevel hierarchy, process of constructor calling in inheritance. Overriding methods, overriding vs. overloading, polymorphism. Abstract class, interface & comparison between abstract class and interface Packages, importing packages. Exception handling basics, types, using try &catch, throw, throws & finally. Threading, synchronization & priorities, thread class, creating thread. Basic applet programming. Life cycle.	**12**	**25**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**
Practical: **Skills to be developed:**			

Intellectual skills:

1. Students will be able to implement basic data structure and control statements in object oriented programming.
2. Student will be able to design class with its basic features.
3. Students can write programs using Java to implement OOP
4. Student will be able to design object oriented programs with the concept of object, class, abstraction, encapsulation, inheritance etc. to provide flexibility, modularity and re-usability in programming.
5. They can also be able to design Meta classes and grouping construct.

List of Practical:

1. Introduction to Java and JDK
2. Java Fundamentals - Data Types, Control Loops
3. Java Fundamentals - Wrapper Classes, Arrays
4. Classes and Objects 5 Inheritance
5. Abstract Class & Interface
6. File I/O and Exception Handling
7. Graphical User Interface (GUI) Programming with Java Swing
8. Applets
9. Java Threads

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Rambaugh, James Michael, Blaha	Object Oriented Modelling and Design		Prentice Hall
Patrick Naughton, Herbert Schildt	The complete reference-Java2		TMH

Reference Books:

Sourav Sahay	”Object-Oriented Programming with C++		Oxford
Blaha, Rumbaugh	Object-Oriented Modeling and Design with UML		Pearson Ed
. Ali Bahrami	Object Oriented System Development		Mc Graw Hill

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	**Computer with moderate configuration**
2.	**JDK**

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 3**	**10**	**10**				**60**
B	**1 to 3**			**5**	**3**	**5**	
C	**1 to 3**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions

should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	All	1	10	10
B	All	5	5	3
C	All	15	3	3

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Note Book	**10**	
On Spot Experiment	**40**	
Viva voce	**10**	**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Secure Software Design & Enterprise Computing	
Course Code: BITCN403	**Semester: 4**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 1 hr./week	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 4	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:

Sl. No.	
1.	To gain knowledge of computer networks.
2.	To gain knowledge of several layers and network architectures
3.	To gain knowledge of communication through networks, protocols and alghorithms.

Objective:

Sl. No.	
1.	Understand the division of network functionalities into layers.
2.	Be familiar with the components required to build different types of networks Be exposed to the required functionality at each layer
3.	Learn the flow control and congestion control algorithms

Pre-Requisite:

Sl. No.	
1.	Understanding of algorithms
2.	Understanding of basic computer architecture

Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Defining computer security, the principles of secure software, trusted computing base, etc, threat modelling, advanced techniques for mapping security requirements into design specifications. Secure software implementation, deployment and ongoing management.	**7**	**14**

02	Software design and an introduction to hierarchical design representations. Difference between high-level and detailed design. Handling security with high-level design. General Design Notions. Security concerns designs at multiple levels of abstraction, Design patterns, quality assurance activities and strategies that support early vulnerability detection, Trust models, security Architecture & design reviews.	**7**	**14**
03	Software Assurance Model: Identify project security risks & selecting risk management strategies, Risk Management Framework, Security Best practices/ Known Security Flaws, Architectural risk analysis, Security Testing & Reliability (Penn testing, Risk- Based Security Testing, Abuse Cases, Operational testing , Introduction to reliability engineering, software reliability, Software Reliability approaches, Software reliability modelling.	**7**	**14**
04	Software Security in Enterprise Business: Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, including public key cryptography, data encryption standard (DES), advanced encryption standard (AES), algorithms for hashes and message digests. Authentication, authentication schemes, access control models, Kerberos protocol, public key infrastructure (PKI), protocols specially designed for e-commerce and web applications, firewalls and VPNs. Management issues, technologies, and systems related to information security management at enterprises.	**8**	**14**
05	Security development frameworks. Security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and e-service systems, as well as the technologies required to develop secure information systems for enterprises, policies and regulations essential to the security of enterprise information systems.	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination		**30**
	Total:		**100**
Assignments: Adhered to theory curriculum as conducted by the subject teacher.			

List of Books
Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
W. Stallings	Cryptography and network security: Principles and practice	Fifth	Upper Saddle River, NJ: Prentice Hall
C. Kaufman, r. Perlman, & M. Speciner	Network security: Private communication in a public world	Second	Upper Saddle River, NJ:Prentice HalL
C. P. Pfleeger, S. L. Pfleeger	Security in Computing	Fourth	Upper Saddle River, NJ:Prentice Hall
Reference Books:			
Gary McGraw	Software Security: Building Security		Addison-Wesley
M. Merkow, & J. Breithaupt	Information security: Principles and practices.		Upper Saddle River, NJ:Prentice Hall

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions (MCQ only with the correct answer)		Subjective Questions			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**

B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** DBMS and SQL injection Attack and DBMS and SQL injection Attack Lab			
Course Code: BITCNS404 + BITCNS494		**Semester: 4**	
Duration: 36 Hrs.		**Maximum Marks: 100 + 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance : 5**	
Practical: 4 hrs./week		**Continuous Assessment: 25**	
Credit: 3 + 2		**Practical Sessional internal continuous evaluation: 40**	
		Practical Sessional external examination: 60	
Aim:			
Sl. No.			
1.	To gain knowledge of computer networks.		
2.	To gain knowledge of several layers and network architectures		
3.	To gain knowledge of communication through networks, protocols and alghorithms.		
Objective:			
Sl. No.			
1.	Understand the division of network functionalities into layers.		
2.	Be familiar with the components required to build different types of networks Be exposed to the required functionality at each layer		
3.	Learn the flow control and congestion control algorithms		
Pre-Requisite:			
Sl. No.			
1.	Understanding of algorithms		
2.	Understanding of basic computer architecture		
Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**

01	**Database Management System Concepts** Introduction, Significance of Database, Database System Applications; Data Independence; Data Modeling for a Database; Entities and their Attributes, Entities, Attributes, Relationships and Relationships Types, Advantages and Disadvantages of Database Management System, DBMS Vs RDBMS	**3**	**6**
02	**Database System Architecture** Three Level Architecture of DBMS, The External Level or Subschema, The Conceptual Level or Conceptual Schema, The Internal Level or Physical Schema, Mapping; MySQL Architecture; SQL Server 2000 Architecture; Oracle Architecture; Database Management System Facilities, Data Definition Language, Data Manipulation Language; Database Management System Structure, Database Manager, Database Administrator, Data Dictionary; Distributed Processing, Information and Communications Technology System (ICT), Client / Server Architecture	**3**	**6**
03	**Database Models and Implementation** Data Model and Types of Data Model, Relational Data Model, Hierarchical Model, Network Data Model, Object/Relational Model, Object-Oriented Model; Entity-Relationship Model, Modeling using E-R Diagrams, Notation used in E-R Model, Relationships and Relationship Types; Associative Database Model	**3**	**6**
04	**File Organization for Conventional DBMS** Storage Devices and its Characteristics, Magnetic Disks, Physical Characteristics of Disks, Performance Measures of Disks, Optimization of Disk-Block Access; File Organization, Fixed-Length Records, Variable-Length Records, Organization of records in files; Sequential file Organization; Indexed Sequential Access Method (ISAM); Virtual Storage Access Method (VSAM)	**4**	**7**
05	**An Introduction to RDBMS** An informal look at the relational model; Relational Database Management System; RDBMS Properties, The Entity-Relationship Model; Overview of Relational Query Optimization; System Catalog in a Relational DBMS, Information Stored in the System Catalog, How Catalogs are Stored	**3**	**6**

06	**SQL – 1** Categories of SQL Commands; Data Definition; Data Manipulation Statements, SELECT - The Basic Form, Subqueries, Functions, GROUP BY Feature, Updating the Database, Data Definition Facilities	**3**	**6**
07	**SQL – 2** Views; Embedded SQL *, Declaring Variables and Exceptions, Embedding SQL Statements; Transaction Processing, Consistency and Isolation, Atomicity and Durability	**3**	**7**
08	**Relational Algebra** Basic Operations, Union (U), Difference (-), Intersection (), Cartesian Product (x); Additional Relational Algebraic Operations, Projection (), Selection (), JOIN ( ), Division ()	**3**	**7**
09	**Relational Calculus** Tuple Relational Calculus, Semantics of TRC Queries, Examples of TRC Queries; Domain Relational Calculus; Relational ALGEBRA vs Relational CALCULUS	**3**	**6**
10	**Normalization** Functional Dependency; Anomalies in a Database; Properties of Normalized Relations; First Normalization; Second Normal Form Relation; Third Normal Form; Boyce-Codd Normal Form (BNCF); Fourth and Fifth Normal Form	**4**	**7**
11	**SQL Injection** Introduction to Injection Attacks; Data Store Injection; Introduction to XML, JavaScript and SQL injection attacks; Different Statement Injection; UNION Operator; Database Fingerprinting	**4**	**6**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination		**30**
	Total:		**100**

Practical:
Skills to be developed:
Intellectual skills:

1. Identify the components required to build different types of networks

2. Choose the required functionality at each layer for given application
3. Identify solution for each functionality at each layer
4. Trace the flow of information from one node to another node in the network

List of Practical: Based on theory lectures.
Assignments:
Adhered to theory curriculum as conducted by the subject teacher.

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
A.Silberschatz, H.F. Korth, S.Sudarshan	Database System Concepts	6th Edition	McGraw Hill
Raghurama Krishnan, Johannes Gehrke	Database Management Systems	3rd edition	McGrawHill Education
Reference Books:			
Bipin C. Desai	Introduction to Database Systems	11th edition	West Group
Hector Garcia-Molina,Jeffrey D. Ullman, Jennifer Widom	Database Systems: The Complete Book	2nd edition	Pearson

List of equipment/apparatus for laboratory experiments:

Sl. No.	
●	Computer

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 11**	**10**	**10**				
B	**1 to 11**			**5**	**3**	**5**	**60**
C	**1 to 11**			**5**	**3**	**15**	

4. Only multiple choice type questions (MCQ) with one correct answer are to be set in the

objective part.

5. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Assignments	**10**	
On Spot Experiment	**40**	
Viva voce	**10**	**60**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** e-Governance			
Course Code:BITCNS405		**Semester: 4**	
Duration: 36 Hrs		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial:1 hr./week		Attendance: 5	
Practical:0		Continuous Assessment: 25	
Credit:4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1	**This course aims to provide a basic understanding of e-governance strategies.**		
Objective:			
Sl. No.			
1	**To familiarizes the students with the concept of e-Governance.**		
2	**To teach how an effective strategic plan can be developed through a process.**		
3	**To teach how to develop the vision, goals and objectives for e-governance.**		
Pre-Requisite:			
Sl. No.			
	None		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Basics Of e-Governance** e-Governance: Policies, Strategies and Frameworks, Information Society, Concepts and Principles,Introduction to ICT and e-Governance, Technology and Society, The State and Governance, Development Policies and Globalization, Business Information Systems, Government Process Re-engineering(GPR).	**7**	**14**
02	**e-Governance Architecture** Planning and Implementing e-Governance, Legal Framework of e-Governance, Enterprise Business Architecture Development, Public Management and Administration, Business Models for Implementation of e-Governance, Change Management and Capacity Building in, e-Governance Projects, Data System Infrastructural	**8**	**18**

	preparedness, Infrastructural preparedness :Legal , Human , Institutional , Technological, Leadership and Strategic Planning		
03	**e-Governance Technologies** Usability of Virtual Environments, Information Management and Digital Archiving, Design and development of Data Exchange Layer for, Government Information Systems, Technology and Individual: Ethics of, Law and Technology, Security and Privacy in a Networked World, Internet of Things: Smart Devices, Processes and Services, Legal Aspects of, Software and Database Protection,Introduction to Development in Cloud, Technical Change and Techno-economic Paradigms.	**8**	**18**
04	**Comparative Study of e-Governance Portals around the Globe** Study of e-Governance models of different countries , Finding the gaps in each model, E-Governance Maturity Model, Case Studies of e-Governance outside India	**7**	**10**
05	**e-Governance Product and Services in India supported by NIC** Overview of National e_Governance Plan(NeGP) , e-POST, AGMARKNET ,Examination Results Portal , Gyandoot e-Governance Project, JUDIS, Indian Passport portal, RuralBazar, Value Added Tax (VAT)	**6**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:
Based on the curriculum as covered by the subject teacher.

List of Books
Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Shirin Madon	E-governance for Development : A Focus on India		Palgrave Macmillan
Ashok Agarwal	E-governance : case studies		University Press India
Reference Books:			
Subhash C. Bhatnagar	E-government : from vision to implementation: a practical guide with case studies		SAGE
C.S.R. Prabhu	E-Governance: Concepts And Case Studies		PHI

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

End Semester Examination Scheme.		**Maximum Marks-70.**		**Time allotted-3hrs.**			
Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Project II**	
Course Code: BITCNS481	**Semester: 4**
Duration: 36 Hrs	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: 100
Tutorial: 0	Attendance:
Practical: 2 hrs./week	Continuous Assessment:
Credit: 1	Practical Sessional internal continuous evaluation: 40
	Practical Sessional external examination: 60
Contents	
Students will do projects on application areas of latest technologies and current topics of societal relevance.	

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-V

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Introduction to Theory of Computer			
Course Code: BITCNS501		**Semester: 5**	
Duration: 36 Hours		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		End Semester Exam: 70	
Tutorial: 1 hr./week		Attendance : 5	
Practical: 0		Continuous Assessment: 25	
Credit: 4		Practical Sessional internal continuous evaluation: NA	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1	To gain knowledge of automata theory.		
2	To understand the theoretical computer science.		
Objective:			
Sl. No.			
1	Study various types of finite automata.		
2	Understand the challenge of theoretical computer science and it's application.		
Pre-Requisite:			
Sl. No.	**None**		
Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Alphabets, Strings and Languages; Automata and Grammars, Deterministic finite Automata (DFA)-Formal Definition, Simplified notation: State transition graph, Transition table, Language of DFA, Nondeterministic finite Automata (NFA), NFA with epsilon transition, Language of NFA, Equivalence of NFA and DFA, Minimization of Finite Automata, Distinguishing one string from other, Myhill-Nerode Theorem.	**7**	**14**
02	**Regular expression[8L]** Definition, Operators of regular expressions and their precedence, Algebraic laws for Regular expressions, Kleen's Theorem, Regular expression to FA, DFA to Regular expression, Arden Theorem, Non Regular Languages, Pumping Lemma for regular Languages . Application of Pumping Lemma, Closure properties of Regular Languages, Decision properties of Regular Languages, FA with output: Moore and Mealy machine, Equivalence of Moore and Mealy Machine, Applications and Limitation of FA.	**8**	**14**

03	**Context free grammar and Context Free Languages** Definitions, Examples, Derivation , Derivation trees, Ambiguity in Grammar, Inherent ambiguity, Ambiguous to Unambiguous CFG, Useless symbols, Simplification of CFGs, Normal forms for CFGs: CNF and GNF, Closure properties of CFLs, Decision Properties of CFLs: Emptiness, Finiteness and Membership, Pumping lemma for CFLs.	**7**	**14**
04	**Push Down Automata** Description and definition, Instantaneous Description, Language of PDA, Acceptance by Final state, Acceptance by empty stack, Deterministic PDA, Equivalence of PDA and CFG, CFG to PDA and PDA to CFG, Two stack PDA	**7**	**14**
05	**Turing machines** Basic model, definition and representation, Instantaneous Description, Language acceptance by TM, Variants of Turing Machine, TM as Computer of Integer functions, Universal TM, Church's Thesis, Recursive and recursively enumerable languages, Halting problem, Introduction to Undecidability, Undecidable problems about TMs. Post correspondence problem (PCP), Modified PCP, Introduction to recursive function theory.	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Daniel I.A.Cohen	Introduction to computer theory	8th Edition	John Wiley Publications
Lewis & Papadimitriou	Elements of the theory of computation		PHI
Hoperoft, Aho, Ullman	Introduction to Automata theory, Language & Computation	3 rd Edition	Pearson Education

Reference Books:

P. Linz	An Introduction to Formal Language and Automata	4th edition	Publication Jones Bartlett

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

1. Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Block Chain Technology	
Course Code: BITCNS502	**Semester: 5**
Duration: 36 Hours	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	End Semester Exam: 70
Tutorial: 1 hr./week	Attendance : 5
Practical: 0	Continuous Assessment: 25
Credit: 4	Practical Sessional internal continuous evaluation: NA
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1	This course aims to provide conceptual understanding of the function of Blockchains. Also to explain what the technology is and how it works at a high level.

Objective:	
Sl. No.	
1	To understand what Blockchain is and why it is used
2	To be able to explain the different components involved within Blockchain
3	Evaluate the setting where a blockchain based structure may be applied, its potential and its limitations.

Pre-Requisite:	
Sl. No.	**No prior experience is required**

Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Introduction to blockchain, structure and operational aspects of Bitcoin blockchain, different types of blockchains.	**3**	**10**
02	**Ethereum Blockchain** Innovation of the Ethereum blockchain, review its protocol, and explore the payment model for code execution.	**5**	**10**
03	**Algorithms & Techniques** Concept of asymmetric key encryption, concept of hashing, different techniques and algorithms to manage the integrity of transactions and blocks in blockchain.	**7**	**10**
04	**Trust Essentials** Different elements of trust in blockchain, Consensus protocol.	**7**	**10**
05	**Setting Up Development Environment Using Hyperledger Composer** Setting up Development Environment using Composer, Introduction to Hyperledger Fabric, Hyperledger Fabric Model,	**8**	**20**

	Various ways to create Hyperledger Fabric Blockchain Network.		
06	**Prospects Of Blockchain** Blockchain transforming business and professionalism, Discussing practical use-cases of Blockchain, Real case scenarios of Blockchain, How governments around the world are using Blockchain.	**6**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Based on the curriculum as covered by subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Melanie Swan	Blockchain: Blueprint for a New Economy		O'Reilly Media, Inc.

Reference Books:

Alex Tapscott and Don Tapscott	Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World		Penguin

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions (MCQ only with the correct answer)		Subjective Questions			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 6**	**10**	**10**				
B	**1 to 6**			**5**	**3**	**5**	**60**
C	**1 to 6**			**5**	**3**	**15**	

1. Only multiple choice type question (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered

A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Network Security and Network Security Lab	
Course Code: BITCNS503 and BITCNS593	**Semester: 5**
Duration: 36 Hrs.	**Maximum Marks: 100 + 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 4 hrs./week	**Continuous Assessment: 25**
Credit: 3+2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60

Aim:

Sl. No.	
1.	To develop basic skills of secure network architecture and explain the theory behind the security of different cryptographic algorithms.
2.	To describe common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.
3.	To study about message authentication and hash functions

Objective:

Sl. No.	
1.	Classify the symmetric encryption techniques
2.	Illustrate various Public key cryptographic techniques
3.	Evaluate the authentication and hash algorithms.
4.	Summarize the intrusion detection and its solutions to overcome the attacks. Basic concepts of system level security

Pre-Requisite:

Sl. No.	
	Fundamental knowledge of networking

Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Security in Computing Environment**	**4**	**7**

	Need for Security, Security Attack, Security Services, Information Security, Methods of Protection.		
02	**Basics of Cryptography [3L]** Terminologies used in Cryptography, Substitution Techniques, Transposition Techniques.	**4**	**8**
03	**Encryption and Decryption** Characteristics of Good Encryption Technique, Properties of Trustworthy Encryption Systems, Types of Encryption Systems, Confusion and Diffusion, Cryptanalysis.	**4**	**8**
04	**Key Encryption** Data Encryption Standard (DES) Algorithm, Double and Triple DES, Security of the DES, Advanced Encryption Standard (AES) Algorithm, DES and AES Comparison. Characteristics of Public Key System, RSA Technique, Key Exchange, Diffie-Hellman Scheme, Cryptographic Hash Functions, Digital Signature, Certificates, Certificate Authorities	**4**	**8**
05	**Network Security** Network Concepts, Threats in Networks, Network Security Controls.	**4**	**8**
06	**IP Security** Overview of IP Security (IPSec), IP Security Architecture, Modes of Operation, Security Associations (SA), Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange.	**4**	**8**
07	**Web Security** Web Security Requirements, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Electronic Transaction (SET).	**4**	**7**
08	**Electronic Mail Security** Threats to E-Mail, Requirements and Solutions, Encryption for Secure E-Mail, Secure E-Mail System.	**4**	**8**
09	**Firewalls** Firewalls – Types, Comparison of Firewall Types, Firewall Configurations	**4**	**8**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester	**4**	**30**

	Examination		
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

Hands on experience of network security

List of Practical: Based on theory lectures.

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Larry L. Peterson, Bruce S. Davie	Computer Networks: A Systems Approach	Fifth	Morgan Kaufmann Publishers
James F. Kurose, Keith W. Ross	Computer Networking – A Top-Down Approach Featuring the Internet	Fifth	Pearson Education
Reference Books:			
William Stallings	Cryptography and network security: principles and practice		Pearson Education
Roberta Bragg, Mark Rhodes-Ousley	Network Security: The Complete Reference		TMH

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Rack server composed of ten servers
2.	Tower server
3.	Firewall, router, UPS, Computer with moderate configuration and high speed

	internet.								
End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.									
Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**					
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks		
A **B** **C**	**1 to 9** **1 to 9** **1 to 9**	**10**	**10**	**5** **5**	**3** **3**	**5** **15**	**60**		
• Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part. • Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.									
Examination Scheme for end semester examination:									
Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**					
A	**All**	**1**	**10**	**10**					
B	**All**	**5**	**5**	**3**					
C	**All**	**15**	**5**	**3**					
Examination Scheme for Practical Sessional examination:									
Practical Internal Sessional Continuous Evaluation									
Internal Examination:									
Continuous evaluation				**40**					
External Examination: Examiner-									
Signed Lab Assignments			**10**						
On Spot Experiment			**40**						
Viva voce			**10**	**60**					

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Information and Coding Theory	
Course Code: BITCNS504 A	**Semester: 5**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1	Introduced to the basic notions of information and channel capacity.
2	To introduce information theory, the fundamentals of error control coding techniques and their applications, and basic cryptography.
3	To provide a complementary U/G physical layer communication
4	**to convolutional and block codes, decoding techniques, and automatic repeat request (ARQ) schemes.**

Objective:	
Sl. No.	
1.	Understand how error control coding techniques are applied in communication systems.
2.	Able to understand the basic concepts of cryptography.
3.	To enhance knowledge of probabilities, entropy, measures of information.

Pre-Requisite:	
Sl. No.	
1.	Probability and Statistics

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Information Theory** Entropy, its characterization and related properties, Huffman codes, Shannon-Fano coding, robustness of coding techniques, Information measure-noiseless coding, discrete memoryless channel – channel capacity, fundamental theorem of information theory.	**9**	**10**

02	**Coding Theory** Error correcting codes: minimum distance principles, Hamming bound, general binary code, group code, linear group code Convolution encoding: algebraic structure, Gilbert bound Threshold decoding: threshold decoding for block codes Cyclic binary codes: BCH codes, generalized BCH code and decoding, optimum codes, concepts of non-cyclic codes.	**9**	**20**
03	**Combinatorial Designs** Definitions of BIBD, Hadamard Designs, Latin Squares, Mutually Orthogonal Latin Squares, Orthogonal Arrays. Constructions of codes using designs: Example: Hadamard codes.	**9**	**20**
04	**Network Coding** Fundamentals of Network Coding: Butterfly networks, graphs and networks. The max-flow min-cut theorem, the multi-source multicast problem, deterministic code design for network coding, randomized network coding application of network coding.	**9**	**20**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
J. A. Thomas and T. M. Cover	Elements of information theory		**Wiley**
J. H. van Lint	Introduction to Coding Theory	**3rd**	Springer

Reference Books:

F. J. MacWilliams and N.J. Sloane	Theory of Error Correcting Codes, Parts I and II		
D. Stinson	Combinatorial Designs: Constructions and Analysis		Springer

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	Unit	Objective Questions	Subjective Questions

		(MCQ only with the correct answer)					
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 4**	**10**	**10**				
B	**1 to 4**			**5**	**3**	**5**	**60**
C	**1 to 4**			**5**	**3**	**15**	

5. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
6. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Advanced Unix and Shell Programming			
Course Code: BITCNS504 B		**Semester: 5**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance : 5**	
Practical: 0		**Continuous Assessment: 25**	
Credit: 3		**Practical Sessional internal continuous evaluation: NA**	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1	To provide the knowledge and skills to make effective use of a wide range of standard UNIX programming and development tools.		
Objective:			
Sl. No.			
1.	Understand Operating System concepts		
2.	Use System calls and memory management		
3.	Do Network configuration and security management in Unix		
Pre-Requisite:			
Sl. No.			
1.	Knowledge of the UNIX Operating System.		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction of UNIX and Shell** Introduction, History, Architecture, Experience the Unix environment, Basic Command sls, cat, cal, date, calendar, who, printf, tty, sty, uname, passwd, echo, tput, bc, script, spell and ispell, Introduction to Shell Scripting, Shell Scripts, read, Command Line Arguments, Exit Status of a Command, The Logical Operators && and ||, exit, if, and case conditions, expr, sleep and wait, while, until, for,$,@, redirection, set and shift, trap.	**7**	**14**
02	**UNIX File System** The file, what's in a filename? The parent-child relationship, pwd,	**7**	**14**

	the Home directory, absolute path names, using absolute pathnames for a command, cd, mkdir, rmdir, Relative path names, The UNIX file system. Basic File Attributes: Is – l, the –d option, File Permissions, chmod, Security and File Permission, users and groups, security level, changing permission, changing ownership and group, File Attributes, More file attributes: hard link, symbolic link, umask, find.		
03	**Simple Filters** Pr, head, tail, cut, paste, sort, uniq, tr commands, Filters using Regular Expression: grep, Regular Expression, egrep, fgrep, sed instruction, Line Addressing, Inserting and Changing Text, Context addressing, writing selected lines to a file, the– f option, Substitution, Properties of Regular Expressions.	**7**	**14**
04	**Awk and Advanced Shell Programming** Awk-Advanced Filters: Simple awk Filtering, Splitting a Line into Fields, printf, the Logical and Relational Operators, Number Processing, Variables, The –f option, BEGIN and END positional Parameters, getline, Built-invariables, Arrays, Functions, Interface with the Shell, Control Flow. The sh command, export, the Command, Conditional Parameter Substitution, Merging Streams, Shell Functions, eval, Exec Statement and Examples.	**7**	**14**
05	**Process and System Administration** Process basics, PS, internal and external commands, running jobs in background, nice, at and batch, cron, time commands, Essential System Administration root, administrator's privileges, startup & shutdown, managing disk space, cpio, tar, Customizing the Environment : System Variables, profile, sty, Aliases, Command History, On-line Command Editing.	**8**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Forouzan Behrouz A	UNIX and Shell Programming		**Thomson Press**

Reference Books:

Stephen Kochan		**Unix Shell Programming**				SAMS	
End Semester Examination Scheme.			**Maximum Marks-70.**		**Time allotted-3hrs.**		
Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A **B** **C**	**1 to 5** **1 to 5** **1 to 5**	**10**	**10**	 **5** **5**	 **3** **3**	 **5** **15**	 **60**
7. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part. 8. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.							

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Human Computer Interaction	
Course Code: BITCNS504 C	**Semester: 5**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	The aim of this course is to teach students to design user interfaces based on the capabilities of computer technology and the needs of human factors.

Objective:	
Sl. No.	
1.	The objective of this course is to give an introduction to the key areas, approaches and developments in the field.
2.	Explain the capabilities of both humans and computers from the viewpoint of human information processing.
3.	Apply an interactive design process and universal design principles to designing HCI systems.

Pre-Requisite:	
Sl. No.	
1.	Knowledge of Software Engineering

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**FOUNDATIONS OF HCI** The Human: I/O channels – Memory – Reasoning and problem solving; The computer: Devices – Memory – processing and networks; Interaction: Models – frameworks – Ergonomics – styles – elements – interactivity- Paradigms.	**12**	**20**
02	**DESIGN & SOFTWARE PROCESS** Interactive Design basics – process – scenarios – navigation – screen design – Iteration and prototyping. HCI in software process – software life cycle – usability engineering – Prototyping in practice – design rationale. Design rules – principles, standards, guidelines, rules. Evaluation Techniques – Universal Design.	**12**	**30**

03	**MODELS AND THEORIES** Cognitive models –Socio-Organizational issues and stakeholder requirements –Communication and collaboration models-Hypertext, Multimedia and WWW.	**12**	**20**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Alan Dix, Janet Finlay, Gregory Abowd, Russell Beale	Human Computer Interaction	**3rd**	**Pearson Education**
Brian Fling	Mobile Design and Development	**1st**	**O"Reilly Media Inc.**

Reference Books:

Bill Scott and Theresa Neil	**Designing Web Interfaces**	**1st**	O"Reilly

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 3**	**10**	**10**				
B	**1 to 3**			**5**	**3**	**5**	**60**
C	**1 to 3**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each**	**Question to be**	**Question to be**

		question	set	answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Multimedia & Graphics	
Course Code: BITCNS504 D	**Semester: 5**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:

Sl. No.	
1	To gain knowledge of working of display systems.
2	To enhance skill to execute variousScan Conversion algorithms in laboratory so as to draw Graphics primitives
3	Familiarization With 2D and 3D graphics.

Objective:

Sl. No.	
1	To understand the basics of computer graphics, different display devices and applications of computer graphics.
2	To learn about algorithmic development of graphics primitives like: point, line, circle, ellipse etc.
3	To impart knowledge of2D and 3D transformations on graphics objects.
4	To familiarize with 2D Viewing and different clipping methods

Pre-Requisite:

Sl. No.	
1.	Basic knowledge of mathematical logic and coordinate geometry.

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**

01	**Introduction to computer graphics & graphics systems** Overview of computer graphics, representing pictures, preparing, presenting & interacting with pictures for presentations; Visualization & image processing; RGB color model, direct coding, lookup table, storage tube graphics display, Raster scan display, 3D viewing devices, Plotters, printers, digitizers, Light pens etc.; Active & Passive graphics devices; Computer graphics software.	**3**	**2**
02	**Scan conversion** Line drawing algorithms; DDA algorithm, Bresenham's line algorithm, Circle generation algorithm; Ellipse generating algorithm; scan line polygon, fill algorithm, boundary fill algorithm, flood fill algorithm.	**4**	**10**
03	**2D transformation Basic transformations** Translation , rotation, scaling ; Matrix representations & homogeneous coordinates, transformations between coordinate systems; reflection shear; Transformation of points, lines , parallel lines, intersecting lines.	**4**	**8**
04	**2D Viewing** Viewing pipeline, Window to viewport Co-ordinate transformation, clipping operations, point clipping, line clipping, clipping circles , polygons & ellipse.	**5**	**10**
05	**3D transformation & viewing 3D transformations** Translation, rotation, scaling & other transformations. Rotation about an arbitrary axis in space, reflection through an arbitrary plane; general parallel projection transformation; clipping, viewport clipping, 3D viewing.	**4**	**8**
06	**Curves** Curve representation, surfaces, designs, Bezier curves, B-spline curves, end conditions for periodic B Spline curves, rational B-spline curves.	**4**	**8**
07	**Hidden surfaces Depth comparison** Z-buffer algorithm, Back face detection, BSP tree method, the Printer's algorithm, scan-line algorithm; Hidden line elimination, wire frame methods , fractal - geometry.	**4**	**8**
08	**Color & shading models** Light & color model, interpolative shading model, Texture.	**4**	**8**
09	**Multimedia Introduction to Multimedia** Concepts, uses of multimedia, hypertext and hypermedia. Image, video and audio standards. Audio: digital audio, MIDI, processing sound, sampling,	**4**	**8**

	compression. Video: MPEG compression standards, compression through spatial and temporal redundancy, inter-frame and intra-frame compression. Animation: types, techniques, key frame animation, utility, morphing. Virtual Reality concepts.		
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Hearn and Baker	Computer Graphics, C Version		**Pearson Education**

Reference Books:

Anirban Mukhopadhyay, Arup Chattopadhyay	**Introduction to Computer Graphics and Multimedia**		Vikas Publishing House

End Semester Examination Scheme. **Maximum Marks-70.** **Time allotted-3hrs.**

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 9**	**10**	**10**				
B	**1 to 9**			**5**	**3**	**5**	**60**
C	**1 to 9**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the

objective part.

2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security)
Subject: Industrial Training and Internship

Course Code: BITCNS581	**Semester: 5**
Duration: 4 Weeks	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: NA
Tutorial: 0	Attendance: NA
Practical: 0	Continuous Assessment: NA
Credit: 1	Practical Sessional internal continuous evaluation:40
	Practical Sessional external examination: 60

Aim:

Sl. No.	
1	To develop industrial understanding.
2	To develop understanding of project management.
3	To cope up with industry oriented real time project environment.

Objective:

Sl. No.	
1	To develop team work.
2	To develop understanding of project management.
3	To be able to implement real life software or hardware based projects.

Pre-Requisite:

Sl. No.	
1.	None

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Major Project I**	
Course Code: BITCNS582	**Semester: 5**
Duration: 40 Hours	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: NA
Tutorial: 0	Attendance: NA
Practical: 4 hrs./week	Continuous Assessment: NA
Credit: 2	Practical Sessional internal continuous evaluation:40
	Practical Sessional external examination: 60

Aim:	
Sl. No.	
1	To develop team work.
2	To develop understanding of project management.
3	To be able to implement real life software or hardware based projects.

Objective:	
Sl. No.	
1	To develop team work.
2	To develop understanding of project management.
3	To be able to implement real life software or hardware based projects.

Pre-Requisite:	
Sl. No.	
1.	None

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Semester-VI

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Elliptic Curve Cryptography			
Course Code: BITCNS601	**Semester: 6**		
Duration: 36 Hrs.	**Maximum Marks: 100**		
Teaching Scheme	**Examination Scheme**		
Theory: 3 hrs./week	**End Semester Exam: 70**		
Tutorial: 1 hr./week	**Attendance : 5**		
Practical: 0	**Continuous Assessment: 25**		
Credit: 4	**Practical Sessional internal continuous evaluation: NA**		
	Practical Sessional external examination: NA		
Aim:			
Sl. No.			
1.	The aim of this course is to teach students ECC technology with a diversified and comprehensive perspective.		
Objective:			
Sl. No.			
1.	The objective of this course is to give an introduction to the key areas, approaches and developments in the field of ECC.		
Pre-Requisite:			
Sl. No.			
1.	Knowledge of cryptography.		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Introduction to Elliptic Curve Cryptography: What is cryptography, What is an elliptic curve. Computing on elliptic curves: Group law and the point at infinity, Elliptic curves in SAGE. , Isomorphisms of elliptic curves:Singular curves, Definition and examples of isomorphisms, *j*-invariant. Endomorphisms and torsion: Endomorphisms, degree, separability, Examples: multiplication by *n*, Frobenius, Torsion points.	**6**	**10**
02	**Elliptic curves over finite fields** Size and structure of $E(\mathbf{F}_q)$: Structure of *n*-torsion, Legendre symbols and point counting, Hasse's theorem. Determining the group order and structure : Characteristic polynomial of Frobenius, Subfield curves, Supersingular curves .	**6**	**10**
03	**Elliptic curve cryptosystems**	**6**	**20**

	Encryption : Definition of secure encryption, Equivalence of semantic security and real-or-random security, ElGamal encryption, Attacks on ElGamal. Encryption and Signatures : Security of ElGamal encryption, Hybrid encryption, Definition of secure signatures, Schnorr identification and signatures . Signatures : Security of Schnorr signatures, ECDSA.		
04	**Discrete logarithm attacks** General attacks on the DLP: Pohlig-Hellman, Baby step-giant step, Pollard rho and lambda. The Menezes-Okamoto-Vanstone attack: Index calculus in finite fields, Weil pairing, MOV attack. Weak elliptic curves: Embedding degree, Supersingular curves, Anomalous curves	**6**	**10**
05	**Pairing-based cryptography** Key exchange and identity-based encryption: Joux 3-party key exchange, IBE definitions, Boneh-Franklin IBE scheme. IBE and Signatures: Security of Boneh-Franklin variant, Boneh-Lynn-Shacham signature scheme . Homomorphic Encryption : Homomorphic ElGamal, Boneh-Goh-Nissim encryption.	**6**	**10**
06	**Algorithms for ECC** Computing the Weil and Tate pairings: Divisors and functions, Defining the pairings, Properties of the pairings, Miller's algorithm. The CM Method of curve construction: Elliptic curves over **C,** Complex multiplication, Computing Hilbert class polynomials.	**6**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
Alfred Menezes, D.C. Hankerson, and S. A.	Guide to Elliptic Curve Cryptography		**Springer.**

Reference Books:

I. Blake, Gerald Seroussi, G. Seroussi, N. Smart	Elliptic Curves in Cryptography					Cambridge University Press	
End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.							
Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A **B** **C**	**1 to 6** **1 to 6** **1 to 6**	**10**	**10**	 **5** **5**	 **3** **3**	 **5** **15**	 **60**
1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part. 2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.							
Examination Scheme for end semester examination:							
Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**			
A	**All**	**1**	**10**	**10**			
B	**All**	**5**	**5**	**3**			
C	**All**	**15**	**5**	**3**			

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Cloud Security	
Course Code: BITCNS602	**Semester: 6**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 1 hr./week	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 4	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	The aim of this course is to teach students cloud security architectures that assures secure isolation of computer, network and storage infrastructures.

Objective:	
Sl. No.	
1.	To understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices.
2.	Able to identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud and evolve appropriate safeguards and countermeasures

Pre-Requisite:	
Sl. No.	
1.	Knowledge of web application development..

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.	**6**	**10**
02	Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud based IT services.	**6**	**10**
03	Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services.	**6**	**10**
04	Approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on-demand computing, shared resources, elasticity and measuring usage.	**6**	**10**
05	Design security architectures that assures secure isolation of	**6**	**20**

	physical and logical infrastructures including compute, network and storage, comprehensive data protection at all layers, end-to-end identity and access management, monitoring and auditing processes and compliance with industry and regulatory mandates.		
06	Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.	**6**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Vic (J.R.) Winkler	Securing The Cloud: Cloud Computing Security Techniques and Tactics		**Elsevier**
Reference Books:			
Thomas Erl	Cloud Computing Design Patterns		Prentice Hall

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 6**	**10**	**10**				
B	**1 to 6**			**5**	**3**	**5**	**60**
C	**1 to 6**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Examination Scheme for end semester examination:				
Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Steganography & Watermarking	
Course Code: BITCNS603A	**Semester: 6**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial:	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	Know the History and importance of watermarking and steganography
2.	Analyze Applications and properties of watermarking and steganography
3.	Demonstrate Models and algorithms of watermarking
4.	**Possess the passion for acquiring knowledge and skill in preserving authentication of Information**

Objective:	
Sl. No.	
1.	To learn about the watermarking models and message coding
2.	To learn about watermark security and authentication.
3.	To learn about stegnography. Perceptual models

Pre-Requisite:	
Sl. No.	
1.	Cryptography

Contents	**4 Hrs./week**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Chapter	Name of the Topic	Hours	Marks
01	**INTRODUCTION** Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems. WATERMARKING MODELS & MESSAGE CODING: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.	**7**	**14**
02	**WATERMARKING WITH SIDE INFORMATION & ANALYZING ERRORS:** Informed Embedding – Informed Coding – Structured dirty-paper codes – Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates	**7**	**14**
03	**PERCEPTUAL MODELS:** Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches – Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients	**7**	**14**
04	**WATERMARK SECURITY & AUTHENTICATION:** Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.	**8**	**14**
05	**STEGANOGRAPHY:** Steganography communication – Notation and terminology – Information theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis	**7**	**14**
	Sub Total:	**36**	**70**

	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker	Digital Watermarking and Steganography		Margan Kaufmann Publishers, New York
Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom	Digital Watermarking		Margan Kaufmann Publishers, New York
Reference Books:			
Michael Arnold, Martin Schmucker, Stephen D. Wolthusen	Techniques and Applications of Digital Watermarking and Contest Protection		Artech House, London

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the

objective part.

- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	All	1	10	10
B	All	5	5	3
C	All	15	5	3

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Multimedia Security			
Course Code: BITCNS603B		**Semester: 6**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 0		**Attendance : 5**	
Practical: 0		**Continuous Assessment: 25**	
Credit: 3		**Practical Sessional internal continuous evaluation: NA**	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	Aim of this course is to provide comprehensive knowledge and hands-on experience about multimedia systems and security technologies.		
Objective:			
Sl. No.			
1.	To understand basic cryptography consept in field of multimedia		
2.	To impart knowledge of data hiding and authentication.		
Pre-Requisite:			
Sl. No.			
1.	Basic Mathematics		
Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Basic Cryptography:** Basic cryptographic services- confidentiality- integrity verification – authentication– primitives for the services – one way functions - symmetric and asymmetric schemes- encryption –block ciphers and stream ciphers - hashing – authentication codes – digital signatures.	**12**	**20**
02	**Data hiding and authentication:** Data hiding algorithms and applications – steganography andsteganalysis- statistical techniques-authentication of audio, image and video data - digital rights management – watermark	**12**	**30**

	embedding and retrieval - digital fingerprinting – anti collusion codes-biometrics and digital forensics – biometric encryption - privacy preserving data mining.		
03	**Multimedia Encryption:** Protection of multimedia data during distribution – vulnerabilities and challenges– encryption schemes for audio, image and video data – streaming of encrypted multimedia – partial and progressive encryption techniques- signal processing in encrypted domain.	**12**	**20**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Borko Furht	DarkoKirovski, Multimedia Encryption and Authentication Techniques and Applications.		Auerbach Publications
Reference Books:			
Borko Furht Darko Kirovski	Multimedia Security Handbook.		CRC Press

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1,2**	**10**	**10**				

B **C**	**1,2** **1,2**			**5** **5**	**3** **3**	**5** **15**	**60**

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249
Department of Information Technology (In-house)

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** System Security			
Course Code: BITCNS603C		**Semester: 6**	
Duration: 36 Hrs.		**Maximum Marks: 100**	
Teaching Scheme		**Examination Scheme**	
Theory: 3 hrs./week		**End Semester Exam: 70**	
Tutorial: 1 hr./week		**Attendance : 5**	
Practical: 0		**Continuous Assessment: 25**	
Credit: 4		**Practical Sessional internal continuous evaluation: NA**	
		Practical Sessional external examination: NA	
Aim:			
Sl. No.			
1.	This course introduces the basics of system security.		
Objective:			
Sl. No.			
1.	The student will be introduced to operating system vulnerabilities and threats and how to safeguard system from those vulnerabilities and threats.		
Pre-Requisite:			
Sl. No.			
1.	Fundamental knowledge in Security		
Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Intruders:** Intruders, Intrusion detection, Intrusion prevention.	**7**	**14**
02	**Malicious Software:** Virus and related threats, Virus countermeasures.	**7**	**14**
03	**Firewalls:** Firewall design principles, Trusted systems.	**8**	**14**
04	**Software Vulnerabilities:** Phishing, Buffer overflow (BOF), Heap overflow, Format string attacks, Cross-site scripting (XSS), SQL Injection.	**7**	**14**
05	Malware Threats and Security Solutions	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester	**4**	**30**

	Examination		
	Total:	**40**	**100**

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Michael T. Goodrich and Roberto Tamassia	Introduction to Computer Security		Addison Wesley

Reference Books:

William Stallings	Network Security Essentials: Applications and Standards	4th edition	Prentice Hall

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

1. Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
2. Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Syllabus of B.Sc. in Information Technology (Cryptography and Network Security)
(Effective from academic session 2019-20)

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject:** Grand Viva	
Course Code: BITCNS681	**Semester: 6**
Duration: 40 Hours	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: NA
Tutorial: 0	Attendance: NA
Practical: 0	Continuous Assessment: NA
Credit: 1	Practical Sessional internal continuous evaluation:0
	Practical Sessional external examination: 100

Name of the Course: B.Sc. in Information Technology (Cryptography and Network Security) **Subject: Major Project II**	
Course Code: BITCNS682	**Semester: 6**
Duration: 40 Hours	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	End Semester Exam: NA
Tutorial: 0	Attendance: NA
Practical: 4	Continuous Assessment: NA
Credit: 4	Practical Sessional internal continuous evaluation:40
	Practical Sessional external examination: 60
Aim:	
Sl. No.	
1	To develop team work.
2	To develop understanding of project management.
3	To be able to implement real life software or hardware based projects.
Objective:	
Sl. No.	
1	To develop team work.
2	To develop understanding of project management.
3	To be able to implement real life software or hardware based projects.
Pre-Requisite:	
Sl. No.	
1.	None