Faculty of Computing Science and Engineering
Department of Computer Science and Cybersecurity

Course Contents
BSc. Cybersecurity
SCHEDULE OF COURSES BY PARTS AND SEMESTER

PART 1: HARMATTAN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core-Compulsory courses	MTH101	Elementary Mathematics I		4-1-0	5
	PHY101	General Physics I		3-1-0	4
	PHY107	Physics Practical I		0-0-3	1
	CHM101	Introductory Chemistry I		3-1-0	4
	CHM103	Practical Chemistry I		0-0-3	1
	CSC101	Introduction to Computing I		2-0-0	2
	BIO101	Biology for Physical Sciences		2-1-0	3
General Courses	LIB001	*Use of Library		0-0-0	0
	SE??	Special Electives		2-0-0	2
				16-4-6	22

* Use of Library, Study Skills and ICT Resources

PART 1: RAIN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core-Compulsory courses	MTH102	Elementary Mathematics		4-1-0	5

	MTH 104	Vector		2-0-0	2
	PHY102	General Physics II		3-1-0	4
	PHY108	Physics Practical II		0-0-3	1
	CSC102	Introduction to Problem Solving		2-0-0	2
	CYB102	Fundamentals of Cyber Security I		2-1-0	3
/ General Courses	SE??	Special Electives		2-0-0	2
	LIB002	*Use of Library		0-0-0	0
				15-3-3	19

* *LIB002 Introduction to Online Database, Referencing and Tools

PART 2: HARMATTAN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core-Compulsory courses	CSC201	Computer Programming I		2-0-3	3
	CYB201	Fundamentals of Cyber Security II	CYB102	2-0-0	2
	CYB203	Internet Architecture		2-0-0	2
	CYB205	Software Defined Networks		2-0-0	2
	CYB207	Information Security & Policy Development		2-0-0	2
	MTH201	Mathematical Methods I	MTH 102	3-1-0	4
	STT201	Introduction to Statistics		2-1-0	3
General Courses	SE??	Special Electives		2-0-0	2
				17-2-3	20

200 LEVEL: RAIN SEMESTER

Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core-Compulsory courses	CSC202	Computer Programming II	CSC201	0-0-6	2
	CSC204	Introduction to Operating System		2-0-0	2
	CYB202	System & Network Administration	CYB201	2-0-3	3
	CYB204	Digital forensics		2-0-0	2
	CYB206	Security Strategies for Web Applications and Social Networks		2-0-0	2
	MTH205	Introduction to Algebra		2-1-0	3
	MTH 202	Mathematical Methods II	MTH 201	3-1-0	4
	SE??	Special Electives		2-0-0	2
General Courses				15-2-9	20

200 LEVEL: RAIN SEMESTER- LONG VACATION					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core course	CYB200	Student Industrial Work Experience Scheme I		0-0-9	3
				0-0-9	3

300 LEVEL: HARMATTAN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core-	CSC301	Fundamentals of Data Structures		2-0-3	3

Compulsory courses	CSC307	Numerical computation I	MTH 201	2-0-0	2
	CSE301	Object Oriented Modelling and Design		2-0-0	2
	CIS 301	System Analysis and Design		2-0-0	2
	CYB301	Biometric Security		2-0-0	2
	CYB303	Cryptographic Techniques		2-0-0	2
	CYB305	Systems Security	CYB202	2-0-0	2
	CYB307	Information Security Engineering	CYB203	2-0-0	2
General Courses	SE??	Special Electives		2-0-0	2
				18-0-3	19

300 LEVEL: RAIN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
a) CoreCompulsory courses	CYB302	Information security Risk Analysis and Management		2-1-0	3
	CYB304	Edge and Perimeter Security		2-0-0	2
	CYB306	Cloud Computing Security		2-1-0	3
	CSC306	Algorithms and Complexity Analysis		2-0-3	3
	CSC308	Numerical computation II	CSC307	2-0-0	2
	CIT316	Introduction to Artificial Intelligence		2-0-3	3
	CSE302	Object Oriented Programming	CSC202	2-0-3	3
General Courses	SE??	Special Electives		2-0-0	2
				16-2-9	21

300 LEVEL: RAIN SEMESTER- LONG VACATION					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core course	CYB300	Student Industrial Work Experience Scheme II		0-0-9	3
				0-0-9	3
400 LEVEL: HARMATTAN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
a) CoreCompulsory courses	CYB401	Usable Privacy and Security		2-0-0	2
	CYB403	Cryptography Applications		2-0-3	3
	CYB405	System Vulnerability Assessment and Testing		2-0-3	3
	CPE413	Data Communication and Networking		2-0-0	2
	CIT401	Technical Communication in computing		2-0-0	2
	CYB407	Cyber Security in Business & Industry		2-0-0	2
	CYB409	Information Disaster Recovery		2-0-0	2
				14-0-6	16

400 LEVEL: RAIN SEMESTER- LONG VACATION					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core course	CYB400	Student Industrial Work Experience Scheme III	Not more than 12 units outstanding	0-0-27	9
				0-0-27	9

500 LEVEL: HARMATTAN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core course	CYB501	Fault tolerant computing		2-0-0	2
	CYB503	Individual Project I		0-0-9	3
	CYB507	Cryptography: Algorithms and Applications	CYB303	2-0-3	3
	CYB509	System Administration		2-0-0	2
	CSC513	Modeling and Simulation		2-1-0	3
	CYB511	Cyber Security Governance &Cyber Law		2-0-0	2
Free electives (Plus 4 Units)	CYB513	Enterprise Security & Information Assurance		2-0-0	2
	CYB519	VoIP and Multimedia Security		2-0-0	2
	CYB515	Forensic Analysis		2-0-0	2
	CYB517	Threats, Exploits & Counter Measures		2-0-0	2
				14-1-12	19

500 LEVEL: RAIN SEMESTER					
Grouping	Course Code	Course Title	Prerequisite/Corequisite	L-T-P	Units
Core course	CYB502	Identity Management		2-0-0	2
	CYB504	Individual Project II	CYB503	0-0-9	3
	CYB508	Special Topics on Information Security		2-0-0	2

	CYB514	Ethical Hacking & Reverse Engineering		2-0-0	2
	CYB510	Network Defense		2-0-0	2
	CIS508	Computer Systems Project Management		2-0-0	2
	CYB506	Multimedia applications and Security		2-0-0	2
Free electives (Plus 2 Units)	CYB 520	Enterprise and perimeter security		2-0-0	2
	CYB512	Information Security Models			
	CYB 518	Privacy in a Networked World			
	CYB516	Application Security			
				14-0-9	17

OUTLINE OF COURSE DESCRIPTION

CSC101: INTRODUCTION TO COMPUTING I (2 UNIT [2-0-0]) 2 Units

a. Definition of computer and computer related concepts such as programme, computer software: Systems and application programmes; minicomputers, mainframes and supercomputer.
b. Discussion of selected application of personal computers: word processing, database management, spreadsheet, graphics, data analysis.
c. Comprehensive history of modern computer technology. Evolution of microcomputer systems. History of computer programme
d. Number system: Binary, Decimal, Hexadecimal. Binary arithmetic; Addition, subtraction, multiplication, division.
e. Social impact of computers: positive impacts, negative impacts.
f. Definition of the following terms: bits, bytes, word, word length, data, information, records, fields, files, database. Data types and organization. Data coding; ASCII

CSC102: INTRODUCTION TO PROBLEM SOLVING (2 UNIT [2-0-0]) 2 Units

Problem solving process. Algorithms; flowcharting. Role of Algorithm in problem solving process, concepts and properties of Algorithm. Implementation strategies, Development of flowcharts, Pseudocodes, Program objects. Implementation of Algorithms in a programming Language- JAVA/C/C++/Fortran. Introduction to scripting Proramming Language

CYB 102: FUNDAMENTALS OF CYBER SECURITY I (L-2; T-1; P-0) 3 Units

The course provides an overview of the introductory topics in cyber security by espousing underlying concepts of cyber security and information security. The course will explore various attack vectors affecting enterprise today. Students will be taken through components of of cybersecurity network architecture. Topics such as basic concepts such as Confidentiality, Integrity, Availability, Authentication, Access Control, Non-Repudiation and Fault-Tolerant methodologies for implementing security, security policies, best current practices, testing security, and incident response, risk management, disaster recovery, access control, basic cryptography and software application vulnerabilities will be taught. Terminologies are introduced.

CSC 201: COMPUTER PROGRAMMING I (3 UNITS [2-0-3]) 3 UNITS

a) Brief survey of programming paradigms – Procedural programming – Object-oriented programming, Functional programming – Declarative programming, non-algorithmic programming– Scripting languages. The effects of scale on programming methodology.

b) Programming the computer in current version of PYTHON: Declarative statements; Input and Output statements; Program compilation and execution; Control and conditional statements; Loops and iteration; Functions, Routines and Sub-programmes.

c) Input/Output; File processing; Port addressing.

d) Program testing and debugging techniques.

CSC 202: COMPUTER PROGRAMMING II (2 UNITS [0-0-6]) (Pre; CSC 201)

This is a programming laboratory course consisting of applications of programming, through case study problems. Students are expected to carry out four laboratory assignments and make two oral presentations after the completion of the second and the fourth assignments. Programmes will be developed using the latest version of PYTHON.

a) Laboratory Assignment I: Programming basics- Data type, basic programme structure; Compiling and executing programmes in text and graphics environment.

b) Laboratory Assignment II: Loop, arrays, searching and sorting.

c) Laboratory Assignment III: Function, Routine, Subroutine sub-programme: multiple procedure calls from a main programme

d) Laboratory Assignment IV: Extensive programming problem with Application to student's field of study and interest.

CSC 204: Operating System I **2-1-0**
3units

Overview of OS: Role and Purpose, Functionality Mechanisms to support Client/server model, hand-held devices, Design issues influences of Security, networking, multimedia, Windows. OS Principles: Structuring methods, Abstraction, processes of resources, Concept of APIS Device organization interrupts.

CYB 200: Student Work Experience Programme **0-0-9** **3**

Web Technology – design and implementation, Hard sub system – identification, repairing, and servicing, Networking – cable crimpling, cable testing, etc.

CYB 201: FUNDAMENTALS OF CYBERSECURITY II (L-2; T-0; P-0) 2 Units Prerequisite–CYB 102

Building on Fundamentals of Cybersecurity 1**,** the course explores modes of and motivation for attacks. Security in layers. Operating system protection mechanisms, intrusion detection systems, formal models of security, cryptography, Steganography, network and distributed system security, denial of service (and other) attack strategies, worms, viruses, transfer of funds/value across networks, electronic voting, secure applications, cybersecurity policy, and government regulation of information technology

CYB 202: System and network Administration (L-2; T-0; P-3) 3 Units Prerequisite – CYB201

This course focusses on the tasks and issues involved in the administration of distributed computer networks. Topics include user access and privileges, DHCP, DNS, remote access, file and print, update and patch management, security and network management service. Authentication, Authorization and Accounting systems are covered with emphasis on using cross-platform authentication. Network services including DNS, mail and web services, SANs, WAN administration and network management tools. Topics will be covered from a practical, business-oriented, cost/benefit perspective and best practice implementation techniques. Hands-on experience will include representative technology from each of these areas.

CYB203: Internet Architecture (L-2; T-0; P-0) 2 Units

Internet Architecture provides student with technical and organizational structure of the Internet. The student will learn how Internet works, addressing architecture, protocol layering and routing structure. Core services on the Internet such as DNS are examined in details.

CYB 204: Digital Forensics (L-2; T-0; P-3) 3 Units

The course content includes best practices in securing, processing, acquiring, examining and reporting on digital evidence. Students will be exposed to current technologies and methods as well as leading edge techniques with practical based projects and research opportunities. This course describes what a digital investigation is, the sources of digital evidence, and the limitations of forensics. Compare and contrast variety of forensics tools.

a) Introduction: Definition, and Limits and types of tools (open source versus closed source).
b) Legal Issues: Right to privacy, Fourth and Fifth Amendments, Protection of encryption keys under the Fifth Amendment, Types of legal authority, Protection from legal processes, affidavits, testimony and testifying.
c) Digital forensic tools: Types, Artifact-focused versus all-in-one tools, Requirements, and Limitations
d) Investigatory process: Alerts, Identification of evidence, Collection and preservation of evidence, Timelines, reporting, chain of custody, and Authentication of evidence.
e) Acquisition and preservation of evidence: Pull-the-plug versus triage, Write-blocking, Forensically-prepared destination media, Imaging procedures, Acquisition of volatile evidence, Live forensics analysis, and Chain of custody.
f) Analysis of evidence: Pull-the-plug versus triage, Write-blocking, Forensically-prepared destination media, Imaging procedures, Acquisition of volatile evidence, Live forensics analysis, and Chain of custody.

CYB 205: SOFTWARE DEFINED NETWORKS (L-2; T-0; P-0) 2 Units

History, Motivation and concepts of SDN, SDN architecture, SDN Application, Controller, Datapath, Control to Data-Plane Interface (CDPI), SDN Northbound Interfaces (NBI), Deployment models, Application areas of SDN, Security using SDN Paradigm.

CYB 206: Security Strategies for Web Applications and Social Networks (L-2; T-0; P-0) 2 Units

This course provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. The course provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking. In addition, this course covers how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet.

CYB207: Information Security & Policy Development (L-2; T-0; P-0) 2 Units

The course addresses ethical, legal, and policy frameworks within which information assurance and secure development lifecycle professionals must practice. It covers ethical, moral, legal and policy issues related to computers and telecommunications systems, such as how they

impact privacy, fair information practices, equity, content control, and freedom of electronic speech. Students are expected to familiar use themselves with information policies of some countries including Nigeria.

CYB 300: Students Industrial Workshop Experience Scheme I 0-0-9 3

Students proceed on a 3 months industrial attachment at the end of Part III

CYB 301 Biometric Security (L-2; T-0; P-0) 2 Units

Introduction to Biometrics, Brief Introduction of digital image processing and MATLAB in biometric image/signal processing, Introduction to Biometric Algorithm and System with emphasis on any two of the following: Face, Fingerprint, Iris, Speech & speaker. Multimodal biometrics, Privacy issues and other aspects of biometrics, Applications of biometrics & future trends. The course also addresses such challenging issues as security strength, recognition rate and privacy as well as alternatives of passwords and smart cards.

CYB 302 Information Security Risk Analysis and Management (L-2; T-1; P-0) 3 Units

Quantitative risk assessment, Qualitative risk assessment, relating threat to vulnerability, defining impact, risk mitigation, risk transference or avoidance, Communicating Risks and Risk management strategies, Risk management technologies.

Principles of applied information security management, governance and security policy, threat and vulnerability management, incident management, risk assessment and risk management frameworks, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations. ISO 27000 series and the Plan-Do-check-Act model, assessments of threat and vulnerabilities, incident response, forensics and investigations, dealing with classified/ sensitive data, legal and regulatory drivers and issues, certification and common criteria, security awareness, education and training, and practical considerations when implementing the frameworks to address current and future threats.

CYB 303 Cryptographic Techniques (L-2; T-0; P-0) 2 Units

Students in this course explores symmetric and asymmetric cryptography, key management, and encryption algorithms such as DES, AES, RSA, and PGP. Discusses PKI, SSL, and VPN including how to use protocols, hashing, digital signatures, and certificates and certificate authorities. It covers policies, procedures, and methods for the proper use of cryptography in secure systems.

a) Symmetric (private key) ciphers: B block ciphers and stream ciphers (pseudorandom permutations, pseudo-random generators), Feistel networks, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Modes of

operation for block ciphers, Differential attack, linear attack, and Stream ciphers, linear feedback shift registers, RC4.

b) Asymmetric (public-key) ciphers: Theoretical concepts (Computational complexity, one-way trapdoor functions), Naive RSA, Weakness of Naive RSA, padded RSA, Diffie-Hellman protocol, El Gamal cipher, Other public-key ciphers, including GoldwasserMicali, Rabin, Paillier, McEliece, and Elliptic curves ciphers.

CYB 304: Edge and Perimeter Security (L-2; T-0; P-0) 2 Units

Students will examine network-based attacks, whether originating from the Internet or the local LAN, and learn about ways to protect, detect, and defend the perimeter network from such attacks. Students will familiarize with techniques in edge security (Firewalls, IDS, IPS, VPN, proxy servers), as well as securing devices on large-scale distributed networks.

CYB305: Systems Security (L-2; T-0; P-0) 2 Units Prerequisite CYB 202

Security Principles, Account Security, File System Security, Assessing Risk, Risk Analysis, and Encryption. The student's basic network and operating system skills will be expanded to include planning, implementation, and auditing of a system's security package. Secure design and secure coding principles, practices, and methods including least privilege, threat modeling, and static analysis. Covers common vulnerabilities such as buffer overruns, integer overflows, injection attacks, cross-site scripting, and weak error handling.

CYB 306 Cloud Computing Security (L-2; T-1; P-0) 3 Units

Introduction to cloud computing, cloud computing vendors cloud Computing threats, Cloud Reference Model. Introduction to data centers: servers, data storage, networking and virtualization. Data center networking, Introduction to server virtualization software: VMware VSphere. Virtual machine management: configuration, placement and resource allocation. Power efficiency in virtual data centers. Fault tolerance in virtual data centers., The Cloud Cube Model and Security or Cloud Computing. Security in the Cloud, Cloud Threats, Threat Mitigation, Cloud and Security Risks, Real World Issues with Cloud Computing, Cloud Security Alliance, National Institute of Standards and Technology, Information Assurance Framework, Cloud Audit, Cloud Management Audit/Assurance Program, Cloud Business Continuity Planning.

CYB307 Information Security Engineering (L-2; T-0; P-0) 2 Units Prerequisite CYB 203

It establishes the foundations for designing, building, maintaining and assessing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, lab exercises, exam, and required student writing assignment are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the information security engineering program.

CSC 301: FUNDAMENTALS OF DATA STRUCTURE (2 UNITS [2-0-0])

Primitive types, Arrays, Records, strings and String processing, data representation in memory, Stack and Heap allocation, Queues, Trees, implantation strategies for stack, queues, trees, Run time storage management, pointers and references, linked structures

CSC 307: NUMERICAL COMPUTATIONS I (3 UNITS [2-0-3])(Pre: MTH201)

a) Numerical Data representation on computer, Computer as a number crunching tool Floating-point number representation and arithmetic.

b) Error, stability, convergence.

c) Theory of computational solution to problem: numerical algorithm formulation and design, numerical software systems.

d) Introduction to use of Octave or Matlab in numerical computation and engineering applications. Emphasis is on the use of software to solve real problems.

e) Iterative solutions of non-linear systems: (Newton's Method)

f) Numerical solution of linear systems

g) Numerical computation of Eigenvalues and eigenvectors

CSC 308: NUMERICAL COMPUTATIONS II (3 UNITS [2-0-3]) (Pre: CSC 307)

a) Curve fitting; function approximation

b) Numerical differentiation and integration (Simpson's Rule, etc.)

c) Explicit and implicit methods

d) Differential equations (Euler's Method, etc.)

e) Linear algebra

f) Finite differences

CIS 301: Systems Analysis and Design Methodology 2-0-3
3

Vital steps in systems analysis: Techniques of systems analysis. General Systems, Considerations: Data capture; Data management; Data security; Communications systems, Maintenance, User involvement; Project handling and control.

CIT316 Introduction to Artificial Intelligence 2-0-3 3

Introduction to AI. Brief history. Different agent architectures. Search: uninformed and heuristic search, A*, local search and optimization. Constraint satisfaction problems. Game playing and adversarial search. Knowledge representation. Logical reasoning. Propositional logic. Planning algorithms. Reasoning under uncertainty. Bayes rule. Belief networks. Decision making Utility theory. Reinforcement learning. Game theory Applications.

CYB 400: Students Industrial Workshop Experience Scheme II 0-0-27 9

Students proceed on a 6 months industrial attachment for the whole of Rain Semester of Part IV

CYB 401 Usable Privacy and Security (L-2; T-0; P-0) 2 Units

There is growing recognition that technology alone will not provide all of the solutions to security and privacy problems. Human factors play an essential role in these areas, and it is important for security and privacy experts to understand how people will interact with the systems they develop. This course is designed to introduce students to a variety of usability and user-interface problems related to privacy and security and to give them experience in understanding and designing studies aimed at helping to evaluate usability issues in security and privacy systems. Some of the topics include: Text passwords; graphical passwords; Authentication in practice; SSL, PKIs, and secure communication; Usability of privacy policies and the dimensions of privacy notice; Social networks and privacy; Access control and policy configuration; Mental models and folk models of security; the usability of software updates; Reasoning about the human in the loop. Topic includes:

a) Social engineering, and Social media.
b) Usability and user experience: Definition of usability and user experience, and the impact that usability (or lack thereof) has on the security and privacy of a system.
c) Human security factors
d) Policy awareness and understanding
e) Privacy policy
f) Design guidance and implication

CYB 403 Cryptography Applications (L-2; T-0; P-3) 3 Units

a) Advanced concepts: Advanced protocols: o Zero-knowledge proofs, and protocols, Secret sharing, Commitment, Oblivious transfer, Secure multiparty computation, Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography, and KLJN scheme.
b) Discuss the dangers of inventing one's own cryptographic methods.

c) Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.

CYB 405: System Vulnerability Assessment (L-2; T-0; P-3) 3 Units

This course focuses on testing methods and techniques to effectively identify and mitigate risks to the security of a company's infrastructure. Topics include penetration testing methodologies, test planning and scheduling, Information gathering, Password cracking penetration testing and security analysis, social engineering penetration testing and security analysis, internal and external penetration testing and security analysis, router penetration testing and security analysis and reporting and documentation. Operating systems fingerprinting, Remote network mapping, Software and Operational Vulnerabilities, Attack surface analysis, Fuzz testing, Patch management and security auditing.

CYB 407: Cyber Security in Business and Industry (L-2; T-0; P-0) 2 Units

A study of the application and integration of cybersecurity, principles, frameworks, standards and best practices to the management, governance, and policy development processes for businesses. Discussions covers the organization, management, and governance of cybersecurity for enterprise IT in business settings; risk and risk management practices; and development and implementation of industry-wide cybersecurity initiatives and programs.

CYB 409 Information Disaster Recovery (L-2; T-0; P-0) 2 Units

Disaster Recovery Philosophy, Principles and Planning, Contingency Plan Components, Agency Response Procedures and Continuity of Operations, Planning Processes, Continuity and Recovery Function, Steps of Disaster Recovery Planning, Role of IT and Network Management in Disaster Recovery, Developing the Disaster Recovery, Executive Support, DRP Leadership, Cross Department Subcommittee, Department Level Teams, Relationship between IT and Network Staff with Departments, Planning Team Skill Inventory, DRP Team applications and data and Construct a comprehensive lifecycle approach to Web application security.

CPE 413: Computer Networks/Communication 2-0-0 2 This course exposes students to the fundamentals of computer network. It focuses on the tasks and issues involved in the administration of distributed computing networks. Topics include user access and privileges, DHCP, DNS, remote access, file and print, update and patch management, security and network management service Authentication, Authorization, and Accounting systems are covered with emphasis on using cross-platform authentication. Network services including firewalls, DNS, mail, and web services, SANs, WAN administration, and network management tools. Topics will be covered from a practical, business-oriented, cost/benefit perspective and best practice implementation techniques. Hands-on experience will include representative technology from each of these

areas. wares, fourier analysis, measures of communication, channel characteristics, transmission media, noise and distortion, modulation and demodulation, multiplexing, TDM, FDM and FCM parallel and serial transmission (synchronous vs. asynchronous).Bus structure and loop systems, computer network Examples and design consideration, data switching principles broadcast techniques, network structure for packet switching, protocols, description of network e.g ARPANET, etc.

CYB 501: Fault Tolerant Computing (L-2; T-0; P-0) 2 Units

Introduction and overview of fault tolerant schemes; fault and error modelling; test generation and fault simulation; concepts in fault-tolerance; reliability/availability modelling; system level diagnosis; low level fault-tolerance – coding techniques (basic principles, parity bit codes, hamming codes, error detection and retransmission codes, burst error correction codes, Reed-Solomon codes, etc.); high-level fault tolerant techniques in systems: rollback, check pointing, reconfiguration; software fault-tolerance; fault tolerant routing; integrated hardware/software fault-tolerance; redundancy, spares and repairs – apportionment, system versus component redundancy, parallel redundancy, RAID system reliability, N-modular redundancy; software reliability and recovery techniques, network system reliability, reliability optimisation.CYB505

CYB 502: Identity Management (L-2; T-0; P-0) 2 Units

a) Identification and authentication of people and devices: Network Access Control (NAC), Identity Access Management (IAM), roles, multi-method identification and authentication systems, biometric authentication systems (including issues such as accuracy/FAR/FRR, resistance, privacy, etc.), as well as usability and tolerability of the methods
b) Physical and logical assets control: various access controls to physical assets including system hardware, network assets, backup/storage devices, etc. Examples are Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), Roles based Access Control (RBAC), inventory tracking methods, and identity creation methods
c) Identity as a Service (IaaS): This topic cover identity management as a service (e.g., Cloud identity) brings forward issues such as the system being out of the user's control with no way to know what has happened to the information in the system, auditing access, ensuring compliance and flexibility to quickly revoke permissions.
d) Third-party identity services: on-premises, cloud, centralized identity services/password management tools, end-point privilege management,
e) Access control attacks and mitigation measures: password, dictionary, brute force, and spoofing attacks; multifactor authentication; strong password policy; secure password files; restrict access to systems; etc.

CYB 503: Individual Project I **0-0-9** **3**

Final year student project

CYB 504: Individual Project II **0-0-9** **3**

Final year student project

CYB505 Multimedia Applications and Security (L-2; T-0; P-0) 2 Units

This course addresses the design and implementation of secure multimedia applications. Concentration is on writing software programs that make it difficult for intruders to exploit security holes. The course emphasizes writing secure distributed programs in Java. The security ramifications of class, field and method visibility are emphasized

CYB 507 Cryptography: Algorithms and Applications (L-2; T-0; P-3) 3 Units Pre-requisite - CYB 303

Overview and Introduction to Cryptography, Mathematical Background, Symmetric Cryptosystems, Stream Ciphers, Block ciphers, Feistel Ciphers, Multiple Encryption, DES/AES, Hash Functions, Data Integrity, Authentication, MAC, Asymmetric, Cryptosystems, Number Theory, Background, Algorithmic Number Theory, Probabilistic Primality testing, True Primality Testing, Factoring Integers, RSA, Security of RSA Encryption, Security of RSA Key Generation, Discrete Logarithm Cryptographic Schemes, Diffie-Hellman, EIGamal, Key Establishment, Identification Protocols, Digital Signatures, Public Key Management, ECC, Quantum Cryptography, Visual Cryptography, Lattice Cryptography.

CYB 508: Special Topics on Information Security **(L-2; T-0; P-0) 2 Units**

A survey of emerging and leading technologies in the cybersecurity field. The aim is to research and evaluate emerging technologies and determine secure implementation strategies for best-fit business solutions. Topic include evolutionary technology development and adoption in organizations.

CYB 509: System Administration (L-2; T-0; P-0) 2 Units

System administration works behind the scenes to configure, operate, maintain, and troubleshoot the technical system infrastructure that supports much of modern life**. Topic includes:**

a) Operating system administration: account management, disk administrations, system process administration, system task automation, performance monitoring, optimization, administration of tools for security and backup of disks and process.
b) Database system administration: installation and configuration of database servers, creation and manipulation of schemas, tables, indexes, views, constraints, stored procedures, functions, user account creation and administration, and tools for database backup and recovery.
c) Network administration: Network administration relates to installation, and supporting various network system architectures (LANs, WANs, MANs, intranets, extranets, perimeter networks [DMZs], etc.), and other data communication systems. OSI Model, securing of network traffic, and tools for configuration of services.
d) Cloud administration: configuring and deploying applications and users in cloud infrastructures, analyzing performance, resource scaling, availability of cloud platforms, identifying security and privacy issues and mitigating risks.
e) Cyber-physical system administration: the architecture of cyber-physical systems, underlying communication standards (Zigbee), middleware, service-oriented architecture, tools supporting real-time control and application of real-world examples (power grid, nuclear facility, IoT, SCADA).

CYB 510: Network Defense (L-2; T-0; P-0) 2 Units

This course captures current concepts in network protection.

a) Network hardening
b) Implementing firewalls and virtual private networks (VPNs)
c) Network monitoring
d) Network traffic analysis
e) Network access control (internal and external)
f) Perimeter networks (also known as demilitarized zones or DMZs) / Proxy Servers

CYB 511: Cyber Security Governance and Cyber Law (L-2; T-0; P-0) 2 Units Pre CYB-207

This course aims to provide students with a broad understanding of the current legal environment in relation to cyberspace. This includes both domestic and international laws as well as the application of jurisdictional boundaries in cyber-based legal cases. Students should have a strong understanding of current applicable legislation and a strong background in the formation of these legal tools.

This course provides an overview of the legal doctrines and principles that apply to the operation and development of computer technology and the Internet. Topics include: issues related to jurisdiction, constitutional issues of free speech, property rights, e-business, and current developments in legislation and case law.

a) Constitutional foundations of cyber law: Executive power, Legislative power, First amendment, Fourth amendment, and Tenth amendment.
b) Intellectual property related to cybersecurity: copyright acts

c) Privacy laws: Laws governing Internet privacy, Laws governing social media privacy, and Electronic surveillance laws
d) Data security law:
e) Digital evidence:

CYB 512: Information Security Models (L-2; T-0; P-0) 2 Units

Basic concepts, Access control List (ACL), Bell-la Padula Model, Biba model, Brewer and Nash model, Capability-based security, Clark-Wilson model, Context-based access control (CBAC), Graham-Denning model, Harrison-Ruzzo-Ullman (HRU), Lattice-based access control (LBAC), Mandatory access control (MAC), Multi-level security (MLS), Non-interference (security), Object-capability model, Role-based access control (RBAC), Take-grant protection model, Protection ring, High-water mark (computer security).

CYB513 Enterprise Security and Information Assurance (L-2; T-0; P-0) 2 Units

A survey of emerging and leading technologies in the cybersecurity field. The aim is to research and evaluate emerging technologies and determine secure implementation strategies for best-fit business solutions. Topics include evolutionary technology development and adoption in organizations.

CYB514 Ethical Hacking and Reverse Engineering (L-2; T-0; P-0) 2Units

An exploration of techniques and technologies for understanding the operation of malicious software and attacks. It discusses and explores techniques for detection, identification and prevention.

Presents reverse engineering of code and network exploits as a method for understanding and Development of countermeasures

CYB 515 Forensic Analysis (L-2; T-0; P-0) 2Units

Analysis of network and host data. Review of network traffic logs (pcap, flow records) and profiles and their types, identification of attack signatures and fingerprints, study of various trace back methods, application of data mining techniques, and the extraction of information (e.g. from malware, including botnet traffic) acquired through the use of network analysis tools and techniques, recovering evidence left behind and technologies that can be used to assist in the analysis of obtained data or in obtaining more data methodologies for recovering data for persistent storage and memory.

CYB 516 Application Security (L-2; T-0; P-0) 2Units

The course addresses the design and implementation of secure applications. Concentration is on writing software programs that make it difficult for intruders to exploit security holes. The course emphasizes writing secure distributed programs in Java. The security ramifications of class, field, and method visibility are emphasized.

CYB 517 Threats, Exploits and Counter Measures (L-2; T-0; P-0) 2Units

Advanced network and host security concepts and mechanisms. Assessing vulnerabilities, writing real working exploits for existing systems in a closed and controlled environment, developing countermeasures to these perceived and real threats. The class will involve a fair amount of programming. Those who take the class are expected to be able to program in C/C++, have some a solid knowledge of assembly language, and be familiar with network basics and programming as well as modern operating systems (Windows, MacOS, Unix)

CYB 518 Privacy in a Networked World (L-2; T-0; P-0) 2Units

Increasing use of computers and networks in business, government, recreation, and almost all aspects of daily life has led to a proliferation of online sensitive data that if used improperly, can harm the data subjects. As a result, concern about the ownership control, privacy, and accuracy of these data has become a top priority. This course focuses on both the technical challenges of handling sensitive data and the policy and legal issues facing data subjects' data.

CYB 519 VoIP and Multimedia Security (L-2; T-0; P-0) 2Units

Introduction to multimedia traffic security, general knowledge and techniques for streaming data traffic, such as VoIP and multimedia. The security challenges unique to such traffic will be covered in detail, including disruption of service, theft of service, and violation of confidentiality, relevant data encryption and authentication techniques will also be covered in detail.

CYB520 Enterprise Security and Information Assurance (L-2; T-0; P-0) 2 Units

A survey of emerging and leading technologies in the cybersecurity field. The aim is to research and evaluate emerging technologies and determine secure implementation strategies for best-fit business solutions. Topics include evolutionary technology development and adoption in organizations.

CSC 513: MODELLING AND SIMULATION (2UNITS [2-0-0])

a) Simulation Programming environments, Requirements analysis and design modeling tools

Testing tools.

b) Configuration management tools Tool integration mechanisms

c) Basic concepts in computer simulation, methodology, experimental design, simulation languages.

CIS 508: COMPUTER SYSTEM PROJECT MANAGEMENT (2 UNITS [2-0-0])

a) Definition of computer project and project management.
b) Components and features of a good computer-based project management technique. Computer network administration.
c) Function of members and team management, team processes, team organization and decision-making, roles and responsibilities in a software team, role identification and assignment, team problem resolution.
d) Project tracking
e) Software Project scheduling, Budgeting and Planning; Project organization.
f) Software measurement and estimation techniques, Risk analysis.
g) Software quality assurance
h) Software configuration management
i) Project management tools