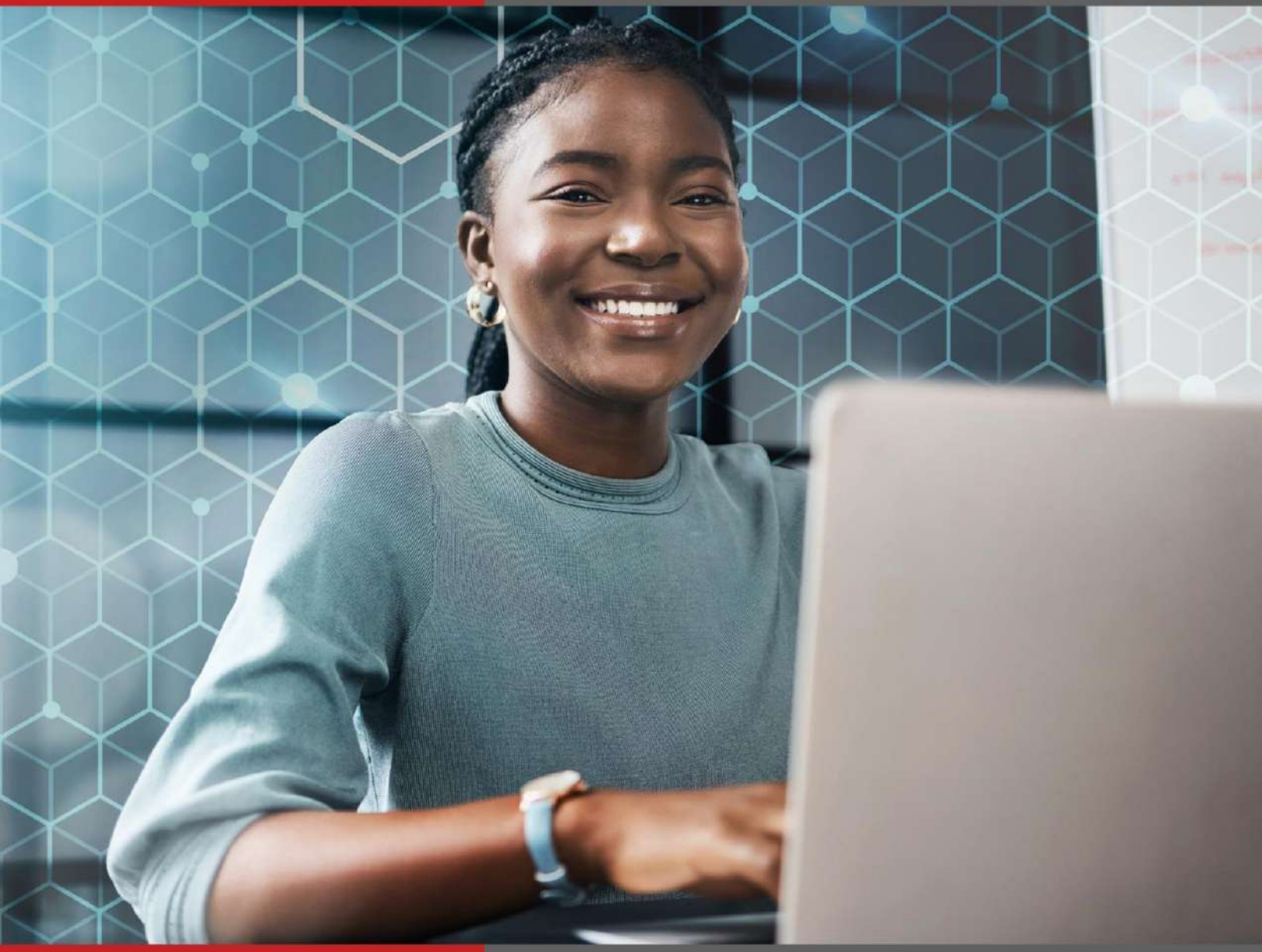
ACADEMIC CITY UNIVERSITY

Program Handbook



MSc CYBER SECURITY

Graduate Programs Team
Academic City University
September 2024

Contents

1.0. Welcome Message

Akwaaba!

Welcome to the Faculty of Computational Science and Informatics at Academic City University!

We are thrilled to welcome you to our MSc in Cybersecurity program—an advanced, industry-driven curriculum designed to equip you with the expertise to tackle modern cybersecurity challenges. In an era of digital transformation, this program empowers you to safeguard critical systems, mitigate cyber threats, and innovate secure solutions for a rapidly evolving technological landscape.

This handbook serves as your comprehensive guide, providing essential insights into your academic journey. The curriculum is meticulously crafted to build proficiency in threat intelligence, risk management, cryptography, ethical hacking, and system security—core competencies that are indispensable across industries such as finance, healthcare, government, and technology.

Beyond technical mastery, this program fosters strategic thinking, adaptability, and leadership, preparing you to become a cybersecurity professional capable of shaping the future of digital security. You will gain hands-on experience with cutting-edge tools, real-world case studies, and innovative problem-solving methodologies to stay ahead in the ever-evolving cybersecurity landscape.

We are excited to support you in this transformative journey and look forward to seeing you lead, innovate, and secure the future.

Welcome to the next frontier in cybersecurity education!

Dr Navel Sharma
Ag. Dean, Faculty of Computational Science and Informatics

2.0. Program Objectives

The MSc in Cyber Security program is designed to provide students with advanced expertise in the most widely used techniques in cyber security, forensics, and technologies that play a key role in apprehending cybercriminals and solving complex security challenges.

The curriculum aims to equip students with the skills necessary for critical decision-making in cyber security situations, fostering the ability to tackle real-world cyber incidents independently. By combining scientific principles with an understanding of behavioural issues, students will gain the practical knowledge needed to address and mitigate cyber threats effectively.

Furthermore, the program focuses on enhancing students' understanding of the broader applications and implications of cyber security on both national and global scales.

3.0. Intended Learning Outcomes

Upon completion of the program, you will be able to:

- Analyse, formulate, and solve complex cyber security and cyber physical infrastructure breaches across broad areas in government, private sector, individual engagements, business, scientific and engineering infrastructures etc.
- Use the knowledge of cyber security and forensics to solve real-world problems.
- Use cutting edge tools and technologies to analyse cyber incidences and breaches.
- Apply knowledge of behavioural, scientific, artistic, legal and law enforcement learning techniques to build intelligent systems and processes to address cyber security issues and incidences.
- Demonstrate use of teamwork, leadership skills, decision making and organisation theory.

4.0. Our Uniqueness

The Master of Science program in Cyber Security offers a unique blend of multidisciplinary perspective that is positioned to attract students and professionals from different graduate streams cutting across Computing, Engineering, IT, Law, Sociology, Social and Enterprise Informatics, Law Enforcement, Policing, Statistics, Mathematics and Business. The uniqueness of our program is that it provides depth and breadth in terms of a

strong interdisciplinary and multidisciplinary approach to tackling the cybercrime malaise from socio-technical, human behavioural, law, corporate, business and scientific perspectives.

The Unique blended format offers flexible Thursdays and some Friday virtual sessions, complemented by immersive on-campus learning on Saturdays. This enables a comprehensive learning experience tailored for working professionals and full-time students. Internship opportunities and organizational-based tasks further enrich the program.

5.0. Graduation Requirements

1. Satisfy all general University requirements (including Eligibility for the Degree).
2. Pass all the required courses on the Course Diet.
3. Complete the prescribed number of credit hours in each category of course specified for the program of study.
4. Attain a minimum Cumulative Grade Point Average (G.P.A) of 2.0.
5. Settle all financial and other obligations to the Academic City University.
6. Should maintain acceptable moral conduct at the University.
7. Should have adhered to all University policies and requirements outlined in the Graduate Student Handbook.

6.0. Structure

Lecture days	Lecture Schedule	Contact Hours
Thursday	5:30 pm - 8:30 pm	3
Friday	5:30 pm - 8:30 pm	3
Saturday	9:00 am - 5:00 pm	6
Total hours per week		12
Total hours per module		48

7.0. Assessment of Learning

Method	Weightage	Detail
Continuous Assessments: Assignments/ Class Tests / Project Work/ Mid Semester Exam	35%	Class / Lab / Home Assignments Closed Book / Open Book / Practical Test & Viva Voce Practice Examinations in a pattern similar to End Semester Exam
Attendance & Participation	5%	
End Semester Exam	60%	End Semester Assessment, Practical work/ Projects.

8.0. Program Diet

MSc. Cyber Security								
TOTAL PROGRAMME CREDITS					36			
Year / Level	S/N	Course Code	Course Status	Course Name	L	T	P	C
Year 1 / Level 500	SEMESTER 1							
	1	CYB5101	Compulsory	Information Security Assurance & Management	2	2	3	3
	2	CYB5102	Compulsory	Network & Enterprise Systems Security Management	2	2	3	3
	3	CYB5103	Compulsory	Criminological Theories	2	2	3	3

	4	CYB5104	Compulsory	Cyberspace Ethics & Law	2	2	3	3
				Total	8	8	12	12
	SEMESTER 2							
	1	CYB5201	Compulsory	Cryptography & Digital Forensics	2	2	3	3
	2	CYB5202	Compulsory	Block Chain and Cryptocurrencies	2	1	3	3
	3	CYB5203	Compulsory	Cyber Psychology & Behaviour	2	1	3	3
				Total	6	5	9	9
Year 2 / Level 600	SEMESTER 1							
	1	CYB6101	Compulsory	Graduate Qualifying Seminar	2	3	6	3
	2	CYB6102	Elective I	Cyber Warfare & Terrorism	2	2	3	3
	3	CYB6103	Elective I	Cyber Security Breaches Case Studies	2	2	3	3
	4	CYB6104	Compulsory	MSc. Thesis Phase 1	2	3	6	3
				Total	6	7	12	12
	SEMESTER 2							
	1	CYB6201	Compulsory	MSc. Thesis Phase II	2	3	6	3
Grand Total					22	23	39	36

9.0. Modular Structure

Below is how modules will be structured for the Cyber Security program

Year	Semester	Module	Courses on Code & Title	
1	1	1	CYB5101	Information Security Assurance & Management
1	1	2	CYB5102	Network & Enterprise Systems Security Management
1	1	3	CYB5103	Criminological Theories
1	1	4	CYB5104	Cyberspace Ethics & Law
1	2	1	CYB5201	Cryptography & Digital Forensics
1	2	2	CYB5202	Block Chain and Cryptocurrencies
1	2	3	CYB5203	Cyber Psychology & Behaviour

Year	Semester	Module	Courses on Code & Title	
2	1	1	CYB6101	Graduate Qualifying Seminar
2	1	2	CYB6102	Cyber Warfare & Terrorism
2	1	3	CYB6103	Cyber Security Breaches Case Studies
2	1	4	CYB6104	MSc. Thesis Phase I
2	2	1	CYB6101	MSc. Thesis Phase II

10.0. Course Briefs

10.1. Year One Semester One Courses:

10.1.1. CYB5101 Information Security Assurance & Management

Required of CYB students

Prerequisite(s): Knowledge of Information Security, Management, Audit

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.1.1.1. Course Objectives

The course will enable students to:

- Demonstrate an understanding of information security governance
- Demonstrate an understanding of information risk management
- Demonstrate an understanding of information security program
- Demonstrate an understanding of information security program management
- Demonstrate an understanding of incident management and response
- Evaluate the legal, ethical, and professional issues in information security
- Develop these skills: Critical thinking, Communication, Information Literacy and Computer Technology Usage.

10.1.1.2. Course Content

Topics to be covered include: threats and vulnerabilities, threat and vulnerability assessment, risks, confidentiality, integrity, and availability; IP and Web Security, security policies; authentication; authorization, access control; risk management; common attack/defence methods; ethical issues, information assurance, components of the assurance ecosystems, enterprise physical security, cryptography, application development security, enterprise incidence response, enterprise business continuity, disaster recovery planning, cyber resiliency, enterprise risk management and governance.

10.1.1.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini-projects, and discussions.

10.1.1.4. Reading Material

The following are recommended reference books:

1. Markus, Christen, Bert Gordijin and Michele Loi, (2020), The Ethics of Cybersecurity, 1st ed. edition. Springer.
2. Mike Chapple, 2020), Access Control and Identity Management (Information Systems Security & Assurance), 3rd edition Jones & Bartlett Learning.
3. Gupta, J. N. D., & Sharma, S. K. (2021). Handbook of Research on Information Security and Assurance. Hershey, PA: Information Science Reference.
4. Kizza, J. M. (2021). Guide to Computer Network Security. London: Springer
5. Lopez, J., Huang, X., & Sandhu, R. (2020). Network and system security: 7th International Conference, NSS, Madrid, Spain, Proceedings. Berlin: Springer

10.1.2. CYB5102 Network & Enterprise Systems Security Management

Required of CYB students

Prerequisite(s): Knowledge of Computer Networks, Social & Enterprise Informatics, Information Security, additionally there is an expectation that students have a general knowledge of IT principles.

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.1.2.1. Course Objectives

By the end of this course, students should be able to:

- Perform the evaluation of business processes associated with managing risks, business continuity, audit, and security challenges in software development.
- Carry out a detailed analysis of enterprise security by performing various types of analysis such as vulnerability analysis, penetration testing, audit trail analysis, system and network monitoring, and configuration management.
- Carry out detailed risk analysis and assessment of enterprise systems using various practical and theoretical tools.
- Design detailed enterprise-wide security plans and policies, and deploy appropriate safeguards (models, mechanisms and tools) at all the levels by providing due consideration to the life-cycle of the enterprise information systems and networks, as well as its legal and social environment.
- Appreciate the need for interoperable network management and understand general concepts and architecture behind standards-based network management
- The student will develop these skills: analytical skills, business skills and communication skills.

10.1.2.2. Course Content

Topics to be covered include: Application of security principles to computer networking, The OSI and TCP/IP models of network communication, Network security at different layers of the OSI and TCP/IP models, Enterprise systems for AAA, Securing Virtual Machine and cloud-based IT infrastructures, Designing networks on selected protocols to support business operations while maintaining identified levels of network security, Supporting secondary network connectivity (wireless, VPNs, BYOD devices, partner networks, cross-domain and other connectivity types) Designing networks to support Resiliency Management, Business Continuity, Disaster Recovery and other principles to avoid network failures that negatively impact the organization's ability to deliver on its core mission, Methods to prevent, detect and respond to security breaches, including the role of Incident Response Teams

10.1.2.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini-projects, and discussions.

10.1.2.4. Reading Material

The following are recommended reference books:

1. William R. Cheswick, and Steven M. Bellovin (2021): Firewalls and Internet Security, Repelling the Wily Hacker, Addison-Wesley
2. Aditya Mukherjee, (2020), Network Security Strategies: Protect your network and enterprise against advanced cybersecurity attacks and threats, 1st edition, Packt Publishing;
3. Joel Scambray, Stuart McClure, and George Kurtz (2021): Hacking Expose Network Security Secrets & Solutions, 2nd Edition, McGraw-Hill Publishers
4. Ross Anderson (2020): Security Engineering; A Guide to Building Dependable Distributed Systems, Wiley Publishers
5. Raymond Panko and Julia Panko, (2018) Business Data Networks and Security, 11th edition, Pearson.

10.1.3. CYB5103 Criminological Theories (Compulsory)

Required of CYB students

Prerequisite(s): Knowledge of Criminology, Computer Security, Cyber Crime, Sociological Theories

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.1.3.1. Course Objectives

This course will equip students with the knowledge and skills to:

- Understand and appreciate the role of social inequality and cultural diversity in the study of criminology.
- Approach the study of crime and criminals from a social scientific perspective.
- Understand crime typologies and examine the nature and causes of crime
- Understand concepts and theories of the crime
- Comprehend how crime statistics are collected and disseminated.
- Examine the procedures devised by formal social agencies, such as police, courts, and correctional agencies to handle individuals who commit delinquent and criminal acts.
- The student will develop these skills: numeracy skills, leadership skills and interpersonal skills

10.1.3.2. Course Content

Topics to be covered include: Victims And Victimization, Theories Of Crime Causation, Rational Choice Theory, Routine Activity Theory, Displacement Theory, Pseudo Ownership, Trait Theories, Social Structure Theories, Social Process Theories, Developmental Theories, Crime Typologies, Computer and Cyber Crimes, Interpersonal Violence, Cyber Terrorism, Cyber Espionage, Cyber Stalking, Identity Theft, Paedophiling , Web of Deceit, Political Crime and Terrorism, Property Crime, Peel Theory of Cyber Policing, Enterprise Crime, Crimes of the New Millennium

10.1.3.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini-projects, and discussions.

10.1.3.4. Reading Material

The following are recommended reference books:

1. Longe, O.B. (2022): Web of Deceit. Creative Research Publishers

2. Bohm, Robert M. & Vogel, Brenda L. (2021) A Primer on Crime & Delinquency Theory, 3rd Ed. Belmont, CA: Wadsworth
3. Cullen, Francis T. (2020) Criminological Theory: Past to Present, 4th Ed. New York: Oxford
4. Ronald L. Akers , Christine S. Sellers and Wesley G. Jennings, Criminological Theories: Introduction, Evaluation, and Application 8th Edition, Oxford University Press; 8th edition , 2020, ISBN-13 : 978-0190935252.
5. Stephen G. Tibbetts and Alex R. Piquero , (2022), Criminological Theory: The Essentials, Fourth edition, SAGE Inc,

10.1.4. CYB5104 Cyberspace Ethics & Law (Compulsory)

Required of CYB students

Prerequisite(s): Knowledge of Legal Aspects of IT, Cyber Security, Cyber Etiquette, Cyber Victimization, Law, Ethics, Patents, Copyright, Trade Secrets

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.1.4.1. Course Objectives

By the end of this course students should be able to:

- Given a cyber operations scenario, explain the authorities applicable to the scenario.
- Provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology, and data.
- Evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking, describe criminal penalties related to unethical hacking, and apply the notion of Grey Areas to describing situations where law has not yet caught up to technological innovation.
- Describe steps for carrying out ethical penetration testing, describe 'ethical hacking' principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.
- Discuss the structure of the legal system and how it enforces laws governing the Internet;
- Evaluate the ethical responsibilities of Internet users, service providers, and content providers;
- Investigate a security breach and the legally required responses to a breach; and apply current case law and statutes governing the Internet to fact-based situations
- The student will develop these skills: critical thinking, analytical skills, and communication skills.

10.1.4.2. Course Content

Topics to be covered include: Netiquette, Digital Culture and Intellectual Property Rights, Computer Crime/Cyber Crimes , Digital Economies and Contemporary Issues, Online Freedom and Usage of technologies , History of the rapid rise in computer and networking technology, cyber abuses, system abuses, Cyber criminality, Protecting software and other intellectual property, Computer crime and legal issues, Issues on the impact and control of computer technology, Data Protection and ePrivacy, IS and global diversity, cyber defamation and online free speech, surveillance, Data Protection, AdTech, Profiling, State Surveillance and Communications Interception, Technology determinism, Interpretive flexibility, Socio-technical rationality and Multiple situated rationalities.

10.1.4.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini projects and discussions.

10.1.4.4. Reading Material

The following are recommended reference books:

1. Carl Gibson (2021): Gift of Fire - A Social, Legal, and Ethical Issues for Computing Technology 5th Edition Publisher: Pearson; 5th edition
2. John Kindt. (2021): Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis (Law, Governance and Technology Series Book 12) 2021 Edition, Kindle Edition Els Publisher: Springer; 2021th edition
3. Penny Duquenoy, Simon Jones & Barry G. Blundell (2020): Ethical, Legal and George W. Reynolds. (2020): Professional Issues in Computing (FastTrack). Cengage Learning; 1st edition
4. Richard A. Spinello, (2020) Cyber ethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace, 7th edition Jones & Bartlett Learning;,
5. Huansheng Ning, (2022) A Brief History of Cyberspace, 1st edition Auerbach Publications.

10.2. Year One Semester Two Courses

10.2.1. CYB5201 Cryptography & Digital Forensics (Compulsory)

Required of CYB students

Prerequisite(s): Knowledge of Legal Aspects of IT, Cyber Security, Cyber Etiquette, Cyber Victimization, Law, Ethics, Patents, Copyright, Trade Secrets

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.2.1.1. Course Objectives

This course will help students to:

- Develop the fundamental principles and theories underlying cryptographic algorithms, including the mathematical foundations of cryptography;
- Learn to apply cryptography to solving data security problems;
- Introduce the concepts how cryptographic algorithms and protocols work and how to use them;
- Provide a broad view of security with practical applications of cryptography to data security.
- Understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
- Understand the history of forensic science, development and its role in criminal investigation.
- Discuss the rules, laws, policies, and procedures that affect digital forensics;
- Perform the steps included in a digital investigation from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, and the completion of legal proceedings;
- Write professional quality reports that include both a summary report and a notes section, which describes the technical procedures used in the investigation;
- Identify important file metadata and apply their use in a forensic investigation; and
- Perform a forensic investigation on a forensic image, using various tools to recover evidence, resulting in a report documenting the investigation
- Undertake problem identification, formulation, and solution.
- Manage information and documentation
- Communicate effectively, with the engineering team and with the community at large

10.2.1.2. Course Content

Topics to be covered include Cryptography and cryptographic schemes, Encryption Methods and Vulnerabilities, Digital Signatures and public and private key cryptography, Protecting Data from Being Compromised Internet, Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems, Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analysing malicious software. Military Computer Forensic Technology, Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware,

10.2.1.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini projects, and discussions.

10.2.1.4. Reading Material

The following are recommended reference books:

1. Shiva V. N. Parasram , (2020), Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux, 2nd Edition, Packt Publishing.
2. Marcelo Sampaio de Alencar, (2022), Cryptography and Network Security 1st Edition, River Publishers.
3. Nour Moustafa, (2022) Digital Forensics in the Era of Artificial Intelligence, 1st edition, CRC Press;
4. Marcelo Sampaio de Alencar, Cryptography and Network Security 1st Edition, Kindle Edition, River Publishers; 1st edition (November 30, 2022, ASIN: B0BHC7996M
5. Nour Moustafa, Digital Forensics in the Era of Artificial Intelligence, CRC Press; 1st edition, 2022, ISBN-13: 978-1032244686.

10.2.2. CYB5202 Block Chain and Cryptocurrencies

Required of CYB students

Prerequisite(s): Knowledge of Finance, Entrepreneurship, Business Management, Accounting, Cryptography, online trading, FinTech

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.2.2.1. Course Objectives

By the end of the course, students should be able to:

- Understand the technology components of block chain-based digital currencies, cryptographic functions and hashes, the process of currency issuance and mining, proof-of-work, consensus and distributed ledger technology.
- Understand digital currencies and be able to conduct transactions from a digital currency wallet.
- Understand more advanced uses of the block chain such as escrow services, asset registration, attestation and smart contracts, and how it can be deployed to a number of industries.
- Understand alternatives to bitcoin, such as alt-coins, Ethereum and Bitcoin Cash.
- Understand what parallels and differences cryptocurrencies have with the existing monetary and banking systems.
- Understand likely frameworks for regulating cryptocurrencies, challenges with current regulatory landscape.
- The course encourages critical thinking and innovation: students will evaluate business problems that could be solved with block chain technology and the impact that it might bring economically and socially
- Demonstrate the ability to construct and deliver clear, concise, and convincing written and oral business communications by preparing executive summaries, written case evaluations, and by presenting their cases.

10.2.2.2. Course Content

Topics to be covered include: Money banking & payment systems, Challenges of digitization, bitcoins and cryptocurrencies, hash functions & symmetric cryptography, Nakamoto Consensus, it's use of economic incentives, mining & transaction fees, cryptographic identity and algorithmic inflation, Ethereum, Smart contracts and tokens, user's perspective; Vulnerabilities, blockchain, different aspects of owning cryptocurrency and interacting with a blockchain, including buying and selling, wallets, supportive infrastructure such as

exchanges and custodians, and the dangers of a digital bearer asset. We will also discuss the risks and, trade-offs of decentralized networks, including possible attack vectors Layer 2 solutions being deployed for Bitcoin and Ethereum, Stable coins, difference between token and ledger money, similarities and differences with existing payment solutions, and the possible disruption of the payments industry, Central Bank Digital Currencies, distinction between central bank money and private money. Digital Yuan and the proposed Digital Euro, Decentralized finance; Tokenization of capital markets, non-fungible tokens, social tokens and online communities, Regulatory & legal issues

10.2.2.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini projects, and discussions.

10.2.2.4. Reading Material

The following are recommended reference books:

1. Ben Stephens (2021): Cryptocurrency Investing for Beginners: Clear and Simple Introduction to Cryptocurrency, Trading, and Mining. Paperback Independent Publishers.
2. Antony Lewis (2021): The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT) Mango Publishers.
3. Nick Furneaux , (2018) Investigating Cryptocurrencies: Understanding, Extracting, and Analysing Blockchain Evidence, 1st edition, Wiley.
4. Sebastian Peyrott, (2022,) Introduction to Ethereum Block Chain Technology: Mastering the Ethereum and Cryptocurrency Technology.
5. Antony Lewis, (2021), The Basics of Bitcoins and Blockchains, Mango.

10.2.3. CYB5203 Cyber Psychology & Behaviour

Required of CYB students

Prerequisite(s): Knowledge of Psychology, Behavioural Sciences, Cyber Security, Cyber Criminals, Cybercrime victims

Corequisite(s): None

Course Credit=3; Lecture Hours=2; Tutorial Hours=0; Practical Hours=3

10.2.3.1. Course Objectives

This course will:

- Orient students to the relatively new branch of Cyber Psychology.
- Help future students of clinical psychology to study and identify Cyber Psychology Behaviours.
- Address mental health issues that arise from cyber bullying, cybercrime and online addiction.
- Create awareness of appropriate online communication and computer mediated psychotherapies.
- The student will develop these skills: interpersonal awareness, emotional intelligence, leadership, self-management, and decision-making

10.2.3.2. Course Content

Topics to be covered include: Meaning of Cyber Psychology and Cyberspace; History; Technology across Lifespan; cyberspace as a psychological space - Basic psychological features of cyberspace-Networks as "Mind" and "Self"- Presence. Social Psychology of cyberspace: Self and community in the age of the Internet. Role of psychologist in cyberspace; Methods of studying – Observational, Correlational, Experimental, Online Methods; Research Ethics in Cyberpsychology; Importance and Application of Cyber Psychology, Social Psychology of Online Groups-Developmental Stages of Mailing Lists; Making Virtual Communities, Work Communicating with Typed Text Chat; Decision-Making Method for Email Groups; Extending Work Group into Cyberspace; Managing Deviant Behaviour in Online Groups. Deviant Behaviour and Cybercrime, Importance of Mental Health in cyberspace; internet-based disorders – Gaming, Cyber Bullying, Cybersickness, Cyberchondriasis, Phantom Effect, Online Depression, Internet Addictions, Nomophobia, Google Effect; Social Media And Cyber psychology Behaviours-Comparison and Low Self-Esteem, Depression, Social Isolation and Ostracism, Negative Relationships, Fear of Missing Out (FOMO), Sleep Deprivation, Addictive Behaviour

10.2.3.3. Mode of Delivery

The course will be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini projects, and discussions.

10.2.3.4. Reading Material

The following are recommended reference books:

1. Spark, R. (2021): Towards Cyberpsychology: Mind, Cognitions and Society in the Internet Age Amsterdam, IOS Press.
2. Irene Connolly, Marion Palmer, Hannah Barton, Gráinne Kirwan (2021), An Introduction to Cyber psychology, Routledge. London
3. Alison Attrill. (2022), Cyberpsychology, 1. 15, Oxford University Press, Oxford, UK, p.278, [ISBN: 978-019871258].
4. Zheng Yan, The Cambridge, (2023) Handbook of Cyber Behaviour 2 Volume Hardback Set (Cambridge Handbooks in Psychology, Cambridge University Press.
5. Majeed Khader, Whistine Xiau and Ting Chai , (2021) Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators , World Scientific.

Journals:

1. Journal of Psychosocial Research in Cyberspace
2. Cyberpsychology, Behaviour and Social Networking
3. Computers in Human Behaviour

10.3. Year Two Semester One Courses:

10.3.1. CYB6101 Graduate Qualifying Seminar

Required of CYB students

Prerequisite(s): completion of at least 24 credits of the CYB degree or consent of the instructor.

Corequisite(s): None

Course Credit=3; Lecture Hours=0; Tutorial Hours=1; Practical Hours=6

10.3.1.1. Course Objectives

By the end of the course, students should be able to;

- Learn about research in order to
    (a) critically read published research,
    (b) start thinking about a thesis topic,
- Work with faculty members of your choice
- To sharpen time management skill in a research environment

10.3.1.2. Course Content

Students are to liaise with relevant industrial government or corporate organisations to identify a cyber security need(s) and formulate/develop solutions to address the challenge(s).

10.3.1.3. Mode of Delivery

The course will be delivered through industrial visits, group presentations, discussions, and report writing.

10.3.1.4. Reading Material

The following are recommended reference books:

1. Rob, T. J. (2022) Before you write your first word...: what you should know about self-publishing that no one tells you! T.J. Rob Books Publications;
2. Bean, R. (2021). Fail fast, learn faster: lessons in data-driven leadership in an age of disruption, big data, and AI. Hoboken: John Wiley and Sons Inc.;
3. Kleppmann, M. (2021). Designing data-intensive applications: the big ideas behind reliable, scalable, and maintainable systems. 17th edition. Sebastopol: O'Reilly Media Inc.

4. Atherton, T. (2020). Technical report writing and style guide: how to write even better technical reports. Independent Publisher (W. A. Atherton).
5. Greenhall, M. (2010). Report writing skills training course: how to write a report and executive summary, plan, design, and present your report, in an easy format. Universe of Learning Publishers.

10.3.2. CYB6102 Cyber Warfare & Terrorism (Elective)

Required of CYB students

Prerequisite(s): Knowledge of Psychology, Behavioural Sciences, Cyber Security, Cyber Criminals, Cybercrime victims

Corequisite(s): None

Course Credit=3; Lecture Hours=3; Tutorial Hours=2; Practical Hours=0

10.3.2.1. Course Objectives

The course will:

- Provide students with the appropriate theoretical foundations on the main cyber warfare concept.
- Expose students to practical techniques that aim in exploiting, attacking, and defending computer networks.
- Provide a comprehensive view of cyber warfare from the technical, legal, and regulatory perspectives.
- Present the deployment of cyber warfare activities at national levels.
- Expose students to the social, ethical, legal, and political aspects of cyber warfare
- The student will develop these skills: analytical skills, communication skills and technical skills.

10.3.2.2. Course Content

Topics to be covered include: Cyber-attacks and defences, Cyber espionage, Cyber sabotage, Cyber politics and vandalism, Nation state malware, for example, Stuxnet, Cyber-attack motivations including hacktivism, private sector, and military, Cyber terrorism and cyber warfare Cyber monitoring, surveillance and intelligence, SCADA systems and public infrastructure, The future of warfare, trends in cyber warfare and terrorism, the increasing impact of such events on the security landscape;, different types of cyber security threats, including cyber terrorism, cyber-crime, and cyber warfare; examples of actual cyber terrorist attacks, motivations, method of operation, and impacts; private, corporate, and national cyber-attack events and their motivations; main types of cyber-attacks and the various tactics and strategies used during attacks; security policy, procedural and technical controls to mitigate the threats of different types of cyber-attacks and the risks they present.

10.3.2.3. Mode of Delivery

The course would be delivered through lectures, tutorials, laboratory sessions, term papers, presentations, mini projects and discussions.

10.3.2.4. Reading Material

The following are recommended reference books:

1. Singer, P. W. and Allan Friedman, (2021). Cybersecurity and Cyberwar (Oxford University Press).
2. Clarke, Richard and Robert K. Knake, (2020). Cyber War (New York: Harper Collins).
3. Clarke and Knake (2022) The Internet as Battlespace. Jan 25. [No class Jan. 18 for MLK Day, or Jan. 20] 1., pp. 1-32, and 69-101. 2.
4. Axelrod, Robert and Rumen Iliev (2021) “The Timing of Cyber Conflict,” Proceedings of the National Academy of Sciences, 2014. 3. “
5. Regner Sabillon, (2020), Cyber Security Auditing, Assurance, and Awareness through CSAM and CATRAM (Advances in Digital Crime, Forensics, and Cyber Terrorism), 1st edition IGI Global

10.3.3. CYB6103 Cyber Security Breaches Case Studies (Elective)

Required of DS students

Prerequisite(s): None

Corequisite(s): None

Course Credit=3; Lecture Hours=3; Tutorial Hours=2; Practical Hours=0

10.3.3.1. Course Objectives

This course will help students to:

- Understand the key concepts, issues and technologies associated with cyber-attacks
- Analyse cyber security incidents
- Describe and discuss some of the technological, social, legal, ethical and personal issues that relate to cyber security incidents.
- The student will develop these skills: analytical skills and communication skills

10.3.3.2. Course Content

Topics to be covered include: A broad range of cyber incidences, breaches, attacks and countermeasures will be discussed. Journal articles and conference proceedings will be explored to evaluate new technologies, mitigating factors, cyber victimization and cybercriminal behaviours. Legal aspects, ethics, trending topics and developments will also be examined

10.3.3.3. Mode of Delivery

The course would be delivered through presentations, conference participation(s), articles prepared for Journals, group presentations and discussions.

10.3.3.4. Reading Material

The following are recommended reference books:

1. Raghvendra, Kumar, Dac-Nhuong Le, Brojo Kishore Mishra , Jyotir Moy Chatterjee and Manju Khari , (2019) Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 1st edition , Wiley-Scrivener.
2. Ryan Gallagher, Melanie Gersten , Khalil Jackson , Deborah Liu , James Massot , Edward Amoroso , Kevin Senator ,and Toby Weir-Jones , (2020) A Case Study on Improving ICS Cyber Security Legislation , Lexeprint Inc.

3. Graeme Payne, (2019), The New Era of Cybersecurity Breaches: A Case Study and Lessons Learned, Cybersecurity Executive Advisors LLC
4. Sherri Davidoff, (2019), Data Breaches: Crisis and Opportunity 1st Edition, Addison-Wesley Professional;
5. Neil Daswani and Moudy Elbayadi, (2021)) Big Breaches: Cybersecurity Lessons for Everyone, 1st Edition, Apress

10.4. Year Two Semester Two Courses

10.4.1. CYB6104/6201 MSc Thesis Phase 1/Phase 2 (Compulsory)

Required of CYB students

Prerequisite(s): Knowledge of Report Writing, Project Documentation and Technical Compositions.

Corequisite(s): None

Course Credit=6; Lecture Hours=0; Tutorial Hours=3; Practical Hours=9

10.4.1.1. Course Objectives

This course will equip students with skills to:

- Understand the links between the components of a technical problem
- Demonstrate the capacity to analyse and define a complex and open problem, put it into its broader context and make a plan for its solution
- Use a background in a specialized discipline and current international research, to develop new ideas and solve new problems
- Work, communicate and report research results in written form in English.
- Use ethical and sustainability principles to evaluate technical solutions and be able understand their business and societal contexts
- Find, analyse and critically evaluate information and use it to identify opportunities for novel work

10.4.1.2. Course Content

Students are to choose from a variety of core and tangential domains in Cyber Security and develop a project-driven thesis to be written and submitted as a capstone project at the end of the program. The students are expected to choose research project that they have spent considerable time in considering and researching (literature review), project design (formulation of a hypothesis), data collection (field and or laboratory), analysis (statistical examination of the data), and finally presentation and synthesis (examination of the statistical results in the context of your hypothesis and literature review). Each of these individual parts will consume considerable time and effort. They are therefore appointed supervisors/advisors whose responsibilities are to guide students through the research process. Supervisors are appointed upon being offered admission into the program.

10.4.1.3. Mode of Delivery

The course will be delivered through seminars, presentations, and a final defence of the thesis.

10.4.1.4. Reading Material

The following are recommended reference books:

1. Siochrú, C. Ó. (2022). A Student Guide to Writing Research Reports, Papers, Theses and Dissertations. Taylor & Francis.;
2. Robbo, J. (2022). APA manual: the simplified guide to APA style formatting, citations and referencing for writers, researchers and students. 7th edition. Independent publishers (Joe Robbo);
3. Chris Ifeanyi Ezeh (2021). Learn best practices of referencing & citing in different styles: - present excellent research work - master referencing rules with ease - shine in MLA, APA, and Chicago styles. EuroAfrica Media Network;
4. Kornuta, H. M. and Germaine, R. W. (2019) A concise guide to writing a thesis or dissertation: educational research and beyond. 2nd edition. Abingdon: Routledge;
5. Turabian, K. L., Booth, W. C, Colomb, G. G., Williams, J. M., Bizup, J., FitzGerald, W. T. (2018) A manual for writers of research papers, theses, and dissertations. 9th edition. Chicago: The University of Chicago Press;

ACADEMIC CITY
UNIVERSITY

#AskACity

Academic City University
Haatso- Agbogba, Accra (Ghana)
www.acity.edu.gh
+233 26 269 3870
info@acity.edu.gh
@acitygh