City University of Hong Kong
Course Syllabus

offered by Department of Electrical Engineering
with effect from Semester A in 2021/2022

Part I Course Overview

Course Title:	Cybersecurity Technology
Course Code:	EE4215
Course Duration:	One Semester (13 weeks)
Credit Units:	3
Level:	B4
Proposed Area: *(for GE courses only)*	☐ Arts and Humanities ☐ Study of Societies, Social and Business Organisations ☐ Science and Technology
Medium of Instruction:	English
Medium of Assessment:	English
Prerequisites: *(Course Code and Title)*	MA2001 Multi-variable Calculus and Linear Algebra, and EE3315 Internet Technology
Precursors: *(Course Code and Title)*	EE2302 Foundations of Information and Data Engineering
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

This course aims to provide students with an understanding of the principles of cybersecurity and computer security technologies, including the principles of ethical hacking, cryptography, and blockchain technologies.

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs[#]	Weighting* (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Describe the basic concepts and current technologies of cybersecurity.		✓		
2.	Apply cryptographic techniques to defend against attacks.		✓	✓	
3.	Describe the defensive techniques and architectures in defending against cyber attacks.		✓	✓	
4.	Apply penetration testing techniques to assess network security.		✓	✓	
** If weighting is assigned to CILOs, they should add up to 100%.*		100%			

[#] Please specify the alignment of CILOs to the Gateway Education Programme Intended Learning outcomes (PILOs) in Section A of Annex.

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to self-life problems.

A3: *Accomplishments*
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

TLA	Brief Description	CILO No.						Hours/week (if applicable)
		1	2	3	4			
Lecture	Key concepts are described and illustrated	✓	✓	✓	✓			3 hrs/wk (Some of the lecture hours will also be conducted as in-class exercises, tutorials and labs)
Tutorial	Key concepts are worked out based on problems	✓	✓	✓	✓			
Lab	Key concepts are applied to investigate or solve network security problems	✓	✓	✓	✓			

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

Assessment Tasks/Activities	CILO No.						Weighting*	Remarks
	1	2	3	4				
Continuous Assessment: 65%								
Tests/Quizzes (at least 2)	✓	✓	✓	✓			40%	
#Assignments (at least 3)	✓	✓	✓	✓			25%	
Examination: 35% (duration: 2hrs , if applicable)								
Examination	✓	✓	✓	✓			35%	
** The weightings should add up to 100%.*							100%	

Remark:

To pass the course, students are required to achieve at least 30% in course work and 30% in the examination. Also, 75% laboratory attendance rate must be obtained.

may include homework, tutorial exercise, project/mini-project, presentation

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
1. Examination	Achievements in CILOs	High	Significant	Moderate	Basic	Not even reaching marginal levels
2. Coursework	Achievements in CILOs	High	Significant	Moderate	Basic	Not even reaching marginal levels

6. Constructive Alignment with Major Outcomes

MILO	How the course contribute to the specific MILO(s)
1	An ability to apply knowledge of engineering is appropriate to the degree discipline. Students will learn security techniques for enhancing the safety of computer, network and portable devices and apply these techniques to the solution of engineering problems.
2	An ability to design and conduct experiments as well as to analyze and interpret data is appropriate to the degree discipline. Students will learn the programming techniques related to Cybersecurity, and apply these techniques to conduct experiments to analyze and interpret data received from the smart card.
3	An ability to design a system, component, or process that conforms to a given specification within realistic constraints is appropriate to the degree discipline. Students will learn design of security system and learn the technique to analysis the risk of the designed system. They are required to work with the constraints specified in the environment including components, interconnectivity and network link.
4	An ability to function effectively and responsibly as a team member is appropriate to the degree discipline. Students will work in groups and split the work in amongst them and coordinate the design into a workable system.
5	An ability to identify, evaluate, formulate and solve engineering problems is appropriate to the degree discipline. Students will design appropriate software related to Cybersecurity technologies.
7	An ability to communicate effectively is appropriate to the degree discipline. Students work in groups and they will practice the skill to communicate with each other..
10	An ability to use necessary engineering tools is appropriate to the degree discipline.

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

Introduction to Cybersecurity

Computer security concepts, the CIA triad, model for network security, threats, vulnerabilities and attacks.

Cryptographic Techniques

Introduction to finite fields; Symmetrical cipher: block cipher, DES, AES, confidentiality modes; Asymmetrical cipher: public key infrastructure, RSA, Diffie-Hellman key exchange; elliptic curve cryptography, hash functions, message integrity and digital signature.

Cybersecurity - Defensive Approach

Red Team vs Blue Team, Endpoint Security; Router & Switch Security; Network Security Devices: Firewalls, IDS, VPNs.

Cybersecurity - Offensive Approach

Security Assessment and Penetration Testing; Hacking Techniques; Web Hacking; Information Gathering; Vulnerability Assessment; Target Exploitation; Privilege Escalation; Maintaining Access.

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

1.	N/A

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

1.	Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters, No Starch Press; 1 edition (December 21, 2014) (ISBN-13: 978-1593275907 ISBN-10: 1593275900)
2.	Andreas Bolfing, Cryptographic Primitives in Blockchain Technology: a Mathematical Introduction, Oxford University Press, 2020.
3.	S.J. Nielson, C.K. Monson: Practical Cryptography in Python: Learning Correct Cryptography by Example, Apress; 1st ed. edition (September 27, 2019)
4.	Ugo Ekpo: Introduction to Cyber Security: Fundamentals, Independently published (October 12, 2018)
5.	Seymour Bosworth, Michel E. Kabay and Eric Whyne , Computer Security Handbook, Sixth Edition [electronic resource] (John Wiley & Sons, 2014, ISBN:9781118127063)
6.	William Stallings, Cryptography and network security: principles and practice, (Pearson, 2014, ISBN 9780133354690)
7.	Richard E. Blahut , Cryptography and secure communication [electronic resource] (Cambridge University Press, 2014, ISBN 9781107014275)