CE4024 and CZ 4024 – Cryptography and Network Security

Academic Year	AY1819		**Semester**	2				
Course Code	CE/CZ4024							
Course Title	Cryptography and Network Security							
Pre-requisites	CE3005 Computer Networks OR CZ3006 Net Centric Computing							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Lab	-

Course Aims

This course aims to develop your ability to understand how basic cryptographic algorithms work and identify the problems associated with the application of cryptography in real-world security systems, and explain the pros and cons of various cryptographic mechanisms.

This course provides an introduction to basic cryptographic algorithms, along with the underlying mathematical foundations guiding the design of aid algorithms, and explores the usage of these primitives in real world applications, particularly applied to network security.

Intended Learning Outcomes (ILO)

This course provides an understanding of cryptography and network security at an introductory level. Upon the successful completion of this course, you shall be able to:

1. Apply the theoretical (mathematical) tools that form the basis of cryptographic algorithms;
2. Explain and analyze the design of cryptographic algorithms;
3. Identify the typical problems associated with the application of cryptography in real-world systems;
4. Explain the security issues in a Cyberspace environment;
5. Explain the design decisions behind a secure network architecture plan;
6. Design basic secure network strategy based on a combination of cryptographic and network security control mechanisms

CE4055 and CZ4055 – Cyber Physical System Security

Academic Year	AY1819	**Semester**	2				
Course Code	CE/CZ4055						
Course Title	Cyber Physical System Security						
Pre-requisites	CE/CZ1006 Computer Organisation And Architecture						
Pre-requisite for	NIL						
No of AUs	3						
Contact Hours	Lectures	26	TEL	-	Tutorials	12	Laboratories: 3

Course Aims

Cyber physical systems are typically designed as a network of interacting elements with physical input and output, and are characterized by the interaction between the physical world (sensors, user inputs, actuators) and the cyber world (processing, decision making). Cyber physical systems are the driving force behind modern civilization, being integral part of technologies, such as additive manufacturing, smartcard-based payment, power delivery systems, drone-based operations, and smart home automation. Cyber physical systems are characterized by stringent performance requirements, such as, extremely low energy budget, small area footprint and often hard real-time constraints. Due to the pervasive nature of the cyber physical systems in our everyday lives, it also runs the risk of huge security hazards.

In this course, we will learn about the basics of cyber physical systems, including the design principles and methodologies. Further, there will be a detailed treatment of the security challenges for cyber physical systems, which vary in practice due to the diverse nature of the application environment of cyber physical systems. These different forms of security breaches, observed across diverse cyber physical systems, will be put in a well-characterized taxonomy, to be systematically identified as attack surfaces. The techniques to handle these attacks will be described in a generic manner, including key management and wireless/RFID communication. The attack surfaces and protection/mitigation principles will then be elaborated with practical case studies, from the representative cyber physical systems such as automotive, smart card systems and smart grid.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the basic concepts of cryptography are used for ensuring security of cyber-physical systems
2. Describe the basic design, architecture and design principles of cyber physical systems
3. Identify the sources of vulnerability in a cyber physical system systematically via attack surfaces
4. Determine how security is incorporated at different abstractions and at different components of cyber physical systems

5. Articulate the principles behind the detection and mitigation of attacks for different attack surfaces of a cyber-physical system
6. Compare and contrast practical cyber physical system security such as for smart grid, smart vehicle, and smart card systems
7. Determine the performance overheads to consider for incorporating security in a cyber-physical system

CE4062 and CZ 4062 – Computer Security (System Security)

Academic Year	AY1819		**Semester**		1			
Course Code	CE/CZ4062							
Course Title	Computer Security (System Security)							
Pre-requisites	CE/CZ2005 Operating Systems							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Student presentations	0

Course Aims

This course aims to equip you with foundational knowledge on issues and techniques required for the cyber security.

You will have the knowledge of different security policies and security models, and have the ability to recognise security features and discover pitfalls in computing systems, including the operating system and softwares.

Intended Learning Outcomes (ILO)

Upon successful completion of this course, you should be able to:

1. Explain the principles of access control and security models in computer systems.
2. Interpret different security mechanisms in modern operating systems.
3. Distinguish different vulnerabilities associated with computer systems.
4. Reproduce and detect vulnerable scenarios in existing software.

CE4064 and CZ 4064 – Security Management

Academic Year	AY1819		**Semester**	1				
Course Code	CE/CZ4064							
Course Title	Security Management							
Pre-requisites	CZ/CE2006 Software Engineering							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	23	TEL	0	Tutorials	4	Student presentations	12

Course Aims

This course aims to develop your ability to identify the problems associated with (cyber and information) security management and understand using case studies that to effectively address them, one needs to design solutions that encompass multiple dimensions, including technology, people, processes and (internal as well as external) regulations.

This course provides an introductory but broad perspective of cyber and information security, and is relevant for anyone pursuing a career in the IT/ICT industry – including those in product design and development, security engineering, penetration testing, network/system administration, as well as, given the proliferation of IT in all walks of our lives, in executive roles across industries and government.

Intended Learning Outcomes (ILO)

This course introduces security management at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the need for effective security management;
2. Identify the typical problems associated with security management;
3. Describe and debate the ways in which various organizations solve these problems;
4. Analyse real world and (possibly) new security incidents or problems, and propose and evaluate possible mitigations.

CE4065 and CZ 4065 – Digital Forensics

Academic Year	AY1819		**Semester**	2				
Course Code	CE/CZ4065							
Course Title	Digital Forensics							
Pre-requisites	CE3005 Computer Networks OR CZ3006 Net Centric Computing; CE/CZ4062 Computer Security (System Security)							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	8

Course Aims

Digital forensics has become increasingly relied upon to obtain evidence suitable for admission to a court of law. Such a process involves the gathering, recovery, and analysis of electronic traces to procure electronic evidence; this done in a manner that maintains a well-documented chain of custody such that the integrity of the electronic evidence can be validated by external parties.

This course provides an introductory but broad perspective of digital forensics and is relevant for anyone pursuing a career in the IT/ICT industry – including those in product design and development, security engineering, penetration testing, network/system administration, as well as, given the proliferation of IT in all walks of our lives, in executive roles across industries and government.

Intended Learning Outcomes (ILO)

This course introduces digital forensics at an elementary level. Upon the successful completion of this course, you shall be able to:

1. Explain the knowledge about what is stored in digital systems and how to retrieve and use such data/information to procure evidence;
2. Describe the different anti-forensic techniques, and how anti-forensics can be detrimental to a forensic analyst's effort in recovering evidence;
3. Describe network forensics, including techniques used to capture data and information on networks, and how to use such data to reconstruct a system/user activity scenario;
4. Explain how data is retained in storage systems;
5. Present the investigative findings in an objective manner.

CE4067 and CZ 4067 – Software Security

Academic Year	AY1819		**Semester**		2			
Course Code	CE/CZ4067							
Course Title	Software Security							
Pre-requisites	CZ/CE2002 Object Oriented Design & Programming OR CZ/CE2005 Operating Systems							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	0	Tutorials	13	Laboratories	-

Course Aims

This course aims to develop skills in software security. It focuses on security attacks launched by supplying specially crafted inputs to software components that modify the intended behaviours of those components, and the secure coding techniques (defences). The modified behaviours of the software components become security critical in a connected world where application systems are constructed from a collection of software components. Software developers who are not familiar with software security are likely to omit suitable defences out of ignorance.

As such, this course will equip you with the deep knowledge about software security attack and defence techniques, a skill necessary to become IT security experts or professional software developers.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the causes for common software vulnerabilities.
2. Include basic defences in their code.
3. make use of software security tools
4. Describe the importance and the recommended phases of a software development process geared towards writing secure code

CE4068 and CZ 4068 – Application Security

Academic Year	AY1819		**Semester**		1			
Course Code	CE/CZ4068							
Course Title	Application Security							
Pre-requisites	CE/CZ2005 Operating Systems; CE3005 Computer Networks OR CZ3006 Net-Centric Computing							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Laboratories	-

Course Aims

The internet has become a convenient platform for commercial transactions executed by application systems. Commercial transactions are obvious targets for criminal activities. Securing such transactions involves multiple parties, hardware components, and protocols which are important to the security of the underlying application systems. Practitioners in this field need to be familiar with current security technologies and appreciate the respective management tasks and responsibilities of the parties involved. This course would support you in fulfilling these expectations.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the various security technologies used for protecting commercial transactions conducted by application systems
2. Describe the fundamentals of risk analysis and security management
3. Determine how and where commercial transactions may be compromised in the web architecture
4. Identify current attack patterns
5. Determine the protection mechanisms appropriate for a given threat