CO3099   Foundations of Cybersecurity

		Student Workload (hours)	
Academic Year:	2020/1		
Module Level:	Year 3	Lectures	22
Scheme:	UG	Seminars	
Department:	Informatics	Practical Classes & Workshops	
Credits:	15	Tutorials	11
		Fieldwork	
		Project Supervision	
		Guided Independent Study	106
		Demonstration	
		Supervised time in studio/workshop	11
		Work Based Learning	
		Placement	
		Year Abroad	
		Total Module Hours	150

Period:	Semester 2
Occurence:	E
Coordinator:	Stanley Fung
Mark Scheme:	UG Module Mark Scheme

No.	Assessment Description	Weight %	Qual Mark	Exam Hours	Ass't Group	Alt Reass't
001	Examination (Final)	60		3		
002	Coursework	40				

Intended Learning Outcomes

On completion of the module, successful students will be able to:
- Describe the working principles of modern cryptosystems including public key cryptography;
- Design and implement secure network applications using standard cryptographic libraries;
- Describe the fundamental principles of security and be able to identify the needed design principle;
- Explain the importance of security requirements in system design;
- Explain the concepts of authentication and authorization, and discuss and compare commonly used methods for each of them;
- Identify common attack vectors, and implementation issues that can result in potential security problems;
- Be able to identify and prevent common client- and server-side attacks in web applications;
- Describe the concepts of privacy and anonymity, and be able to apply mechanisms for achieving database privacy;
- Demonstrate familiarity with secure communication protocols (such as, for example, TLS) and some attacks on them.

Teaching and Learning Methods

Class sessions together with lecture slides, recommended textbooks, worksheets, printed solutions, and web support.

Assessment Methods

Marked coursework, traditional written examination.

Pre-Requisites

-

Co-Requisites

-

Excluded Combinations

-

Guided Independent Study: Indicative Activities

Guided reading and other information sources.