COAP: Cryptography

Module Title:	Cryptography
Language of Instruction:	English

Credits:	10

NFQ Level:	7

Module Delivered In	2 programme(s)

Teaching & Learning Strategies:	The teaching and learning strategies used in the module are a combination of traditional lectures and laboratory exercises. The laboratory exercises include group work and peer review. The module covers a number of threshold concepts that are explicitly highlighted for the students.

Module Aim:	The module provides a broad understanding of the various forms of cryptography, the fundamental security goals achieved through cryptographic primitives, algorithms and protocols, and their possible weaknesses. The module puts particular emphasis on practical skills and cryptographic implementations in real-life applications.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Understand and describe the most prevalent cryptographic primitives, algorithms and protocols.
LO2	Select the appropriate cryptographic tools for various real-world scenarios.
LO3	Apply modern cryptographic techniques to enhance the overall security of a system.
LO4	Analyse and critically appraise the security of a cryptographic system.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*
No recommendations listed
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.*
No requirements listed

Module Content & Assessment

Indicative Content
Hash Functions and Applications Integrity verification, password verification, salting, keyed hashing, MACs, PRFs, Merkle trees, authenticated encryption
Symmetric Cryptography Classical ciphers, substitution ciphers, transposition ciphers, block ciphers, the Feistel scheme, SPN networks, AES, modes of operation, stream ciphers, RC4, ChaCha
Asymmetric Cryptography Public-key encryption, RSA, elliptic-curve cryptography, cryptographic hardness assumptions, digital signatures, blind signatures
Key Exchange Protocols Diffie-Hellman, public-key infrastructure, web of trust
Applications and Real-World Deployments SSL and TLS, trusted computing, digital rights management, blockchains and cryptocurrencies

Assessment Breakdown	%
Continuous Assessment	20.00%
Project	30.00%
End of Module Formal Examination	50.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Short Answer Questions	The students will answer a series of short questions that test their knowledge of cryptographic primitives, algorithms, protocols and real-world use cases.	1,2	20.00	Week 7

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	The students will complete an individual project that is shared across modules. The project will have a cryptographic component. For example, users will need to be authenticated and data will need to be stored securely.	2,3	30.00	Week 11

No Practical

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	n/a	1,2,3,4	50.00	End-of-Semester

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	3.00
Laboratory	12 Weeks per Stage	3.00
Independent Learning	15 Weeks per Stage	11.87
	Total Hours	250.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	5	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	5	Mandatory