Title	Cryptography and Protocols
Long Title	Cryptography and Protocols
Credits	5
NFQ Level	Expert
Module Author	Dr.Hazel Murray

Module Description:

Cryptography is integral to our online world and information systems. It is essential that when building these systems we understand the significance of the cryptographic applications we use. In this module the student will learn the fundamentals of cryptography and its application in security protocols. These protocols allow systems to achieve information security, privacy and trust. Students will learn the mathematics and cryptographic tools to analyse and understand the strengths and shortcomings of such security protocols and will develop an understanding of how to improve insecure systems. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Apply mathematical concepts (number theory, geometry and group theory) to understand the working and capabilities of symmetric cryptography, public key cryptography, digital signatures and hash functions.
LO2 Critically evaluate and enable real-world implementations of symmetric cryptography, public key cryptography, digital signatures and hash functions.
LO3 Develop security protocols which leverage cryptographic techniques to achieve confidentiality, authentication and key exchange.
LO4 Analyse future cryptographic needs and applications of cryptography to achieve system security.
LO5 Evaluate technical and research papers which will aid continuous learning and students' ability to stay up to date with best practice in the field.

Indicative Content

Introduction to cryptography
What are the key security objectives? What are the attacks? What protections do we expect? Introduce the CIA triad and the three fundamental building blocks in cryptography: symmetric cryptography, public-key cryptography and hash functions. Cover the notation used in cryptography.
Symmetric cryptography
Types of symmetric cryptography; stream ciphers, block ciphers. Begin with the core fundamentals of the technology and then implement and evaluate real implementations. E.g. 3DES, AES modes, Blowfish, etc.
Public-key cryptography
Begin with the number theory, primes and factorization knowledge students need to understand Diffie-Hellman and RSA. Real-world implementations of both will then be studied. Fundamental group theory and geometry concepts will be covered for student to understand elliptic curve cryptography. Implementations of elliptic curve cryptography will be created and discussed.
Security protocols
Protocol notation. Analysis of protocols for confidentiality, protocols for authentication (X.509, NSPK), protocols for key establishment (NSSK, Otway-Rees, Kerberos, NSPK, X.509). Focused on research and analysis based examples and exercises designed to develop student's ability to self-research and critically examine new technologies and developments.
Digital signatures and PKI
Hash functions such as MD5, SHA, RIPEMD. Signature schemes with appendix, with recovery and with hash and redundancy functions. RSA, RSA with SHA and ECDSA will be covered. PKI and digital certificates. Set up and maintenance of Let's encrypt certificates.
Hash functions and password security
Hashing and salting, password attacks, password security policies, password representations.
Secure email
Signed and encrypted messages, PGP. Implementation and evaluation.
Advanced technologies
Cloud key management and encryption approaches, hardware security modules, quantum-resistant cryptography.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Short Answer Questions	Students are set a series of mathematical, research and programming questions designed to test their knowledge of cryptography fundamentals and their implementations.	1,2	30.0	Week 7
Short Answer Questions	Students are set a series of mathematical, research, programming and implementation based questions designed to test their knowledge of security protocols and their implementations.	3,4,5	30.0	Week 11
Project	Students will submit a project that studies an information system. Students will discuss the cryptography and protocols that should be imbedded in that system to make it secure. Students should reference the strengths and weaknesses of the chosen implementation.	1,2,3,4,5	40.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **Niels Ferguson, Bruce Schneier, Tadayoshi Kohno 2011, *Cryptography engineering: design principles and practical applications*, Wiley**