Title	Practical Cryptography
Long Title	Practical Cryptography
Credits	5
NFQ Level	Expert

Module Description:

Cryptography is an essential part of building secure and robust information systems and applications. In this module students will gain a hands-on understanding of practical cryptographic applications and their correct implementations in information systems. This will include an understanding of symmetric and asymmetric cryptography and hash functions. 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 Critically evaluate a range of real-world cryptographic algorithms with respect to their security and efficiency.

LO2 Appraise the application of cryptographic algorithms as solutions in real-world systems.

LO3 Design and deploy cryptography as an imbedded feature in information communication and access procedures.

LO4 Assess the pitfalls and limitations in security software and develop an ability to use available documentation and best practice guidelines to overcome these barriers.

LO5 Communicate cryptographic analysis and design outcomes to a wider audience of peers through presentation to a professional standard.

Indicative Content

Introduction to cryptography

What are the key security objectives? What are the attacks? What protections do we expect? CIA triad. Introduce the key sources for documentation (NIST, OWASP,RFCs).

Symmetric cryptography

Types of symmetric cryptography; stream ciphers, block ciphers. Algorithms in use: 3DES, AES modes, Blowfish, etc. Applications of symmetric cryptography: Secure payment, file encryption, message encryption, authentication (Kerberos).

Asymmetric cryptography

How it works: Basic Number theory concepts. Algorithms in use: Diffie Hellman, RSA & Elliptic Curve Cryptography. Applications: Key exchange, digital signatures, certificates.

Hashing

How it works: hash functions. Algorithms in use: MD5, RIPEMD, Whirlpool, SHA. Applications: Message Digest and Password Verification.

Protocols

Applications of symmetric and Asymmetric cryptography including key management. Correct implementation of TLS, OAuth (OICD), WPA 2.0.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Presentation	Learners propose a plan to secure an application using cryptographic techniques. The criteria used to select an appropriate algorithm and parameters are documented and presented to a professional standard using various methods which may include a short written proposal and an oral presentation.	1,2,5	20.0	Week 6
Project	Learners will develop a full implementation of a secure and robust application with embedded security. The relevant cryptography must be applied in a secure manner using best-practice implementations and up-to-date algorithms. Learners will communicate the limitation, restrictions and deployment features in a detailed technical report. Learners will also communicate the security features and performance of the cryptographic techniques used to a diverse audience of technical and non-technical professionals using various methods which may include an academic poster, a blog post, a short presentation or a paper	1,2,3,4,5	80.0	Sem End

No End of Module Formal Exam

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework Only

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		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

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		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

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