Title:	Practical Cryptography APPROVED
Long Title:	Practical Cryptography

Module Code:	CYBR9003	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Expert
Field of Study:	Cyber Skills
Valid From:	Semester 1 - 2021/22 (September 2021)
Module Delivered in	1 programme(s)
Module Coordinator:	Donna OShea
Module Author:	Hazel Murray
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 CyberSkills 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.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
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. You may not enrol on this module if you have not acquired the learning specified in this section.*
No requirements listed

Module Content & Assessment

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.

Assessment Breakdown	%
Course Work	100.00%

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 Examination

Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner 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 Learner 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

Module Resources

Recommended Book Resources

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

Supplementary Book Resources

- **Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone 1996, *Handbook of Applied Cryptography*, CRC Press, Inc. https://cacr.uwaterloo.ca/hac/ [ISBN: 0-8493-8523-7]**
- **Jean-Philippe Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption* [ISBN: 9781593278267]**

Recommended Article/Paper Resources

- **OWASP *Transport Layer Protection Cheat Sheet***
  https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
- **OWASP *Authentication Cheat Sheet***
  https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Supplementary Article/Paper Resources

- **Nadia Heninger, Zakir Durumeric, Eric Wustrow and J. Alex Halderman 2012, *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices*, USENIX Security Symposium**
  https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf

Other Resources

- **Github repository: Svetlin Nakov 2018, *Practical Cryptography for Developers*, MIT**
  https://cryptobook.nakov.com/
- **PDF: 2014 *Study on cryptographic protocols*, ENISA**
  https://www.enisa.europa.eu/publications /study-on-cryptographic-protocols/at_download/fullReport
- **Website: Gary C. Kessler *An Overview of Cryptography***
  https://www.garykessler.net/library/crypto.html
- **Website: Damien Giry *BlueKrypt Cryptographic Key Length Recommendation***
  https://www.keylength.com/
- **Website: Cryptosense *Java Cryptography White Paper***
  https://cryptosense.com/whitepapers/java-crypto-security-whitepaper
- **Website: OWASP *Cryptographic Storage Cheat Sheet***
  https://cheatsheetseries.owasp.org/cheat sheets/Cryptographic_Storage_Cheat_Sheet .html

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KSSDE_9	Certificate in Secure Software Development	2	Mandatory