H9CRYPT: Cryptography

Module Code:	H9CRYPT
Long Title	Cryptography CONDITIONAL APPROVAL
Title	Cryptography
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	MICHAEL BRADFORD
Module Author:	Margarete Silva
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	

Learning Outcomes

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

#	Learning Outcome Description
LO1	Interpret the background and history of cryptography and ascertain future trends in cryptography.
LO2	Critically assess the principles of modern cryptography and appraise the scientific approach to modern cryptography.
LO3	Compare, contrast, and account for the cryptographic theories, principles and techniques that are used to establish security properties.
LO4	Analyse, choose and assess existing methods for cryptography and reflect upon the limits and applicability of such methods.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	

H9CRYPT: Cryptography

Module Content & Assessment

Indicative Content
Introduction • Examine some classical encryption schemes and their inadequacies • Review modern and scientific approach to cryptography with an emphasis on formal definitions and mathematical proofs • Principles of modern Cryptography • Explore the notion of perfect secrecy, and present a scheme that probably achieves this notion of security • Future trends
Mathematical Preliminaries • Topics in linear algebra, number theory, probability theory, and statistics.
Modern Cryptography and Computational Security • Limitations of the One-Time Pad • Computational Secrecy (considering computational secrecy instead of perfect secrecy) • Pseudorandomness and Pseudorandom Generators (also known as a stream cipher in practice) • The Pseudo One-Time Pad • Proofs of Security • Quantum cryptography • How cryptographic solutions are determined
Private Key Cryptography • Stronger Security Notions • Pseudorandom Functions and Block Ciphers • CPA-Secure Encryption from PRFs/Block Ciphers • Modes of Encryption • Security Against Chosen-Ciphertext Attacks
Message Integrity • Message authentication codes • Hash Functions and collision resistant hashing • Authenticated Encryption • Secure Communication Sessions
Public Key Cryptography • The Public-Key Revolution • Diffie-Hellman Key Exchange • Public-Key Encryption • RSA-Based Public-Key Encryption
Cryptographic Analysis • Techniques • Tools • Algorithms
Digital Signatures • Digital Signatures • RSA-Based Signatures • Identification Schemes • Public-Key Infrastructure (PKI)

Assessment Breakdown	%
Coursework	40.00%
End of Module Assessment	60.00%

Assessments

Full Time

Coursework

Assessment Type:	Continuous Assessment	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	4
Non-Marked:	No		

Assessment Description:
Students will be presented with a number of in-class problem scenarios (e.g., 5 x 8%) and will be required to apply cryptographic principles and techniques to a practical security situation.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	60
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
Learners are required to complete a formal end-of-semester examination.

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

H9CRYPT: Cryptography

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	1	Every Week	1.00
Tutorial	No Description	1	Every Week	1.00
Independent Learning	No Description	8.5	Every Week	8.50
			Total Weekly Contact Hours	2.00

Module Resources

Recommended Book Resources

J. Katz, L. Yehuda. (2015), Introduction to Modern Cryptography, 2nd Edition. Chapman & Hall.

Supplementary Book Resources

W. Stallings. (2016), Cryptography and Network Security: Principles and Practice, 7th Edition. Pearson, [ISBN: 0978013444428].

C. Paar, J. Pelzl, B. Preneel. Understanding Cryptography: A Textbook for Students and Practitioners,, 2010. Springer.

This module does not have any article/paper resources

Other Resources

[website], Network World,
http://www.networkworld.com

[website], Schneier on Security,
http://www.schneier.com

[website], Cisco Security,
http://tools.cisco.com/security/center/h ome.x

[website], Privacy Rights Clearinghouse,
http://www.privacyrights.org/ar/chrondat abreaches.htm

[website], OWASP,
https://www.owasp.org/index.php/Main_Pag e

[website], EU Cyber security,
http://ec.europa.eu/digital-agenda/en/cy bersecurity

[website], European Union Agency for Network and Information Security (ENISA),
https://www.enisa.europa.eu/

[website], Secunia,
http://secunia.com/

[website], Commtouch,
http://www.cyren.com/security-center-new .html#dashboard

[website], CERT,
http://www.cert.org/

[website], The Hacker's Community Online,
http://www.hacker.org/

Discussion Note:	