Manchester Metropolitan University

Unit Specification (Collaborative/Postgraduate/Flexible Framework Use Only)

Unit Details & Outline

Unit Title	Cryptography & Encryption		
Unit Code	6G7Z1011		
Occurrence(s)	MMU Science & Engineering		
Unit Abbreviation	Crypt & Encrypt		
Level of Study	Level 7		
Credit Value	30	**ECTS Value**	15
Home Department	Division of Computer Science and Information Systems School of Computing, Mathematics and Digital Technology		
Home Faculty	Science and Engineering		
Unit Co-ordinator	**Keith Yates**		
Key Words	Cryptography, Encryption		

Unit Description

Brief Summary	The unit covers theoretical discussion of the key encryption algorithms: Diffie-Hellman, RSA, Digital Signatures, modern symmetric cryptosystems DES and AES. Additionally we will code the algorithms and their variants in a modern programming language and implement cryptosystems over a computer network.
Indicative Content	Indicative topics of equal weighting:

	Classical Cryptography; Shannon's Theory; Block Ciphers; Hash Functions; RSA Algorithm and variants; Discrete and Public-Key Algorithms; Signatures; Pseudo-random number generators; Identification Schemes and Entity Authentication; Key Distribution; Key Agreement Schemes.

Learning Outcomes

Unit Learning Outcomes	On successful completion of this unit students should be able to: 1. Explain the mathematical ideas underpinning encryption; 2. Critically analyse basic cryptographic algorithms and propose appropriate uses for them; 3. Assess the strengths and weaknesses of a particular algorithm, and determine its suitability for a particular task; 4. Code and modify algorithms to perform specific encryption tasks.

Assessment

Summative Assessment

Element	Type	Weighting	Learning outcomes assessed
1	Coursework	40 %	1-4
2	**Exam**	60 %	1-4

Employability and Sustainability Outcomes

Outcomes	***Element of Assessment***
Apply skills of critical analysis to real world situations within a defined range of contexts.	*1*
Demonstrate a high degree of professionalism.	*1, 2*
Express ideas effectively and communicate information appropriately and accurately using a range of media including ICT.	*1, 2*
Develop working relationships using teamwork and leadership skills, recognising and respecting different perspectives.	
Manage their professional development reflecting on progress and taking appropriate action.	*1, 2*
Find, evaluate, synthesise and use information from a variety of sources.	*1, 2*
Articulate an awareness of the social and community contexts within their disciplinary field.	
Use systems and scenario thinking.	
Engage with stakeholder/interdisciplinary perspectives.	

Description of each element of Assessment

Summative

Element 1: *Coursework, designed and coded solutions to implement and analyse encryption.*

Element 2: *Written three hour exam covering the theory and uses of the main algorithms used in encryption and cryptography specifically:*

1. How the key algorithms work.
2. How an algorithm is encoded into a high level language.
3. What the strengths and weaknesses of a particular algorithm are
4. An awareness of what type of algorithm/technique is used to deal with a particular security concern

Formative

Students receive formative feedback during supported weekly laboratory sessions

Mandatory Learning & Teaching Requirements	*N/A*
Minimum Pass Mark	*N/A*

Learning Activities

Breakdown of Student Learning Activity	**Type of Activity**	**%**
	Summative Assessment	25
	Directed Study	25
	Student-centred Learning	50

Learning Resources

Books recommended for purchase by students	The unit does not follow any specific book.
Essential Reading/ Resources	
Further Reading/ Resources	Menezes A. J. (1996) *Handbook of Applied Cryptography*, CRC, ISBN 13-978-0849385230 Schneier B.(1996) *Applied Cryptography:Protocols, Algorithms and Source Code in C*, John Wiley, 2nd Ed. ISBN 13-978-0471117094 Hoffstein J. Pipher, J. Silverman J.H. (2008*) An Introduction to Mathematical Cryptography*, Springer, ISBN 13-978-1441926746 Stinson D. R. (2005) *Cryptography: Theory and Practice*, Chapman Hall, 3rd Ed. ISBN 13-978-1584885085 K. M. Martin K. M. (2012) *Everyday Cryptography*, Oxford University Press, ISBN 13-978-0199695591

	MMU's VLE will be used to deliver course materials, assessments and to support blending learning.
Specialist ICTS Resources	Hardware and software requirements decided annually and communicated to specialist Technical Support.
Additional Requirements	None

Administration

JACS Code	I120
HESA Academic Cost Centre	121 IT, Systems Sciences and Computer Software Engineering (C1)
Date of Approval	19 December 2013
Date of Most Recent Consideration	19 December 2013
Unit External Examiner	Prof. Reinhold Behringer
Unit Assessment Board	Science and Engineering