MACS H6014: Secure Communications & Cryptography

Short Title:	Secure Communications & Cryptography APPROVED
Full Title:	Secure Communications & Cryptography

Module Code:	MACS H6014

ECTS credits:	10

NFQ Level:	9

Module Delivered in	1 programme(s)

Module Contributor:	Mark Cummins

Module Description:	Module aims include: • identify vulnerabilities in data communication systems • analyse and evaluate the different types of encryption processes available • demonstrate how to secure data communications systems

Learning Outcomes:

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

1. Analyse and evaluate the different types of encryption processes available
2. Identify vulnerabilities in data communication systems
3. Analyse existing technologies and future new technologies
4. Assess vulnerabilities in systems and identify limitations to the application of each technology

Module Content & Assessment

Indicative Content
Role of secure communications in society Review of communication applications: Users and needs, Nature and limitations of secure communication , Types of security threats, secure applications, IPsec and VPNs; threats, risk assessment, viruses; passwords, authentication protocols, hashing (MD5, SHA), random numbers, steganography, classical crypto; PGP, S/MIME, SSH, SSL, IPSec
Threats and Security Management Technical threats to communication security, authentication, confidentiality, integrity (data signatures), availability (PINs, passwords, biometrics, challenge-response control, tamper proof systems. Cipher Algorithms and Key management.
Cryptography Overview of Cryptography, Privacy, Mathematical Overview, Transposition and Substitution Ciphers, Rotor Machine and Polyalphabetic Ciphers, Block Ciphers: DES, Can DES be attacked? Block Ciphers: AES, Public Key Systems, RSA System, Key Management, Digital Signatures and Authentication, Stream Ciphers, Linear Shift Registers, Non-Linear Shift Registers, Watermarking and Steganography, Applications
Secure Communication Threat models, Applied Crypto, Principles, ciphers, pseudo-randomness, encryption schemes. Hashing, One Way Functions and Commitment, Authentication and shared key distribution, Public Key Cryptography, Public Key Digital Signatures, Public Key Infrastructure (PKI), Web and Transaction Layer Security (TLS & SSL), Internet Layer/Protocol security (IP-sec), Denial-Of-Service and Intrusions Attacks on Hosts and Networks, Secure E-Commerce Applications: Copyright Protection, Voting, Auctions. Secure email and Virtual Private Networks.
Tools used to obtain security Encryption, Steganography, Identity based networks, Anonymized networks, Anonymous communication devices, Methods used to "break" security, Bugging, Computers (general), Laser reading of windows, Systems offering a degree of secure communication , Anonymous cellphones, Landlines, Anonymous Internet, Programs offering more secure communications, Skyps, Zfone, secure IRC and Web chat, Trillian, WASTE, hushmail, CryptoHeaven

Indicative Assessment Breakdown	%
Course Work Assessment %	50.00%
Final Exam Assessment %	50.00%

Course Work Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	Researching and implementing a solution for secure communications	3,4	30.00	Week 11
Written Report	Analyse and assess an existing secure communication solution	3,4	20.00	Week 7

Final Exam Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	n/a	None	50.00	End-of-Semester

Indicative 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.*
Reassessment Description Students will need to repeat both the exam and coursework elements

ITB reserves the right to alter the nature and timings of assessment

Indicative Module Workload & Resources

Indicative Workload: Full Time	
Frequency	**Indicative Average Weekly Learner Workload**
Every Week	30.00
Every Week	60.00
Every Week	110.00

Resources

Recommended Book Resources

Richard E. Blahut 2014, *Cryptography and Secure Communication*, 1 Ed., Cambridge University Press [ISBN: 978-110701427]

Douglas R. Stinson 2008, *Cryptography: Theory and Practice*, CRC Press

Keith M. Martin 2012, *Everyday Cryptography: Fundamental Principles and Applications*, 1 Ed., Oxford University Press [ISBN: 978-019969559]

Jonathan Katz 2014, *Introduction to Modern Cryptography*, 2 Ed., Chapman and Hall/CRC [ISBN: 978-146657026]

Supplementary Book Resources

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone 1996, *Handbook of Applied Cryptography*, CRC Press

B. Schneier 1996, *Applied Cryptography*, 2nd Ed., Wiley

This module does not have any article/paper resources

Other Resources

Internet based resource: *The Cryptology ePrint Archive*
http://eprint.iacr.org/

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_KMACS_R	Master of Science in Computing in Applied Cyber Security	1	Mandatory