MIOT H6016: Secure Communication & Cryptography

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

Module Code:	MIOT H6016

ECTS credits:	5

NFQ Level:	9

Module Delivered in	1 programme(s)

Module Contributor:	Mark Cummins

Module Description:	The purpose of this module is to allow learners identify vulnerabilities in data communication systems and analyse and evaluate the different types of encryption and security processes available. The module with teach and 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 and security processes available 2. Identify vulnerabilities in data communication systems 3. 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, threats, risk assessment, authentication protocols, hashing, random numbers, evolution of cryptography and going forward.
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.
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. Secure email and Virtual Private Networks.
Cryptography Overview of Cryptography, Privacy, Mathematical Overview, Transposition and Substitution Ciphers, Block Ciphers, Public Key Systems, RSA System, Key Management, Digital Signatures and Authentication, Stream Ciphers.

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*
Project	Research and evaluate an existing solution for secure communications	1	20.00	Week 6
Project	Analyse and assess a given secure communication solution	2,3	30.00	Week 11

Final Exam Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	End-of-Semester Final Examination	1,2,3	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.

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	60.00
Every Week	65.00

Resources

Recommended Book Resources

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

Douglas R. Stinson 2001, *Cryptography: Theory and Practic*, CRC Press

Keith M. Martin 2012, *Everyday Cryptography: Fundamental Principles and Applications*, 1 Ed., Oxford University Press [ISBN: 978-01996955]

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

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

Supplementary Book Resources

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

This module does not have any article/paper resources

Other Resources

Website: *The Cryptology ePrint Archive*
http://eprint.iacr.org/

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_EMIOT_R	Master of Engineering in Internet of Things Technologies [BN535R 60 credits taught with a 30 credit research project]	2	Mandatory