MODULE SPECIFICATION PROFORMA

Module Code:	COM735

Module Title:	Applied Cryptography

Level:	7	**Credit Value:**	20

Cost Centre(s):	GACP	JACS3 **code** HECoS code::	G170 101029

Faculty:	Arts, Science and Technology	**Module Leader:**	Prof. Vic Grout

Scheduled learning and teaching hours	21 hrs
Guided independent study	179 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
MSc Cyber Security	✓	☐

Pre-requisites
None.

Office use only
Initial approval: 28/11/2018 Version no:1
With effect from: 01/09/2019
Date and details of revision: Version no:

Module Aims

This module will allow students to develop practical skills in realising secure computing, communications and storage based on a variety of theoretical cryptographic principles. There will be a complementary focus on both the underlying mathematics and their implementation in the form of available protocols on real-world systems.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Evaluate cryptographic methods for a variety of purposes in both theory and practice	KS4 KS9	KS6 KS10
2	Assess strengths and weaknesses of systems in terms of recognised security metrics, including resilience to attack	KS4 KS9	KS6 KS10
3	Balance the expectations of secure computing against the difficulties of practical implementation	KS4 KS9	KS6 KS10
4	Apply appropriate practical cryptographic tools in the form of available protocols in real-world scenarios	KS4 KS9	KS6 KS10

Transferable skills and other attributes

Derogations

None.

Assessment:

Indicative Assessment Tasks:

The assessment for this module will be a 50/50 split between a formal exam and a practical implementation assignment. The exam will allow students to demonstrate proficiency in the underlying mathematics, including assessing the strengths, weaknesses and complexities of various algorithms and suchlike. The practical assignment will involve the extended selection and application of tools from a cryptographic protocol suite – such as IPsec – for a given real-world scenario.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1 2	Examination	50	2 hours	
2	3 4	Practical	50		3,000

Learning and Teaching Strategies:

The module will be led by lectures on essential topics but students will be expected to extend parts of the material in their own time. This applies to both the theoretical and practical elements of the module content. Students will also be given reading lists and useful URLs to develop their work on the module. Lectures will be interspersed with smaller tutorial-based sessions to consolidate learning.

Syllabus outline:

A brief history of cryptographic techniques and current relevance
Secure storage and communication
Information security
System availability, data confidentiality and integrity, authentication and non-repudiation
Symmetric, asymmetric and public-key cryptography
Cryptosystems, cryptographic algorithms and implementation
Cryptanalysis and threats
Electronic commerce and digital currencies
Cryptographic standards, legislation and politics
Cryptographic toolkits and protocol suites
IPsec: TLS, SSH, modes,
End-to-end and link-based cryptography
Cryptography in emerging computing technology

Indicative Bibliography:

Essential reading

Moodle VLE Module Page (New material will be posted frequently)

Blokdyk, G. (2018), *IPSec: A Clear and Concise Reference*. Lightning Source.

Piper, F. and Murphy, S. (2002), *Cryptography: A Very Short Introduction*. Oxford: Oxford University Press.

Other indicative reading

IEEE Transactions on Information Forensics and Security, http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206

'Schneier on Security', https://www.schneier.com/

'Handbook of Applied Cryptography Resource Page, http://cacr.uwaterloo.ca/hac/