MODULE **DESCRIPTOR**

MODULE TITLE	PRACTICAL CRYPTOGRAPHY		
MODULE CODE	CO4520 (L7)	CREDIT VALUE	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

The aims of this module are to:

•Provide an in-depth understanding of theoretical and practical aspects of cryptography.
•Introduce cryptographic standards and best practices that students will most likely encounter as a security professional.
•Identify which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation.
•Provide an understanding of potential weaknesses and problems with ciphers and cryptographic protocols.
•Apply symmetric and asymmetric cryptography and best practices as appropriate for a given scenario to achieve data protection.
•Critically discuss cryptographic attacks and countermeasures.

MODULE **CONTENT**

Introduction
History of cryptography
Substitution ciphers, e.g. Caesar cipher, affine ciphers, etc.
Transposition ciphers, e.g. reverse order, columnar chipher, etc.

Symmetric Encryption
Block cipher design principles
Block cipher operation
DES, 3DES, AES, IDEA, etc.
Stream ciphers
RC4, RC5, RC6
Weaknesses

Asymmetric Encryption
Public-key cryptography principles and operation
RSA
Diffie-Hellman Key Exchange
Elliptic Curve Cryptography

Cryptographic data integrity algorithms
Cryptographic hash functions
MD5, SHA, RIPEMD
Message authentication codes
weaknesses
Digital signatures

Key management and distribution
Symmetric key distribution using symmetric encryption
Symmetric key distribution using asymmetric encryption
Distribution of public keys
X.509 Certificates
Public Key Infrastructure (PKI)

Attacks
Ciphertext-only
Known plaintext
Chosen plaintext

Chosen ciphertext
Birthday paradox
Man-in-the-middle

Applications
Random number generators
SSL/TLS protocol
Virtual Private Networks (VPN)
Steganography
Cryptography and malware
Cryptography and the cloud
Cryptocurrency

Digital rights management (DRM)

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Evaluate and compare theoretical and practical aspects of cryptography.
2. Research and report on cryptographic attacks and countermeasures.
3. Critically discuss and evaluate cryptographic controls for data protection.
4. Select appropriate techniques and apply them to solve a given problem.

TEACHING METHODS

The theoretical material will be delivered during the lectures. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to cryptography. During the workshops, students will be introduced to cryptographic concepts, tools and techniques, and have the opportunity to participate in hands-on activities. Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss practical findings. As a result of the discussions, additional directed reading may be required. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

Distance Learning

The module tutor will deliver live online lectures. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in a live lecture will have the opportunity to answer and reflect on guided questions in the subsequent live lectures or participate asynchronously on discussion boards. Where appropriate, students will be also provided with relevant further reading, web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver invited talks and enhance the students' experience.

Virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. Students will be provided with access to virtual laboratories through which they will be able to complete the practical components of the module. The students will obtain the practical sheets from Blackboard and they are expected to follow the instructions included in the practical sheets to complete the lab work. If students have difficulties with a particular exercise, they are expected to contact the module tutor or post a question on the discussion forum, where the module tutor and/or their peers can provide feedback. Different means of communication will be utilized by the tutor to offer support to the students based on the reported issue, i.e. email, Skype, MS Teams, virtual laboratory, etc.

Through the virtual laboratories, the students are expected to apply their theoretical knowledge to solve security problems in a professional and legal way. Feedback to the students will be provided asynchronously through Blackboard. If the need arises, the module tutor will schedule live sessions to provide further feedback to the students.

ASSESSMENT METHODS

This module is assessed through a report and an examination.