Liverpool John Moores University

Title:	APPLIED CRYPTOGRAPHY
Status:	Definitive
Code:	**6017DACOMP** (125377)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Qi Shi	Y

Academic Level:	FHEQ6	**Credit Value:**	20	**Total Delivered Hours:**	57
Total Learning Hours:	200	**Private Study:**	143		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	22
Practical	6
Tutorial	27

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Design and analysis of crypto solutions for securing a selected networked application.	40	
Exam	AS2	Examination	60	2

Aims

To develop an understanding of various security vulnerabilities in and threats to computer networks as well as the importance of network security.
To assess critically a variety of cryptographic algorithms and security techniques for protection of computer networks.
To promote the use of appropriate security techniques to solve network security

problems.

Learning Outcomes

After completing the module the student should be able to:

1	Explain a variety of generic security threats and vulnerabilities.
2	Identify and analyse particular security problems for a given application.
3	Demonstrate advanced knowledge of cryptographic algorithms, security protocols and mechanisms for the provision of security services needed for secure networked applications.
4	Apply appropriate security techniques to solve network security problems.

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Securing a network application	2	3	4
Exam	1	2	3

Outline Syllabus

Fundamentals of cryptography and network security: cryptographic concepts and models, number theory, security concepts, security threats and vulnerabilities, authentication principles and means, trust management, and importance of network security and its applications.
Cryptographic techniques: cryptanalytic attacks, conventional/symmetric cryptography (e.g. AES), block cipher operation, stream ciphers, public-key/asymmetric cryptography (e.g. RSA), cryptographic key distribution, key establishment, hash functions (e.g. SHA), message authentication code and digital signatures (e.g. DSA).
Security measures: message integrity, message confidentiality, user and message authentication, public-key certification, key certificate validation and revocation, and X.509 directory authentication services.
Network security applications: network-based authentication protocols and services (e.g. Kerberos), IP security (e.g. IPSec) for secure Internet-based communications, virtual private networks, web security (e.g. SSL/TLS), e-mail security (e.g. PGP), and wireless security.

Learning Activities

Include attending lectures and tutorials, as well as reading online resources.
This module will have online practical.

Notes

The spectacular growth of the Internet has spawned a great demand for awareness of security threats to computer networks and application of security techniques to network protection. In response to the demand, this module examines various security issues, cryptographic algorithms and security services that are essential for network protection.