Applied Cryptography

Module Information

2022.01, Approved

Summary Information

Module Code	6618YCOM
Formal Module Title	Applied Cryptography
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 6
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
YPC International College (Kolej Antarabangsa YPC)

Learning Methods

Learning Method Type	Hours
Lecture	22
Practical	6
Tutorial	27

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
JAN-PAR	PAR	January	12 Weeks

Aims and Outcomes

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.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Explain a variety of generic security threats and vulnerabilities.
MLO2	2	Identify and analyse particular security problems for a given application.
MLO3	3	Demonstrate advanced knowledge of cryptographic algorithms, security protocols and mechanisms for the provision of security services needed for secure networked applications.
MLO4	4	Apply appropriate security techniques to solve network security problems.

Module Content

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.
Module Overview	
Additional Information	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.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Securing a network application	40	0	MLO2, MLO3, MLO4
Exam	Exam	60	2	MLO1, MLO2, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Qi Shi	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings