Cryptography. Security and Forensics

Module Information

2022.01, Approved

Summary Information

Module Code	5552NCCG
Formal Module Title	Cryptography. Security and Forensics
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 5
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
Nelson and Colne College Group

Learning Methods

Learning Method Type	Hours
Lecture	60

Module Offering(s)

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

SEP_NS-PAR	PAR	September (Non-standard start date)	12 Weeks

Aims and Outcomes

Aims	This module introduces students to the theoretical principles of cryptography and its practical applications. It looks at the interaction between cryptography and security, and introduces the process of forensic investigation.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Examine and assess symmetric encryption algorithms, ciphers, public key encryption protocols and signatures, and their uses.
MLO2	2	Analyse the security issues related to encryption methods
MLO3	3	Carry out and evaluate a digital Forensic Investigation on devices or networks or cyberattacks using recognised methods and within legal and professional guidelines

Module Content

Outline Syllabus	Modular arithmetic, groups, finite fields and probability; random number generation. Symmetric encryption and ciphers. Historical and modern ciphersPublic key encryption algorithms. Primality testing and factoring and discrete logarithms. Key exchange and signature schemes. Analysis of implementation issues. Public key confidentiality and integrity. Common attacks on public key encryption schemesSecurity of encryption. Provable security. Random oracles. Provable security without random oracles. Hybrid encryption. Key Encapsulation Mechanisms (KEMs)Access structures for secret sharing schemes. Applying shared RSA signature generation. Zero-Knowledge proofs. Secure multi-party computation. Evaluating different applications of cryptography; quantum cryptography.Network Security protocols. Network Security cryptographic types.Processes and procedures for digital Forensic Investigation. Tools required to conduct digital Forensic InvestigationCarry out a forensic investigation
Module Overview	
Additional Information	

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Case Study Analysis	50	0	MLO1, MLO2
Report	Forensic Investigation Report	50	0	MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings

Silvester Czanner	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings