Liverpool John Moores University

Title:	CRYPTOGRAPHY. SECURITY AND FORENSICS
Status:	Definitive
Code:	**5552NCCG** (129515)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Nelson Campus

Team	Leader
Silvester Czanner	Y
Robert Askwith	

Academic Level:	FHEQ5	**Credit Value:**	20	**Total Delivered Hours:**	60
Total Learning Hours:	200	**Private Study:**	140		

Delivery Options
Course typically offered: S1, S2 and NS2 (S2 for Jan)

Component	Contact Hours
Lecture	60

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	Case Study	Case Study Analysis	50	
Report	Report	Forensic Investigation Report	50	

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.

Learning Outcomes

After completing the module the student should be able to:

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

Learning Outcomes of Assessments

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

Case Study Analysis	1	2
Forensic Investigation Report	3	

Outline Syllabus

Modular arithmetic, groups, finite fields and probability; random number generation. Symmetric encryption and ciphers. Historical and modern ciphers

Public 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 schemes

Security 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 Investigation

Carry out a forensic investigation

Learning Activities

Lectures
These will not normally be traditional didactic lectures in which the student plays little active part, but will be delivered in small groups of up to 20

Notes

-