Module Specification

1. Factual information			
Module title	**T318: Applied Network Security**	**Level**	**Undergraduate**
Module tutor		**Credit value**	**30**
Module type	**Taught**	**Notional learning hours**	**8**

2. Rationale for the module and its links with other modules

- People, organizations, and enterprises are becoming increasingly dependent on digital services. Therefore, the need arises to protect information from being maliciously intercepted, disrupted, or misused.

3. Aims of the module

The aims and objectives of this course are to:

- Define the threats to network security, and describe the differences between them.
- Describe encryption techniques, including symmetric and asymmetric encryption methods.
- Explain the most widely used encryption algorithms and standards, with focus on wireless, cloud, and internet security.
- Equip students to be able to assess and manage network security risks, and implement appropriate countermeasures.
- Allow students to perform independent research in the area and to critically read and analyse third party material.

4. Pre-requisite modules or specified entry requirements

Students should have completed the study of the course T216B & TM260

5. Intended learning outcomes	
A. Knowledge and understanding	**Learning and teaching strategy**
After studying the course you will be able to: A1. Describe the operation of encryption techniques: symmetric and asymmetric ciphers, block and stream ciphers A2. Define and explain the differences between different encryption algorithms and standards A3. Analyse and compare the performance of different encryption methods A4. Design and implement encryption algorithms A5. Describe the protocols for physical, network, and transport level security A6. Define the most common threats to network and internet security, explain their operation, and discuss their differences A7. Describe the protocols and countermeasures used for protecting network and internet traffic	• 25% face-to-face tutorial sessions • TMA work • Course textbook and support material

B. Cognitive skills	Learning and teaching strategy
After studying the course you will be able to: B1. Recognise the threats to network security and assess their inherent risks B2. Read, evaluate, and critically review technical documents and extract useful information from these documents on topics related to network security and cryptography algorithms	• 25% face-to-face tutorial sessions • TMA work • Course textbook and support material

C. Practical and professional skills	Learning and teaching strategy
After studying the course you will be able to: C1. Use the studied concepts to implement, analyse, and assess different encryption algorithms and techniques C2. Identify the threats to network security and take appropriate countermeasures	• 25% face-to-face tutorial sessions • TMA work • Course textbook and support material

D Key transferable skills	Learning and teaching strategy
After studying the course you will be able to: D1. Become an independent self-learner in order to tackle more advanced topics and remain up-to-date in the field of network security	• 25% face-to-face tutorial sessions • TMA work • Course textbook and support material

D Key transferable skills	Learning and teaching strategy
D2. Improve your technical writing skills on topics related to cryptography and network security	

6. Indicative content.
1. Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques; Block Ciphers: Electronic Code book, Cipher Block Chaining, Stream Ciphers
2. Data Encryption Standard (DES), Advanced Encryption Standard (AES), Multiple Encryption and Triple DES
3. Public-Key Cryptography, RSA algorithm, Key Management and Distribution
4. Cryptographic Hash Functions, Secure Hash Algorithm (SHA), Message Authentication Codes, User Authentication, Digital Signatures
5. Physical Level Security, Network Access Control, IEEE 802.1x, Cloud Security, Risks and Countermeasures
6. Network Level Security, IP Security (IPSec), Virtual Private Networks (VPN), Encapsulating Security Payload, Internet Key Exchange
7. Transport Level Security, Secure Sockets Layer, HTTPS, Secure Shell (SSH)
8. Application Level Security, Web Security Considerations, Email Security
9. Wireless Network Security, Mobile Device Security, IEEE 802.11i Wireless LAN Security
10. Threats and Attacks: Malicious Software, Viruses, Worms, Social Engineering, SPAM, Trojans, (Distributed) Denial of Service Attacks
11. Countermeasures: Intrusion Detection, Firewalls
12. Legal and Ethical Issues: Cybercrime and Computer Crime, Intellectual Property, Privacy

7. Assessment strategy, assessment methods and their relative weightings
TMA Work: 20% MTA: 30% Exam: 50%

	8. Mapping of assessment tasks to learning outcomes												
Assessment tasks	**Learning Outcomes**												
	A1	A2	A3	A4	A5	A6	A7	B1	B2	C1	C2	D1	D2
TMA	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
MTA	✓	✓	✓	✓									✓
Final Exam	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓

9. Teaching staff associated with the module	
Tutor's name and contact details	**Contact hours**
To be appointed at a later date since this is a new course.	

10. Key reading list				
Author	**Year**	**Title**	**Publisher**	**Location**
William Stallings	**2014**	**Cryptography and Network Security: Principles and Practice, 6th Edition**	**Pearson Education**	**USA**

11. Other indicative text (e.g. websites)
• **Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, 1996** • **Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. [Chapters available for download at: http://cacr.uwaterloo.ca/hac/]** • **Chris Sanders and Jason Smith, "Applied Network Security Monitoring: Collection, Detection, and Analysis", 1st Edition, Syngress, 2014** • **Jaydip Sen (Ed.), Applied Cryptography and Network Security, InTech, 2014. Available online: http://www.intechopen.com/books/applied-cryptography-and-network-security** • **Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, "Security in Computing", 5th Edition, Prentice Hall, 2015** • **Douglas Stinson, "Cryptography Theory and Practice", 3rd Edition, Chapman and Hall/CRC Press, 2005**