Module Specification

1. Factual information			
Module title	**TM290: Cryptography and Internet Security**	**Level**	**2**
Module tutor	**TBA**	**Credit value**	**10**
Module type	**Taught**	**Notional learning hours**	**3**

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

- Nowadays, people shop online, work online, play online. As our lives become increasingly dependent on digital services, the need arises to protect our personal information from being maliciously intercepted, disrupted, or misused.

3. Aims of the module

The aims and objectives of this module 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 internet security.
- 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 TM112

5. Intended learning outcomes	
A. Knowledge and understanding	**Learning and teaching strategy**
Upon completing this module, students will be able to: **A1.** Describe the operation of symmetric ciphers **A2.** Define and explain the differences between different encryption algorithms and standards **A3.** Describe the operation of asymmetric ciphers **A4.** Analyse and compare the performance of different encryption methods **A5.** Design and implement simple encryption algorithms **A6.** Define the most common threats to internet security, explain their operation, and discuss their differences **A7.** Describe the protocols and countermeasures used for protecting internet traffic	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

B. Cognitive skills	**Learning and teaching strategy**
Upon completing this module, students will be able to: **B1.** Recognise the threats to online security **B2.** Read, evaluate, and critically review technical documents and extract useful information from these documents on topics related to cryptography and internet security	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

C. Practical and professional skills	Learning and teaching strategy
Upon completing this module, students will be able to: **C1.** Use the studied concepts to analyse and assess the efficiency of different encryption standards **C2.** Identify the threats to internet security and take appropriate countermeasures	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

D Key transferable skills	Learning and teaching strategy
Upon completing this module, students will be able to: **D1.** Demonstrate independent self-learning capabilities in order to tackle more advanced topics and remain up-to-date in the field of cryptography and internet security **D2.** Employ your technical writing skills on topics related to cryptography and internet security	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

6. Indicative content.	
1.	Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques
2.	Block Ciphers: Electronic Code book, Cipher Block Chaining
3.	Data Encryption Standard (DES), Advanced Encryption Standard (AES), Multiple Encryption and Triple DES
4.	Pseudorandom Number Generation and Stream Ciphers
5.	Public-Key Cryptography, RSA algorithm, Diffie-Hellman Key Exchange
6.	Cryptographic Hash Functions and Secure Hash Algorithm (SHA)

6. Indicative content.
7. Key Management and Distribution: Symmetric Key Distribution Using Symmetric and Asymmetric Encryption, Distribution of Public Keys, Public-Key Infrastructure
8. User Authentication: Remote User-Authentication Using Symmetric and Asymmetric Encryption
9. Transport-Level Security, Web Security Considerations, Secure Sockets Layer, HTTPS, Secure Shell (SSH)
10. IP Security (IPSec), Encapsulating Security Payload, Internet Key Exchange
11. Malicious Software, Viruses, Worms, Social Engineering, SPAM, Trojans, Denial of Service Attacks
12. Firewalls, Wireless Network Security, IEEE 802.11i Wireless LAN Security

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**
TBA	

10. Key reading list				
Author	**Year**	**Title**	**Publisher**	**Location**
William Stallings	**2014**	**Cryptography and Network Security: Principles and Practice, 6th Edition**	**Pearson Education**	**USA**
Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies	**2015**	**Security in Computing, 5th Edition**	**Prentice Hall**	
• **Introduction to cyber security – OU Module: http://www.open.edu/openlearn/ocw/course/view.php?id=1218**				

11. Other indicative text (e.g. websites)
https://lms.arabou.edu.kw/