Module Title	**Cybersecurity and Cryptography**
Course Title	BEng (Hons) Electronic and Computer Systems Engineering
School	☐ ASC ☐ ACI ☐ BEA ☐ BUS ☒ ENG ☐ HSC ☐ LSS
Division	Electrical and Electronic Engineering
Parent Course (if applicable)	
Level	6
Module Code *(showing level)*	EEE_6_CSC
JACS Code (completed by the QA)	
Credit Value	20 credit points
Student Study Hours	Contact hours: 52 Student managed learning hours: 148 Placement hours: 0
Pre-requisite Learning	Familiarity with basic data structures, computer organization, hardware and software of a typical computer system including the operating system**.** Good skills of Computer Programming in a High-level language, such as C++ or Java. Good knowledge of basic and linear algebra and on number theory and finite fields.
Co-requisites	None
Excluded combinations	None
Module co-ordinator	
Short Description (max. 100 words)	This module provides a thorough discussion on cybersecurity and cryptography. It covers thoroughly computer security, network security, information security and mobile security. It discusses critical network security techniques, including the use of firewalls, encryption, intrusion detection, and enterprise-wide security policies. Network security is a major concern when designing and maintaining modern networks, which typically use open protocols and connect to public networks such as the Internet. Cryptographic algorithms in network protocols and network applications as well as the security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses) are examined.
Aims	This module aims to provide study to the fascinating realm of cybersecurity including various examples of current security topics.

	The main goal is to provide a broad and comprehensive coverage of the entire network security field and an up-to-date survey of developments in computer security. It aims a firm grasp of the concepts and history of network development and network security as they have evolved. It targets to define the threats to computer and network systems, evaluating the relative risks of these threats, and developing cost-effective and user-friendly countermeasures. It is also intended to burst the mystique, shine a light into how and why people attack computers and networks, and prepare the student with the right techniques to begin winning the computer and network security game. A few objectives in this area collectively encompass the following: • Recognition that security is risk management and inherently includes tradeoffs. • Familiarity with the implications of hostile users, including social engineering attacks and misuse cases. • A framework for understanding algorithms and other technological measures for enhancing security. • Strategic and tactical design issues in information security.
Learning Outcomes (4 to 6 outcomes)	Knowledge and Understanding: • Analysis and modelling of the underlying principles and practices of computer and network security. Identify the concepts, structure and mechanisms that underline Information security, Network Security and Cryptography (A1, A2, A3). • Mathematically analyse and test algorithms such as DES, RSA, categorise and compare the motivations and weaknesses in various methods for applying secret key (block) encryption to a message stream such as cipher block chaining (CBC), cipher feedback mode (CFB), and counter mode (CTR) (A1, A2, A3). Intellectual Skills: • To present a detailed analysis of system protection and security including threads and mechanisms for providing computer and network security. Analyse mathematically Secret and public key cryptographic algorithms; analyse authentication techniques; relate and analyse how one can use a hash for a message authentication code (MAC); analyse Network and web security (B1, B2, B3, B4) Practical Skills: • Categorise and classify security relevant tools, standards and security constraints. Perform modular arithmetic and breakdown the basic theory of security algorithms (e.g. Totient function and Euler's theorem) (C1, C4, C6). • Explain the problems solved by multi-factor authentication methods including biometrics. Implement computing algorithms and programs to encrypt and decrypt data (C2, C3). Transferable Skills: • To be able to compose, design and implement mathematical/computer methods to simulate security and cryptographic algorithms by using programming languages such as C++/Java/Python. To effectively communicate and critically evaluate observed results in a technical format (D2, D3, D4, D6)

Employability	This module is suitable for students who intend to work in security enterprises as network security engineers, analysts, programmers, managers or developers. The material covered is particularly relevant to students specialising in the concepts, structure, and mechanisms of cybersecurity and cryptography. Students will be equipped with the essential theory and practice enabling them to understand, design, implement, test, evaluate and simulate security algorithms, in both industry and research. Students will be specialised in the design and implementation of the most important and modern areas of computer security. Students will attain the technical expertise and knowledge to take a good idea from conception through to a viable security design, as well as security maintenance and administration, a key characteristic for many employers.
Teaching and learning pattern	Contact hours includes the following: (please click on the checkboxes as appropriate) √ Lectures ☐ Group Work: ☐ Seminars ☒ Tutorial: ☒ Laboratory ☒ Workshops ☒ Practical ☒ VLE Activities
Indicative content	History, overview, and principles of security. Relevant security tools, standards, and/or engineering constraints. Legal and ethical security issues. Computer and network security classifications. System and Network threats. Vulnerabilities and exploitation. Cryptography as a security tool. Mutual trust, user authentication and implementation of security defences. Message authentication codes. Firewalling to protect systems and networks. Data security and integrity. Symmetric and asymmetric ciphers. Classical and advanced encryption techniques. Public-key cryptography. Cryptosystems. Cryptographic data integrity algorithms and message authentication codes. Mutual trust. Network access control and cloud security. Web security, SSL, Secure Shell (SSH), IP security. Wireless network security. Electronic Mail Security (PGP, S/MIME). Internet security and authenticating applications (Kerberos) Resource protection models Trusted computing and Side-channel attacks Software security.
Assessment method (Please give details – of components, weightings, sequence of components, final component)	Formative assessment: Verbal feedback in Tutorial and weekly workshops (lab exercises). Quizzes as part of the lab exercises (Logbook) Summative assessment: Component 1 (EX1_60) – Written examination 60% • Exam: 2-hour unseen written exam (60%) (A1, A2, A3, B1, B3)

	Component 2 (CW1_40) – Coursework (CW) 40% comprises two subcomponents: a Logbook and an assignment. • SC1_60: Logbook 60% (B2, C3, C4, D2, D4) • SC2_40: Assignment 40% (B4, C2, C6, D3, D6)

	Workshop logbook detailing the practical work constitutes 20%. A laboratory manual will be provided for each student containing details of laboratory organisation and procedures and the instructions for the individual exercises/assignments/mini projects. The practical workshop includes use of cybersecurity and cryptography. **Assignment (formal report)** not exceeding 2000 words. This component will constitute 20% of the module mark. Students will have to write a technical formal report by selecting one among a few given topics in the areas of cybersecurity and cryptography. To be awarded a pass in the module a student must: (a) achieve an overall weighted average mark for the module of at least 40% and (b) achieve the minimum threshold mark (30%) in each of the two components.
Mode of resit assessment (if applicable)	Summative assessment: Standard mode of referral 2-hour unseen written exam (60%) Coursework (40%)
Indicative Sources ***(Reading lists)***	Core materials: **10. Cryptography and Network Security: Principles and Practice**, 7th edition (2017), William Stallings, Pearson Education Limited, Print ISBN: 9781292158587, 1292158581, eText ISBN: 9781292158594, 129215859X **11. Computer Security**, 2nd edition (2019), Matt Bishop, Addison-Wesley Professional PTG, Print ISBN: 9780321712332, 0321712331, eText ISBN: 9780134097176, 0134097173 Optional reading: 1. **Network Security Essentials: Applications and Standards, International Edition**, 6th edition (2017), William Stallings, Pearson Education Limited, Print ISBN: 9781292154855, 1292154853, eText ISBN: 9781292154916, 1292154918 2. **Introduction to Computer and Network Security**, (2014), Richard R. Brooks, Chapman & Hall, Print ISBN: 9781439860717, 1439860718, eText ISBN: 9781439860724, 1439860726 3. **Introduction to Computer Security: Pearson New International Edition**, 1st Edition (2014), Michael Goodrich; Roberto Tamassia, Pearson Education Limited, Print ISBN: 9781292025407, 1292025409, eText ISBN: 9781292037912, 1292037911 4. **Principles of Information Security**, 6th Edition (2018), Michael E. Whitman; Herbert J. Mattord, Cengage Learning,

Print ISBN: 9781337102063, 1337102067, eText ISBN: 9781337516938, 1337516937

Other Learning Resources	VLE (Moodle) site for this module: it contains weekly lecture notes, workshop laboratory exercises, tutorial problems and additional support teaching and learning material.