Partnered with

The Knowledge Hub Universities
Egypt

Course Specification A

BSc (Hons) Ethical Hacking and Cyber Security
TKHU026

School of Computing

Academic Year: 2025/2026

Please note: This specification provides a concise summary of the main features of the course and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if they take full advantage of the learning opportunities that are provided.

We regularly review our course content, to make it relevant and current for the benefit of our students. For these reasons, course modules may be updated.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education. Changes have only been made where an aspect of the provision at Coventry University is not relevant to the delivery at TKH or where specific information relevant to the delivery of this course in Egypt must be introduced, e.g. entry requirements, course management.

PART A.1 Course Specification

Ethical Hacking and Cyber Security (Foundation Year)

1. Introduction

This document outlines level 3 of the BSc Ethical Hacking and Cyber Security and should be considered along with Part A.2 Ethical Hacking and Cyber Security document.

Ethical Hacking and Cyber Security Level 3

The Level 3 course will normally introduce prospective students where English is not their first language to the key concepts in Ethical Hacking and Cyber Security as well as the academic study skills and language they will need to operate effectively at degree level. Successful completion of Level 3 will enable progression to Level 4 of the BSc Ethical Hacking and Cyber Security programme. Level 3 consist of 80 credits of subject-specific modules and 40 credits of academic English skills modules. The course will be fully taught in English with embedded specialist English-language and study skills to support students in their further undergraduate study in Coventry University degree courses.

Overall Aims of Level 3

Level 3 will enable students to:

- Become familiar with the key concepts in Ethical Hacking and Cyber Security.
- Develop the language and subject-specific academic study skills necessary to study at university level.
- Manage their own learning and acquire transferable skills such as communication, initiative and problem solving that equips and orientates students for higher education.

There is a global shortage of engineers, computing scientists and construction professionals and employment opportunities remain extremely buoyant.

The course is designed to foster a critical, analytical and experiential approach to embedded study skills and subject-specific academic English. The course supports students towards informed career choices, with awareness of their own strengths and knowledge of career pathways. Successful completion of this year will enable progression to year 2 (Level 4) of the BSc Ethical Hacking and Cyber Security programme. This year aims to develop knowledge and skills that can be applied to solving scientific problems. The educational experience also aims to develop students' intellectual and personal skills. The course has equal proportions of applied science and engineering (40 credits), mathematics (40 credits) and English language (40 credits).

The mathematics modules cover algebra, descriptive and inferential statistics, trigonometry, vectors and vector operations, differential and integral calculus, some simple solution methods for various types of differential equations and methods to characterise and handle uncertainty. The Applied Science and Engineering modules aim to develop the students working knowledge of the scientific theories that underpin the engineering disciplines. The first develops students' scientific knowledge and laboratory skills. The second module develops the theory and introduces the application of theory through the use of design, including the concept of prototyping and the use of computer aided design.

2 Outline and Educational Aims of the Course

Level 3 in BSc Ethical Hacking and Cyber Security is designed to provide an introduction to relevant mathematic concepts and scientific theories and their application in the design of scientific solutions.

Successful completion of the course enables progression to Level 4 of the BSc Ethical Hacking and Cyber Security programme

The course will be fully taught and assessed in English with embedded specialist English-language and study skills support.

Level 3 year of study forms part of the BSc in Ethical Hacking and Cyber Security programme.

Coventry University Level 3: General Course Aims:

Level 3 will enable students to:

- Become familiar with the key concepts in their chosen subject area.
- Develop the language and subject-specific academic study skills necessary to study at university level.
- Manage their own learning and acquire transferable skills such as communication, initiative and problem solving that equips and orientates students for higher education.

Ethical Hacking and Cyber Security Level 3 - Specific Course Aims:

This Level 3 in Ethical Hacking and Cyber Security aims to provide students with a firm basis for onward study in this bachelor's degree and develop knowledge and skills that can be applied to solving scientific problems. The educational experience also aims to develop students' intellectual and personal skills.

It provides opportunities for students to:

- Acquire a broad knowledge of mathematical concepts and physical science theories relevant to science and its' technological, environmental, cultural, economic and social context;
- Develop practical skills appropriate to computing;
- Strengthen study skills and academic English language skills, specific to the subject areas;
- Become an independent learner and acquire transferable skills such as communication, presentation, visual and digital fluency, critical reflection, initiative and problem solving;
- Recognise and respond appropriately to ethical values, the public interest and professional standards;
- Develop appropriate skills, understanding and experience to prepare students for successful transition into further and higher education in computing.

3 Course Learning Outcomes

A student who successfully completes the course will have achieved the following learning outcomes and be able to:

1. demonstrate an understanding of the relevant mathematical and scientific principles
2. apply fundamental design and analysis methods to investigate and propose solutions to scientific problems;
3. apply knowledge of physical sciences to computing issues
4. apply the necessary study and research skills in support of written, oral and group assessments
5. contribute effectively to a team and implement the necessary planning to achieve objectives;
6. clearly communicate research, concepts, solutions and recommendations

4 Course Structure and Requirements, Levels, Modules, Credits and Awards

Modules within level 3 of the course and their credit value is identified in Table 1a. All modules are mandatory.

Module Credit Level	Module Code	Module Title	Credit Value	Course Learning Outcomes	Semester
3	KH3123CEM	Applicable Mathematics	20	1,2	1
3	KH3125EXQ	Foundation Physics	20	1,2,3	1
3	KH3111HUM	Foundation Academic English 1 for Engineering and Computing	20	4,5,6	1
3	KH3129CEM	Applied and Computational	20	1,2	2

		Mathematics			
3	KH3126EXQ	Applied Science and Engineering	20	1,2,3	2
3	KH3112HUM	Foundation Academic English 2 for Engineering and Computing	20	4,5,6	2

Table 1a.

Progression to level 4 BSc Ethical Hacking and Cyber Security

To progress to Level 4 of the BSc in Ethical Hacking and Cyber Security degree, a student must have passed or been credited with all the modules.

5 Criteria for Admission and Selection Procedure

1 AS Level grade D and 5 GCSEs (including English Language, Mathematics and Science) at A*- C or 9 - 4 in the new GSCE grading structure **OR** 8 GCSEs (including English Language, Mathematics and Science) at A*- C or 9 - 4 in the new GSCE grading structure) **OR** Tawjihiya/General Secondary School certificate with minimum 60% **OR** Pass grades in IB Diploma.

In the case of applicants whose first language is not English, an adequate proficiency in English must be demonstrated. This would normally be a minimum IELTS score of 5.5 (with no less than 5.0 in each component) or equivalent.

All equivalent qualifications are welcome, as are mature students with alternative experience.

PART A.2 Course Specification (Published Document)

Ethical Hacking and Cyber Security

1. Introduction

This document outlines level 4, 5 and 6 of the BSc Ethical Hacking and Cyber Security and should be considered along with Part A.1 Ethical Hacking and Cyber Security document.

Cyber Security is a rapidly growing area, which has an impact throughout society. The need for Cyber Security specialists is highlighted in the Department for Digital, Culture, Media & Sport (DCMS) Cyber Security Breaches Survey published in March (2021), 39% (2.3 million) of all UK businesses reported a cyber breach or attack in 2020/2021.

As one of the first universities to offer a degree program in Ethical Hacking, Coventry has over a decade of experience teaching cyber security and producing graduates who go onto successful careers in the sector.

Coventry University's Ethical Hacking and Cybersecurity BSc (Hons) course has been developed to provide you with an excellent practical and theoretical understanding of cybersecurity, hacking, digital forensics, and the underlying computer science behind these topics. Graduates of the course will be able to identify, analyse and demonstrate the threats to modern information systems, and be able to advise organisations on how to secure their systems against those threats.

The course is aimed at:

- People wishing to move on to become penetration testers, security consultants, network security specialists or digital forensics practitioners
- People with an interest in the practical application of Computer Science, who would like a job in a fast changing and dynamic industry
- People interested in the practical aspects of IT management

Students on the course will study topics under 4 key themes:

- Ethical Hacking: Web Security, Penetration Testing, Reverse Engineering and Exploit Development
- Security Operations: Risk Management, Incident Response and information security management
- Digital Forensics: Data recovery, and the examining of digital evidence
- Network Security: Designing, developing, and administrating network infrastructure.

The course also examines more traditional computer science topics, such as programming and operating systems.

2 Available Award(s) and Modes of Study

Title of Award	Mode of attendance	UCAS Code	FHEQ Level
BSc (Hons) Ethical Hacking and Cyber Security	3 Years FT		6
Fall Back: BSc Ethical Hacking and Cyber Security			6
Diploma in Higher Education Computing			5
Certificate in Higher Education Computing			4

[1] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/real-world-impact

3 Awarding Institution/Body	Coventry University
4 Collaboration	Autonomous Franchise
5 Teaching Institution and Location of delivery	Coventry University Branch at TKH The Knowledge Hub Universities Campus New Administrative Capital, Residential Area 7, R7, Cairo Governorate
6 Internal Approval/Review Dates	Date of approval: August 2019 Date for next review: 2026/27
7 Course Accredited by	N/A
8 Accreditation Date and Duration	N/A
9 QAA Subject Benchmark Statement(s) and/or other external factors	Quality Assurance Agency for Higher Education (QAA) Computing Benchmark Statement ACM Cyber Security curriculum guidance NCSC requirements
10 DBS requirement	Not required
11 Date of Course Specification	May 2023
12 Course Director	

13 Outline and Educational Aims of the Course

The main aim of the Ethical Hacking and Cyber Security degree is to allow students to gain knowledge, practical skills and experience in topics related to a career in information security. This includes:

- specialised practical skills such as penetration testing, incident response, and malware analysis.
- Traditional computer science topics like programming and cryptography.
- The legal and ethical factors around security

Graduates of the Ethical Hacking and Cyber Security course will:

- have a clearly targeted and developed set of skills in computer science with special emphasis on security

- To be able to critically evaluate and defend against the threats posed to modern information structures and will be able to apply defences against such threats,
- be able to devise methods of testing a systems security and possess the skills needed to break into systems that have vulnerabilities
- Utilise and implement organisational structures, such as the SOC (Security Operations Centre) to protect systems and organisations against cyber attack.
- be able to advise a company on how to set up secure systems

The skills base of this course generally resides within the body of knowledge defined by the QAA Computing benchmark statement. As well as the technical foci, the courses all contain content that prepares students in social, ethical, legal and professional aspects of a cooperative human environment such as the workplace.

14 Course Learning Outcomes

On successful completion of the course a student will be able to:

1. **Computer Systems:** Demonstrate a deep understanding of common software, platforms, and systems, with the ability to use and secure these systems

2. **Penetration Testing:** Use a range of tools, (such as nmap and Metasploit), and techniques (such as PTES, or the Cyber Kill Chain), to perform structured penetration tests on systems and networks, and create appropriate reports.

3. **Security Operations and Incident Management:** Evaluate and apply risk management and MAPE-K principles to computer systems and infrastructure, using appropriate methodologies and technologies for risk management and incident response.

4. **Programming:** Create solutions to a variety of computational and real-world problems using appropriate programming languages.

5. **Secure Systems and Code Review** be able to create software and systems that use appropriate tools, techniques, standards, and best practices in order to minimise the chance of exploitable errors and be able to analyse third-party code to determine level of risk.

6. **Computer Architectures:** critically evaluate the role of the underlying computer architecture, including traditional operating systems, cloud based infrastructures, and virtualisation, in security.

7. **Networking:** Demonstrate knowledge of the principles behind computer networks and apply these principles to the design and management of secure network infrastructure.

8. **Digital Forensics:** Analyse the artefacts of data recovery that compromise the study of computer forensics in accordance with applicable law and ACPO principles. Examine sources of electronic evidence, search and seizure issues, imaging digital evidence, and validating image file integrity.

9. **Human Factors**: Analyse the role that human factors, such as security policy and social engineering, can have on security.

10. **Professional Practice:** understand professional practices of the modern cyber security and wider IT industry, including technical (e.g. version control / automated testing) but also social, ethical & legal responsibilities

11. **Transferable Skills:** apply a wide variety of degree level transferable skills including time management, team working, written and verbal presentation to both experts and non-experts, and critical reflection on own and others work.

---

15 Course Structure, Modules, Credits and Progression and Award Requirements

15.1 Progression through course

To progress from one level to the next, students must meet the requirements specified in the University regulations. The conditions for progression from one level to the next and the classification of degrees awarded will be determined by the number and level of successful module passes achieved in accordance with the University Regulations.

Semester of Study/One Academic year at Coventry University (Optional)

The course structure and timing of delivery at The Knowledge Hub shall be aligned with the equivalent course at Coventry University to enable a student to complete a semester of study/one academic year at Coventry University as part of their studies. The marks achieved at Coventry University will be used in the assessment of the student's performance at the end of each level and used in the calculation of the final degree classification.

15.2 Conditions for fall back award

For a fall back award students must meet the relevant requirements specified in the University regulations.

Modules within the course, their status (whether mandatory or options), the levels at which they are studied, and their credit value are identified in the table below.

Credit level	Module Code	Title	Learning Credit	Assessment credit	Mandatory/ Optional	Course Learning Outcomes
4	KH4014CMD	Cyber Security Fundamentals	20	20	Mandatory	1,2,6, 10
4	KH4017CMD	Introduction to Programming	20	20	Mandatory	4, 10
4	KH4018CMD	Networking and Computer Architectures	20	20	Mandatory	1, 6, 7
4	KH4016CMD	Information Security Management	20	20	Mandatory	3, 8, 10
4	KH4019CMD	The Ethics and Legal Frameworks of Cyber Security	20	20	Mandatory	7, 9, 10, 11
4	KH4015CMD	Foundations of Computer Science	20	20	Mandatory	1,6, 10
5	KH5038CMD	Practical Penetration Testing	20	20	Mandatory	1, 2, 10
5	KH5039CMD	Programming and Operating Systems	20	20	Mandatory	1, 4, 6
5	KH5037CMD	Foundations of Networking	20	20	Mandatory	1, 5, 7
5	KH5040CMD	Security Operations	20	20	Mandatory	3, 10
5	KH5036CMD	Digital Forensics	20	20	Mandatory	1, 3, 8
5	KH5041CMD	The Internet and Web Technologies	20	20	Mandatory	1, 2, 4
6	KH6036CMD	Advanced Penetration Testing	20	20	Mandatory	1, 2, 11
6	KH6041CMD	Reverse Engineering and Exploit Development	20	20	Optional	1 ,2, 5
6	KH6042CMD	Secure Network Design and Management	20	20	Optional	1, 5, 7, 9
6	KH6038CMD	Digital Security Risk and Audit Management	20	20	Mandatory	3, 10
6	KH6037CMD	Applied Cryptography	20	20	Mandatory	1, 5, 10
6	KH6035CMD	Advanced Digital and Network Forensics	20	20	Optional	1, 3,8
6	KH6040CMD	Research Project Preparation	20	20	Mandatory	8, 11
6	KH6039CMD	Research Project Delivery	20	20	Mandatory	8, 11

Cascade of Awards:

BSc Route:

BSc (Hons) Ethical Hacking and Cyber Security
↓
BSc Ethical Hacking and Cyber Security
↓
Diploma of Higher Education in Computing
↓
Certificate of Higher Education in Computing

16 Criteria for Admission and Selection Procedure

Level 4 entry

Students applying with an International Baccalaureate with a score of 29 or above, to include one from Mathematics, Physics, Chemistry, Design Technology or IT at Higher level.

A-level: BBB to include one from Mathematics, Physics, Chemistry, Further Mathematics, Computer Science, Computing or Design Technology. Excludes General Studies.

Students who have achieved a Diploma with 2.5 GPA out of 4 or 3.0 CGPA out of 5 (Subject to syllabus match).

Students are required to have an IELTS score of at least 6.0 overall with a minimum of 5.5 in each skill or TOEFL iBT with a score of 79 and a minimum component score of 18.

Nonstandard entry students will be considered on a case-by-case basis.

17 Academic Regulations and Regulations of Assessment

This Course conforms to the Regulations for the delivery of Coventry University Undergraduate awards at the Coventry University Branch at The Knowledge Hub, Egypt.

18 Indicators of Quality Enhancement

The Course is managed by the School of Computing Board of Study, of The Knowledge Hub.

The Programme Assessment Board (PAB) for The Knowledge Hub is responsible for considering the progress of all students and making awards in accordance with both the University and course-specific regulations.

The assurance of the quality of modules is the responsibility of the Boards of Study which contribute modules to the course. This activity will be performed in partnership with Coventry University, UK.

External Examiners have the opportunity to moderate all assessment tasks and a sample of assessed work for each module. They will report annually on the course and/or constituent modules and their views are considered as part of

the Collaborative Course Quality Enhancement Monitoring (C-CQEM). Details of the C-CQEM process can be found on The Knowledge Hub's web site.

Students are represented on the Student Forum and Board of Study, all of which normally meet two or three times per year. They are also represented at the branch board which happens once every year. Student views are also sought through module and course evaluation questionnaires.

The QAA's Higher Education Review undertaken in February 2015 confirmed that Coventry University meets the UK expectations regarding the:

- setting and maintenance of the academic standards of awards
- quality of student learning opportunities
- quality of the information about learning opportunities
- enhancement of student learning opportunities

19 Additional Information

Enrolled students have access to additional, key sources of information about the course and student support including:

* Academic Course Director(s) are responsible for particular activities across the course and are able to provide advice and support to students in course-related matters;

* Student Handbook;

* Module Descriptors;

* CCQEM Reports;

* The Knowledge Hub Study Support Information.