t

**MODULE SPECIFICATION**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Part 1: Information** | | | | | | | | |
| **Module Title** | | Cryptography, mathematics and algorithms | | | | | | |
| **Module Code** | | CY201 | | **Level** | | 5 | | |
| **For implementation from** | | September 2020 | | | | | | |
| **UWE Credit Rating** | | 30 | | **ECTS Credit Rating** | | 15 | | |
| **Faculty** | | Environment and Technology | | **Field** | |  | | |
| **Department** | | Computer Science and Creative Technologies | | | | | | |
| **Contributes towards** | | BSc (Hons) Cyber Security Technical Professional  Compulsory | | | | | | |
| **Module type:** | | Standard | | | | | | |
| **Pre-requisites** | | | None | | | | | |
| **Excluded Combinations** | | | None | | | | | |
| **Co- requisites** | | | None | | | | | |
| **Module Entry requirements** | | | None | | | | | |
|  | | | | | | | | |
| **Part 2: Description** | | | | | | | | |
| This module introduces students to the theoretical principles of cryptography and looks at some practical applications, many of which are used on a daily basis. Apprentices are expected to investigate the inner workings of cryptographic systems and how to correctly use them in real-world applications. Apprentices are expected to explore the mathematical algorithms in relation to cryptography and their applications. Apprentices are also expected to analyse the symmetric encryption methods and ciphers, public key cryptography and the security issues related to their implementation. In addition, apprentices are expected to investigate advanced encryption protocols and their applications.  The module covers some of the mathematical principles and theory that underpin computing.  Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.  This module will be based on ensuring that apprentice’s practical skills and knowledge gained in the block release sessions are carried into the workplace to inform their employment and generation of evidence of competency.  You will cover:   * automata, computability and complexity * sets, relations and functions * graphs and trees * main cryptographic techniques   + concepts of authentication, integrity and non-repudiation   + e.g. symmetric, public key, secure hash, digital signing, block cipher etc.   + how they are applied and to what end and their limitations   + examples of badly applied or implemented cryptographic techniques * key management   + key features, benefits and limitations of symmetric and public key cryptosystems   + significance of entropy * the role of cryptographic techniques in a range of different systems   + e.g., GSM, chip and pin, hard disk encryption, TLS, SSL, privacy enforcing technology   + practical issues introducing such into service and updating them. | | | | | | | | |
| **Part 3: Assessment** | | | | | | | | |
| This module is assessed by a combination of techniques: Completion of a course workbook and a 30 inue presentation.  Component A:  Apprentices will complete a course workbook, based on short research tasks, which will require them to demonstrate their understanding of cryptographic techniques, their underpinning theory, their pros and cons, and how they are applied to protect systems.  Component B:  A 30 minute presentation where apprentices will show how they have chosen an appropriate algorithm and technique to solve a given requirement. They will demonstrate the solution and satisfactorily explain its operation to an audience without specialised expertise. | | | | | | | | |
|  | | | | | | | | |
| Identify final timetabled piece of assessment (component and element) | | | | | **B1** | | | |
| **% weighting between components A and B** (Standard modules only) | | | | | | | **A:** | **B**: |
| **50%** | **50%** |
|  | | | | | | | | |
| **First Sit** | | | | | | | | |
| **Component A** (controlled conditions)  **Description of each element** | | | | | | | **Element weighting**  **(as % of component)** | |
| 1. Coursework | | | | | | | 100% | |
| **Component B**  **Description of each element** | | | | | | | **Element weighting**  **(as % of component)** | |
| 1. Presentation | | | | | | | 100% | |
| **Resit (further attendance at taught classes is not required)** | | | | | | | | |
| **Component A** (controlled conditions) **Description of each element** | | | | | | | **Element weighting (as % of component)** | |
| 1. Presentation | | | | | | | 100% | |
| **Component B  Description of each element** | | | | | | | **Element weighting (as % of component)** | |
| 1. Coursework | | | | | | | 100% | |
|  | | | | | | | | |
| **Part 4: Learning Outcomes & KIS Data** | | | | | | | | |
| **Learning Outcomes** | On successful completion of this module students will be able to:   1. Implement and analyse algorithms (Component B) 2. Configure and use security technology components and key management (Component A and B) 3. Understand appropriate mathematical techniques relevant to practical computing scenarios (Component A) 4. Explain how hardware and cryptographic techniques are used to protect systems (Component A) 5. Explain complex cryptographic concepts to non-experts (Component B) | | | | | | | |
| **Key Information Sets Information (KIS)**  **Contact Hours**  **Total Assessment** | The table below indicates as a percentage the total assessment of the module which constitutes a;  **Written Exam**: Unseen or open book written exam  **Coursework**: Written assignment or essay, report, dissertation, portfolio, project or in class test  **Practical Exam**: Oral Assessment and/or presentation, practical skills assessment, practical exam (i.e. an exam determining mastery of a technique) | | | | | | | |
| **Reading List** | Reading list to be added | | | | | | | |

***FOR OFFICE USE ONLY***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **First Approval Date (and panel type)** | *Date of first {panel} approval* | | | |
| **Revision ASQC Approval Date**  *Update this row each time a change goes to ASQC* |  | **Version** | *1* | *Link to RIA* |
|  |  |  |
|  |  |  |
|  |  |  |