ROBERT GORDON UNIVERSITY ABERDEEN

## MODULE DESCRIPTOR

### Module Title

Computer Security and Cryptography

| | | | |
|---|---|---|---|
| Reference | CM3104 | Version | 3 |
| Created | October 2018 | SCQF Level | SCQF 9 |
| Approved | July 2016 | SCQF Points | 15 |
| Amended | November 2018 | ECTS Points | 7.5 |

### Aims of Module

To provide students with the knowledge and skills needed to understand the digital security landscape and the role of cryptography in securing computer-based information systems. This module will provide students with a good theoretical underpinning for assessing security requirements and preparing strategies to overcome threats.

### Learning Outcomes for Module

On completion of this module, students are expected to be able to:

| | |
|---|---|
| 1 | Demonstrate understanding of the information security requirements of commercial and public sector organisations and private individuals, and the threats posed to vulnerabilities in modern information systems. |
| 2 | Identify established principles of good information security and apply these to examples of information infrastructures. |
| 3 | Demonstrate understanding of the role of cryptography in providing security services for modern computer systems. |
| 4 | Implement appropriate security techniques to secure information and mitigate risk. |
| 5 | Demonstrate an awareness and ability to apply security standards as documented in professional codes of conduct of computing & IT professional bodies, e.g. BCS, ACM, ABET. |

### Indicative Module Content

Information Security: Digital threats, risks, forms of attack, categories and types of adversary, security needs, human factors. Information security governance and risk management. Security services: Confidentiality, Availability and Data Integrity. Authentication, Authorisation. Non-repudiation. Symmetric Cryptography. Block ciphers and Stream ciphers. Modern block cipher design. Substitution and Transposition. Confusion and Diffusion. Feistel ciphers, Advanced Encryption Standard. Public Key Cryptography. Asymmetric cryptography algorithms, e.g. RSA, El Gamal, Elliptic Curve cryptography. Key Exchange protocols: e.g. Diffie-Hellman. Hash Functions and Digital Signatures. Authentication systems: Symmetric and Asymmetric Protocols. Certificates and Public Key Infrastructures. Future developments in cryptology, e.g. advanced security protocols, quantum cryptography. Standards and Best Practice Guides: ISO 27001, ISO 27014, ISO 27036.

| Module Ref: | CM3104 v3 |
|---|---|

## Module Delivery

Key concepts are introduced and illustrated through lectures. The understanding of students is tested and further enhanced through tutorials and interactive labs. In the laboratories the students will progress through a sequence of exercises to develop sufficient knowledge of the subject.

| Indicative Student Workload | Full Time | Part Time |
|---|---|---|
| Contact Hours | 48 | N/A |
| Non-Contact Hours | 102 | N/A |
| Placement/Work-Based Learning Experience [Notional] Hours | N/A | N/A |
| TOTAL | 150 | N/A |
| *Actual Placement hours for professional, statutory or regulatory body* | | |

## ASSESSMENT PLAN

*If a major/minor model is used and box is ticked, % weightings below are indicative only.*

### Component 1

| Type: | Coursework | Weighting: | 100% | Outcomes Assessed: | 1, 2, 3, 4, 5 |
|---|---|---|---|---|---|
| Description: | Coursework assignment. | | | | |

## MODULE PERFORMANCE DESCRIPTOR

### Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the module.

| Module Grade | Minimum Requirements to achieve Module Grade: |
|---|---|
| **A** | The student needs to achieve an A in C1. |
| **B** | The student needs to achieve a B in C1. |
| **C** | The student needs to achieve a C in C1. |
| **D** | The student needs to achieve a D in C1. |
| **E** | The student needs to achieve an E in C1. |
| **F** | The student needs to achieve an F in C1. |
| **NS** | Non-submission of work by published deadline or non-attendance for examination |

## Module Requirements

| | |
|---|---|
| Prerequisites for Module | None. |
| Corequisites for module | None. |
| Precluded Modules | None. |

## INDICATIVE BIBLIOGRAPHY


| | |
|---|---|
| 1 | PFLEEGER, C., PFLEEGER, S.L. and MARGULIES, J., 2015. Security in Computing. 5th ed. Prentice Hall. |
| 2 | STALLINGS, W. and BROWN, L., 2014. Computer Security: Principles and Practice. 3rd ed. Pearson. |
| 3 | STALLINGS, W., 2016. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson. |
| 4 | GOLMAN, D., 2011. Computer Security. 3rd ed. Wiley. |
| 5 | FERGUSON, N., 2010. Cryptography Engineering: Design Principles and Practical Applications. Wiley. |
| 6 | ANDERSON, R., 2008. Security Engineering: A Guide to Building Dependable Systems. 2nd ed. Wiley. |
| 7 | MARTIN, K.M., 2012. Everyday Cryptography: Fundamental Principles and Applications. Oxford University Press. |
| 8 | BOSWORTH, S., KABAY, M., and WHYNE, E., 2014. Computer Security Handbook. 6th ed. Wiley. |