MODULE SPECIFICATION

Name of Module		Introduction to Cyber Security					
Parent School/Dept		Computer Science					
Programme(s) where module is offered		BSc Computer Science with Electrical Engineering; BSc Computer Science with Economics; BSc Computer Science with Business; BSc Computer Science with International Relations; BSc Computer Science with Political Science;					
Status (core, option, free choice)		Core		**Pre-Requisite Modules or Qualifications**		Mathematics, Programming and Problem Solving	
FHEQ Level	6	**Unit Value**	6 ECTS	**Module Code**	CS385	**Module coordinator**	Suncica Hadzidedic
Semester taught		Fall		**Applicable From**		2019	

Educational Aims of the Module

Rapid advances in technology have positive effects on modern life, but also bring drawbacks. Every new technology reintroduces the question of whether security provided for the previous technology is applicable to the new one. Security as an inevitable integral part of today's information systems became even more so with the expansion and popularization of the Internet. The Internet, as a tool which brought unexpected and advanced ways of human communication and interaction, forced the consideration of security requirements of security-unaware and predominantly security-inexperienced users. In other words, dealing with the Fundamental Dilemma of Security.

Therefore, the aim of the course is to define what cyber security is (encompassing information, computer and network security), and point out the objectives of this area. In addition, it is to equip students with analytical skills to identify security threats and vulnerabilities in a system, to provide with problem solving skills to create security policies and recovery plans, and as well as practical skills to implement security plans and policies, and to use cryptographic algorithms and protocols and security applications and standards. Thus, the aims are:

1. Studying information, network and application security.
2. Demonstrating and applying the working of various private and public key ciphers, as well as cryptographic protocols.
3. Surveying security tools and applications; including e-mail security, IP security, biometrics.
4. Understanding a broad range of issues related to security management.
5. Discussing up-to-date cyber security issues.

Module Outline/Syllabus

The module is organized around the following topics:

- **Introduction:** Definition of IS security, Why security?, Main objectives and services, Security application and techniques
- **Security threats**: Attacks and threats
- **Security risks and vulnerabilities**: Vulnerabilities, Risk assessment
- **Countermeasures / Protection Mechanisms**: Security management
  - **Classical cryptography:** Substitution and transposition ciphers, Rotor machines, Cryptanalysis of classical ciphers (frequency calculation and index of coincidence)
  - **Modern cryptography:** Classification of modern ciphers (private-key and public-key cipher characteristics), Conventional ciphers, Block ciphers (Feistel, DES, AES), Stream ciphers (LFSR), Modes of operation
  - **Public-key cryptography:** Elements of modular arithmetic, RSA cipher, El-Gamal
  - **Cryptographic protocols**: Key management and distribution protocols for symmetric and public-key ciphers, Diffie Hellman, Hash functions, Digital signature, Digital certificates and PKI
  - **Network security**: Introduction to networks, Firewalls, Tools for e-mail security – PGP and S/MIME, Tools for Internet security – SSL/TLS
- **Selected security technologies and topics**
  - IPSec, Authentication systems – Kerberos
  - Biometrics and steganography
  - Security in the cloud
  - Botnets (how to stop them)

Assignments/practical exercises:

- Programming – cryptanalysis; AES

- Peer-reviewed
  - critical analysis of a video on cyber security topic
  - critical analysis of a cyber security scientific article
  - present an assigned cyber security topic
  - quizzes based on lecture topics
- Project
  - *Fraud/theft detection: Behavior analysis (dataset)*
  - *Malware detection (dataset)*
  - *Internet security – secure online service*
  - *Audit: Risk assessment + security policy development*

Student Engagement Hours			
Type	**Number per Term**	**Duration**	**Total Time**
Lectures	30	2 hours	60 hours
Practical/lab sessions	15	2 hours	30 hours
		Total Contact Hours	**90**
		Total Guided/Independent Learning Hours	**60**
		Total Engagement Hours	**150**

Assessment Method Summary				
Type	**Number Required**	**Duration / Length**	**Weighting**	**Timing/Submission Deadline**
Project (Group)	1	3,000 words	15%	End of semester
Assignments (peer-reviewed)	3	500 words; 5-10 minutes	10%	Week 4, Week 8, Week 12
Participation	30	N/A	5%	Every week – 1 lecture, 1 lab
Mid-term exam	1	90 minutes	20%	Week 9
Final Exam	1	180 minutes	50%	End of semester

Module Outcomes

Intended Learning Outcomes:

By the end of the course students will be able to:

1. Understand the technical and social nature of IS Security.
2. Demonstrate the knowledge of key security objectives – CIA - and mechanism to achieve the same.
3. Show the ability to use historic ciphers and simplified versions of private-key and public-key ciphers, and understand their drawbacks.
4. Gain in-depth knowledge of cryptographic protocols, security infrastructure and security tools.
5. Acquire knowledge in the latest cyber security issues and current approaches to preventing/detecting/resolving these.

→

Teaching and Learning Strategy:

1. Project (ILO: 1-5)
2. Lectures (ILO:1-5)
3. Laboratory – practical applications (ILO: 1-5)
4. Attendance and Participation (ILO: 1-5)
5. Independent study (ILO: 1-5)
6. Mid-term Exam (ILO: 1-5)
7. Final Exam (ILO: 1-5)

→

Assessment Strategy

1. Project (ILO:1-5)
2. Assignments (Research and practical) (ILO:1-5)
3. Participation (lab and class discussions) (ILO:1-5)
4. Mid-term exam (ILO: 1-3)
5. Final exam (ILO: 1-5)

Practical Skills

1. Mathematical calculations in cryptography
2. Programming assignments for private key ciphers, security algorithms and web security.
3. Use of security tools, e.g.: CrypTool, Weka, password cracker, port-scanner, packet-sniffer, memory space recovery
4. Developing security plans and policies
5. Performing risk assessment

→

Teaching and Learning Strategy:

1. Project (PS: 2-5)
2. Lectures (PS:1,4,5)
8. Laboratory – practical applications (PS: 1-5)
3. Attendance and Participation (PS: 1-5)
4. Independent study (PS: 1-5)
5. Mid-term Exam (PS: 1,4,5)
6. Final Exam (PS: 1,4,5)

→

Assessment Strategy

1. Project (PS:2-5)
2. Assignments (Research and practical) (PS:1-

<table>
<tr><td></td><td></td><td>5)
3. Participation (lab and class discussions) (PS:1-5)
4. Mid-term exam (PS: 1,4,5)
5. Final exam (PS: 1,4,5)</td></tr>
<tr><td rowspan="2"><u>Transferable Skills</u>

1. Entrepreneurship - Entrepreneurial approach to solving cyber security issues
2. Integration of different pieces of knowledge into one capstone project
3. Critical analysis and evaluation of articles and scientific work (in the area of cyber security)
4. Expressing technical ideas in a natural language – writing reports
5. Developing into a lifelong learner</td><td>⟶</td><td><u>Teaching and Learning Strategy:</u>

1. Project (TS: 1-5)
2. Lectures (TS:1,3,4,5)
9. Laboratory – practical applications (TS: 2-5)
3. Attendance and Participation (TS: 1-5)
4. Independent study (TS: 1-5)
5. Mid-term Exam (TS: 3,4)
6. Final Exam (TS: 3,4)</td></tr>
<tr><td>⟶</td><td><u>Assessment Strategy</u>

1. Project (TS: 1-5)
2. Assignments (Research and practical) (TS: 1-5)
3. Participation (lab and class discussions) (TS: 1-5)
4. Mid-term exam (TS: 3,4)
5. Final exam (TS: 3,4)</td></tr>
</table>

Key Texts and/or other learning materials

Set Texts:

- Amoroso, Edward G., and Matthew E. Amoroso. *From CIA to APT: An Introduction to Cyber Security*. Independently published, 2017.
- Stallings W., Cryptography and Network Security: Principles and Practice, Fifth Edition, Prentice Hall 2011, ISBN 0136097049

Supplementary Reading:

- Boyle R. and Panko R., Corporate Computer Security, Third Edition, Prentice Hall 2013, ISBN 0132599023
- Stallings W., Network Security Essentials: Applications and Standards, Fourth Edition, Prentice Hall 2010, ISBN 0136108059
- Stallings W., Brown, Computer Security – Principles and Practice, Second Edition, Pearson International, ISBN 0135137116
- Schneier B., Applied Cryptography: Protocols, algorithms and source code in C, Second Edition, John Wiley & Sons, Inc., 1996, ISBN 0471128457

Please note: This specification provides a concise summary of the main features of the module and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the learning opportunities that are provided. More detailed information on the learning outcomes, content and teaching, learning and assessment methods of each module and programme can be found in the departmental or programme handbook. The accuracy of the information contained in this document is reviewed annually by the University of Buckingham and may be checked by the Quality Assurance Agency.

Date of Production	Spring 2019
Date approved by School Learning and Teaching Committee	
Date approved by School Board of Study	
Date approved by University Learning and Teaching Committee	
Date of Annual Review	