2024 / 25

School of Science and Computing

☎ +353 (0)51 302037

✉ Eleanor.Reade@setu.ie

www.wit.ie/schools/science_computing

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Module Descriptor

Data Security
(Computing and Mathematics)

Data Security (A36201)

Short Title: Data Security
Department: Computing and Mathematics
Credits: 5 **Level:** Advanced

Description of Module / Aims

This module provides the essentials of data security. Topics covered include relevant security threats and vulnerabilities and the services available to address these threats. Cryptographic foundations that underpin many security mechanisms are covered. Network security is covered in the context of ensuring secure access to data in motion. Security-enabled frameworks like Distributed Ledger Technology (also known as blockchain) and privacy preserving techniques are highlighted.

Programmes

	stage/semester/status
HDip in Science in Data Analytics (WD_KDAAN_G)	1 / 2 / M

Indicative Content

- Introduction to computer security: security threats; attack methods; common vulnerabilities; security services
- Cryptography: symmetric encryption; modern encryption; block vs stream ciphers; public key cryptography
- Message authentication and integrity: hash functions; collisions; MACs; digital signatures; digital certificates
- Computer system security: Access controls, TLS/SSL, SSH, firewalls
- Distributed Ledger Technology, trust and managing consensus using cryptography
- Privacy and data governance when storing and working with data

Learning Outcomes

On successful completion of this module, a student will be able to:

1. Assess the various security threats and attack methods to which data may be susceptible.
2. Appraise the role of cryptography in computer and data security, including its benefits and limitations.
3. Test and use cryptographic software and set up secure systems for managing data.
4. Evaluate the benefits of distributed ledgers (including blockchain), including their transparency, resistance to tampering, and decentralised nature.
5. Appraise the role of privacy protection when collecting, storing and performing operations on personal data.

Learning and Teaching Methods

- This module will be presented by a combination of lectures and practicals.
- The lectures will be used to introduce new topics and their related concepts.
- The practical element allows the student to put into practice the theoretical concepts covered in the lectures.

Learning Modes

Learning Type	F/T Hours	P/T Hours
Lecture	24	24
Practical	24	24
Independent Learning	87	87

Assessment Methods

	Weighting		Outcomes Assessed
Continuous Assessment	100%		
In-Class Assessment		50%	1,2,3
Assignment		50%	1,4,5

Assessment Criteria

<40%: Unable to describe key data security technologies. Unable to distinguish between different types of data security threat or to present instances of them in a clear manner. Unable to effectively use relevant tools.

40%–49%: Can describe in detail key security threats and technologies. Can carry out basic configuration of technologies to implement security policies and to store data in a distributed manner. Able to present instances of data security weaknesses and to assess the privacy implications of a basic system.

50%–59%: In addition to the above, can reason about the various approaches to security and their benefits and limitations. Able to explain in context and present instances of privacy threats and how they might be realised. Able to model data in a software system with multiple usage scenarios and security requirements, including those drawn from the Confidentiality, Integrity, Availability (CIA) triad.

60%–69%: In addition, can explain basis of a variety of cryptographic schemes. Can competently make use of security and privacy procedures, tools and technologies in the context of the intended use of data. Able to present and explain why data privacy in analytical settings is difficult to achieve.

70%–100%: All of the above to an excellent level. Can demonstrate an understanding of some the trade-offs involved in providing security, trust and privacy. Able to demonstrate in detail how to protect data, its subjects and its users.

Essential Material(s)

- "General Data Protection Regulation." https://gdpr-info.eu/
- "OpenSSL Cryptography and SSL/TLS Toolkit." https://www.openssl.org/
- "The Keys to Data Protection - A Guide for Policy Engagement on Data Protection." https://privacyinternational.org/si
09/Data%20Protection%20COMPLETE.pdf

Supplementary Material(s)

- "SANS Cyber Security Resources." https://www.sans.org/security-resources/?msc=main-nav
- "The CERT Division at SEI, CMU." https://www.sei.cmu.edu/about/divisions/cert/index.cfm
- Bashir, Imran. *Mastering Blockchain.* 4th ed.. Birmingham, UK: Packt Publishers, 2023.
- Bharajia, N. *Data Privacy: A runbook for engineers.* New York: Manning Publications, 2022.
- Morris Chang, J., D. Zhuang and G. Dumindu Samaraweera. *Privacy-Preserving Machine Learning.* New York: Manning Publications, 2023.
- Stallings, W. and L. Brown. *Computer Security: Principles and Practices.* 4th ed.. London: Pearson, 2017.

Requested Resources

- Computer Lab: BYOD Lab