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

Applied Cryptography (Computing and Mathematics)

Applied Cryptography (A13542)

Short Title: Applied Cryptography
Department: Computing and Mathematics
Credits: 5 **Level:** Introductory

Description of Module / Aims

This module provides students with a detailed introduction to cryptography, including both the fundamentals and leading techniques as applied to the security of systems, applications and communications.

Programmes

		stage/semester/status
COMP-0451	BSc (Hons) in Applied Computing (International) (WD_KACCM_BI)	2 / 4 / M
COMP-0451	BSc (Hons) in Applied Computing (WD_KACCM_B)	2 / 4 / M
COMP-0451	BSc (Hons) in Applied Computing (WD_KCOMP_B)	2 / 4 / M
COMP-0451	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	2 / 4 / M
COMP-0451	BSc (Hons) in Computer Science (WD_KCMSC_B)	2 / 4 / M
COMP-0451	BSc (Hons) in the Internet of Things (International) (WD_KINTT_BI)	2 / 4 / M

Indicative Content

- Security context: threats & attacks; security standards, services & mechanisms
- Introduction to cryptography: terminology; block and stream ciphers; cryptanalysis; limitations of cryptography
- Symmetric encryption: classical schemes; modern algorithms; deployment modes
- Random numbers: entropy concept; pseudo random generation
- Public-key cryptography: number theory background; requirements; techniques – RSA, Diffie-Hellmann, elliptic curve cryptography; performance issues
- Authentication functions: principles; hash functions; collisions; MACs, digital signatures
- Key management: symmetric key distribution protocols; public key authentication; digital certificates & PKIs; trust models
- Practical applications & deployment issues: placement of encryption function; key storage; application case studies

Learning Outcomes

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

1. Recognise the role (and limitations) of cryptography in securing systems, communications, and applications.
2. Describe leading cryptographic models and algorithms (symmetric ciphers, public-key schemes and hash functions) and explain their mathematical basis in outline terms.
3. Recognise the significance of random numbers in the context of cryptography.
4. Compare the computational performance of leading cryptographic algorithms.
5. Discuss the storage, exchange and management of keys in both symmetric and public-key systems.
6. Describe a selection of practical applications of cryptography.
7. Make effective use of a cryptographic software application or library.

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	
Practical	24	
Independent Learning	87	

Assessment Methods

	Weighting	Outcomes Assessed
Final Written Examination	50%	1,2,3,5,6
Continuous Assessment	50%	
Practical	50%	4,5,6,7

Assessment Criteria

<40%: Unable to describe and compare major cryptographic models and algorithms. Poor understanding of role of cryptography in computer security. Poor understanding of mathematical foundations.

40%–49%: Can describe and compare the main cryptographic models and algorithms. Can provide overview of main steps of leading encryption and authentication algorithms. Can carry out analysis of key strength.

50%–59%: In addition to the above, can describe in detail the leading encryption and authentication algorithms, as well as their mathematical basis. Can demonstrate the significance of key length and an understanding of attack scenarios.

60%–69%: In addition, provide worked examples of encryption algorithms and solve encryption problems (using small numbers). Can derive and explain basis of several cryptographic schemes.

70%–100%: All of the above to an excellent level. Can analyse complexity and performance of relevant algorithms.

Essential Material(s)

- "GNU Privacy Guard." https://www.gnupg.org/
- "The OpenSSL project." https://www.openssl.org/

Supplementary Material(s)

- Ferguson, N., B. Schneier and T. Kohno. *Cryptography Engineering*. Indianapolis: Wiley, 2010.
- Gollmann, D. *Computer Security*. 3rd ed. Chichester: Wiley, 2011.
- Stallings, W. *Computer Security: Principles and Practice*. 3rd ed. Harlow: Pearson, 2014.
- Stallings, W. *Cryptography and Network Security*. 6th ed. Boston: Pearson, 2014.

Requested Resources

- Computer Lab: BYOD Lab