WM280-15 Cryptosystems

27/28

Department
WMG
Level
Undergraduate Level 2
Module leader
Sandy Taramonli
Credit value
15
Module duration
10 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Secure systems aim to create a trusted environment that protects sensitive data, maintains system functionality, and mitigates risks associated with unauthorized access, data breaches, and other security threats. The goal of a secure system is twofold: to ensure the protection and integrity of information and resources by enabling authorized and desired actions while preventing unauthorized access, malicious activities, and undesirable incidents. However, achieving this goal poses significant challenges. These challenges include defining which events are acceptable and which are not, predicting future possibilities, and determining the system's boundaries. Notwithstanding these challenges, there exist established approaches to constructing secure systems that provide robust protection and maintain system functionality while minimising the occurrence of unwanted incidents. Cryptography plays a crucial role in achieving these goals. It is an essential tool that allows us to protect information and ensure confidentiality, integrity, and authentication. It provides mechanisms to protect sensitive information, verify the identity of users and devices, and enable secure communication over unsecured networks. Cryptographic techniques, such as symmetric-key and public-key cryptography, are used in various contexts including secure messaging, online transaction protection, and virtual private networks (VPNs). This module introduces concepts of cryptography and explores how they are practically applied to ensure strong security measures in secure systems.

Module aims

This module serves as a fundamental component within the broader subject, offering students the opportunity to deepen their knowledge and skills in the field of cybersecurity. By engaging with this module, students will develop the ability to design robust security architectures tailored to specific scenarios. Moreover, students will acquire practical expertise in configuring systems using cryptographic techniques to achieve the desired security objectives. By actively participating in this module, students will enhance their overall understanding of trust and security, equipping them with the necessary tools to thrive in the dynamic landscape of cyber security.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Outline content
The content of this module will be taught from a cyber security perspective.

Symmetric Key Cryptography:

- Block ciphers (e.g., Data Encryption Standard, Advanced Encryption Standard)
- Stream ciphers (e.g., Rivest Cipher 4)
- Modes of operation (e.g., Electronic Codebook, Cipher Block Chaining, Counter Mode)
- Key management and distribution
- Message authentication codes
- Key derivation functions

Public-Key Cryptography:

- RSA algorithm
- Diffie-Hellman key exchange
- Elliptic Curve Cryptography
- Digital signatures (e.g., Rivest Shamir Adleman, Digital Signature Algorithm)
- Key exchange protocols (e.g., Secure Socket Layer/Transport Layer Security, Secure Shell)

Hash Functions and Message Digests:

- Cryptographic hash functions (e.g., Secure Hash Algorithm-256, Message Digest Algorithm)
- Applications of hash functions (e.g., password storage, data integrity)
- Message Digest algorithms (e.g., Hash Based Message Authentication Code)

Cryptographic Protocols and Applications:

- Secure communication protocols (e.g., Secure Socket Layer/Transport Layer Security, Internet Protocol Security)
- Secure email (e.g., Pretty Good Privacy)
- Virtual Private Networks
- Secure File Transfer (e.g., Secure Shell, Secure Copy Protocol)

Cryptographic Attacks and Countermeasures:

- Cryptanalysis techniques, Side-channel attacks etc.

- Key management and secure key storage
- Random number generation
- Cryptographic standards and certifications

Applied Cryptography in Real-World Systems:

- Encryption in storage systems
- Access control
- Blockchain technology
- Privacy-enhancing technologies (e.g., homomorphic encryption)

Cryptographic Tools:

- Introduction to cryptographic libraries (e.g., OpenSSL)
- Practical implementation of cryptographic algorithms

Legal and Ethical Aspects:

- Cryptography policies and regulations
- Ethical considerations in cryptography
- Cryptography and privacy laws

Design and development of cryptosystems

The future of cryptography

Learning outcomes

By the end of the module, students should be able to:

- Design a security architecture that satisfies the security needs of a given scenario. [CITP: 2.1.1, 2.1.2, 2.1.8, 2.1.10, C13]
- Configure systems, applying cryptographic techniques as needed, to achieve desired security objectives. [CITP: 2.1.10, C12, C13]
- Develop secure cryptosystems by effectively utilising programming languages and cryptographic tools to implement cryptographic operations. [CITP: 2.1.8, C12, C13]
- Analyse the suitability of cryptographic algorithms to meet specific security requirements, evaluating their security properties, strengths, and limitations. [CITP: 2.1.11, 2.2.2, C13]

Indicative reading list

Reading lists can be found in Talis

Specific reading list for the module

Interdisciplinary

Cryptography is an inherently interdisciplinary subject. It combines ideas from mathematics and

computer science together with social studies on the usability of secure systems, and these will be demonstrated throughout the module.

Subject specific skills

This module enables students to develop an understanding of the fundamentals of cryptography, knowledge of cryptographic algorithms and when to use them, as well as an ability to use cryptography to build secure systems.

Transferable skills

Critical thinking, problem solving, written communication, and presentation skills

---

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	44 hours (29%)
Assessment	66 hours (44%)
Total	150 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Assessment component			
Closed book test	30%	24 hours	No
The test will assess the ability to analyse and evaluate cryptographic algorithms, using different question formats, including multiple choice questions, short answer questions, or case study questions, or any combination of these question types.			
Reassessment component is the same			
Assessment component			
Coursework	70%	42 hours	Yes (extension)
Students are given a scenario (which varies from year to year) and are required to design a cryptosystem, implement it and write a report to present the proposed system.			
Reassessment component			
Coursework			No
Students are given a scenario (which varies from year to year) and are required to design a cryptosystem, implement it and write a report to present the proposed system.			

Feedback on assessment

Feedback will be provided via Tabula using standard WMG feedback mechanisms.

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security