WM9C5-15 Management of Cryptosystems

23/24

Department
WMG
Level
Taught Postgraduate Level
Module leader
Henry Caushi
Credit value
15
Module duration
2 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Cryptography is an essential tool in modern cyber security. It allows us to protect sensitive information, authenticate users and devices, and enable secure communication over insecure networks. Cryptographic techniques are used in a wide range of contexts, including secure messaging, protecting online transactions, and virtual private networks (VPNs). This module provides an introduction to the fundamental concepts of symmetric-key and public-key cryptography, and their practical applications.

Module aims

This module introduces students to the fundamental concepts of cryptography and its role in cyber security. By the end of the module, students should be able to differentiate between symmetric-key and public-key cryptography, recognise examples of each and understand their advantages and disadvantages in different use cases. Additionally, students will learn how to design and manage secure cryptosystems for different applications. Important cryptographic protocols such as TLS, PGP and the Signal Protocol are analysed in detail in order to establish their strengths, weaknesses, and where they require human trust. Most importantly, participants are presented with a critical understanding of how and when a given protocol should (and should not) be used in

a system design scenario.

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.

Introduction to cryptography:

- Why do we need cryptography?
- Historical encryption schemes

Symmetric-key encryption:

- Block ciphers: DES, 3DES, AES
- Stream ciphers and block cipher modes of operation
- Constructions: Feistel structures and substitution-permutation (SP) networks
- Entropy and key length
- The key exchange problem

Public-key encryption:

- RSA and elliptic-curve cryptography
- Hybrid-key encryption
- Public-key infrastructure (PKI) and key authentication

Hash algorithms:

- Properties: Irreversible, deterministic, collision resistance, length
- Algorithms: MD5, SHA
- Applications: Authentication, known good/bad files, file integrity
- Known weaknesses: Attacks including brute force, rainbow tables and length extension attacks

Message authentication:

- Message authentication codes (MACs)
- Digital signatures

Important protocols:

- TLS and X509 certificates
- PGP

The future of cryptography:

- Overview of blockchains and cryptocurrencies
- Introduction to post-quantum cryptography

Learning outcomes

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

- Be familiar with commonly used cryptographic primitives and protocols
- Critically evaluate the properties of different cryptographic algorithms
- Be able to design secure cryptosystems that meet different application requirements
- Evaluate the use of different cryptographic techniques used to build cryptosystems

Indicative reading list

Wong, D., 2021. Real-World Cryptography. Manning Publications.
Schneier, B., Kohno, T. and Ferguson, N., 2013. Cryptography engineering: design principles and practical applications. Wiley.
Anderson, R., 2021. Security Engineering. John Wiley & Sons.

View reading list on Talis Aspire

Interdisciplinary

Cryptography is an inherently interdisciplinary subject. It combines ideas from mathematics, electronics 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 course 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 skills, and the ability to independently build large, secure systems

---

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	60 sessions of 1 hour (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time	Eligible for self-certification
In class test	20%	12 hours	No
There will be a 20% in-class test held during the last lecture.			
Application of cryptography in a scenario	80%	48 hours	Yes (extension)
Students are given a scenario (which varies from year to year) and are required to build a cryptosystem that solves that scenario, together with an evaluation of the features of their system. Their findings will be assessed via the configuration proposed, an accompanying 2500-page report, and a video demonstration of the proposal.			

Assessment group R

	Weighting	Study time	Eligible for self-certification
Application of cryptography in a scenario	100%		Yes (extension)
Students are given a scenario (which varies from year to year) and are required to build a cryptosystem that solves that scenario, together with an evaluation of the features of their system. Their findings will be assessed via the configuration proposed, an accompanying 2500-page report, and a video demonstration of the proposal.			

Feedback on assessment

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

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- ES94N-10 Crypto-systems & Data Protection
- ES94N-15 Crypto-systems & Data Protection

Courses

This module is Core for:

- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)