WM9C5-15 Management of Cryptosystems

21/22

Department
WMG
Level
Taught Postgraduate Level
Module leader
Harjinder Lallie
Credit value
15
Module duration
2 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Singapore Institute of Management, Singapore

Description

Introductory description

Modern cyber systems use cryptography to protect various properties of data (confidentiality, integrity, authenticity etc) when it is stored on or moving between computer systems. Examples include the encryption of data at rest on mass storage devices such as disc drives or USB removable drives; protection of data in transit between a user's web browser and the web server where they are engaged in some sort of financial transaction; authentication protocols to assure one part of a system as to the identity of another part of the system with which is interacting; and the underlying properties that give cryptocurrencies their perceived value.

Module aims

This module equips participants with critical insight into the application of cryptography in a range of practical scenarios. There is an emphasis on how cyber security consultants position cryptosystems in system designs. The focus is on understanding the resulting properties of sophisticated cryptographic protocols, algorithms and configurations, rather than on analysis of the deep mathematics within. The module analyses standard cryptographic patterns that may be applied to achieve particular patterns of protection in typical scenarios.

Practical exercises are used to demonstrate cryptographic principles. Participants engage with cryptographic hashes to understand their strengths and weaknesses concerning data integrity. Participants are provided a detailed understanding of different attacks (brute force, dictionary, rainbow tables, synthetic collisions) and mitigations (salting, stretching, large keyspace). Participants are exposed to symmetric and public key encryption. Particular attention is paid to the use of hybrid systems to address the key exchange problem in a computationally efficient manner, securing confidentiality over time and in transit. This is developed to show how a public key infrastructure also offers assurance through digital signatures. The challenge of having the relevant key available for authorised use, yet unavailable for unauthorised use is a common theme.
Important cryptographic protocols – such as X509 PKI (Public Key Infrastructure), IPSec (Internet Protocol Security), TLS (Transport Layer Security), SSH (Secure SHell) – are analysed in detail in order to establish where that most human requirement, trust, is located. Most importantly, participants are presented with a critical understanding of how and when a given protocol should (not) be used in a system design scenario.
Cryptosystems are pivotal to various blockchain technologies including cryptocurrencies. The module explores the role of cryptography in these technologies and equips participants with a detailed working knowledge of these applications.

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.

- Cryptographic hashes. Understand terminology: hash, digest, message authentication code, function. Hash properties: irreversible, deterministic, collision resistance, length. Application: authentication, known good / bad files, file integrity. Cryptographic attacks: brute force, rainbow tables, password salting / stretching, collisions. Hash algorithms: MD5, SHA, and others.
- Encryption theory. Terminology: plaintext, ciphertext, key, algorithm, protocol. Concepts: entropy, one-time pad, complexity, initialisation vectors.
- Symmetric encryption. Encryption over distance or time – the key exchange problem. Example algorithms – DES, Triple DES, AES.
- Asymmetric encryption. Properties: encrypting for known recipient, signing by authentic sender. Establishing trust: certificate authenticity, hierarchy (X509) and web (OpenPGP), certificates. Consequences of loss of key control – revocation certificates.
- Hybrid encryption. Using asymmetric encryption to share symmetric key. SSL/TLS
- Other specific protocols. Kerberos, IPSEC
- Data protection. At rest, in transit
- Blockchain and Virtual currencies. Distributed consensus, peer-to-peer network, the ‘51% attack’, immutability, apparent anonymity. Virtual currencies: bitcoin Ethereum, wallets, transactions, smart contracts, anonymity and privacy in the Bitcoin ecosystem.

Learning outcomes

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

- Critically analyse the properties of cryptographic hashes.
- Evaluate competing cryptographic techniques in the solution of well defined cyber problems.
- Critically analyse the properties of symmetric encryption
- Critically analyse the properties of cryptographic key management systems.
- Critically analyse the properties of asymmetric (public key) encryption
- Critically analyse the properties of digital signatures.
- Critically analyse the properties of cryptographic protocols.

Indicative reading list

Reading lists can be found in Talis

Specific reading list for the module

Research element

The module content draws upon and highlights research within the domain. Module assessment typically requires participants to perform further research in order to prepare an appropriate response to the assessment task.

Interdisciplinary

Although the module is largely dedicated towards the development of discipline-specific technical, professional and analytical skills, these are necessarily interdisciplinary in nature ranging from abstract mathematics to human trust.

International

The module is designed for an international cohort. Learning materials and examples will be drawn from a range of disciplines and cultures.

Subject specific skills

Equip student to configure cryptosystems to achieved desired properties.

Transferable skills

Critical thinking, problem solving.

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Tutorials	12 sessions of 1 hour (8%)
Practical classes	15 sessions of 1 hour (10%)
Online learning (independent)	30 sessions of 1 hour (20%)
Assessment	83 hours (55%)
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 must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Assessment component			
Application of Cryptpography in a Scenario	100%	83 hours	Yes (extension)

The specific scenario and the related cryptographic activity will vary from year to year. Typically, the task will require the practical configuration of some cryptographic components and an analysis of the properties of a related cryptosystem. Word count and similar constraints on scale will be specified in the assignment.

Reassessment component is the same

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:

- Cyber Security Management (New Degree)