CYM040 Applied Cryptography

Module description

Cryptography provides the core toolkit that underpins most digital security technologies. An understanding of what cryptography does, and its limitations, is critical to developing a wider appreciation of the security of everyday digital applications. Since cryptography provides tools for atomic security services such as confidentiality and data integrity, an appreciation of cryptography also equips you with a fundamental understanding of what security means in cyberspace. Note that this module adopts a non-mathematical approach to cryptography, very much considering it from the perspective of what any good cyber security professional needs to know and avoiding unnecessary technical details.

Module goals and outcomes

In this module you will explore the role of cryptography in supporting digital security for everyday applications such as the internet, mobile phones, wireless networks and cryptocurrency. You will develop an understanding of the functionality and purpose of the main cryptographic tools we use today. You will learn how to make decisions about which cryptographic tools are most appropriate to deploy in specific settings. You will also explore the wider infrastructure surrounding cryptography and how this impacts the overall security of systems deploying cryptography.

Upon successful completion of this module, you will be able to:

1. Explain the precise role that cryptography plays in the security of any digital system.

2. Identify and compare a range of cryptographic mechanisms that can be used to provide core security services such as confidentiality, data integrity, data origin authentication, non-repudiation and entity authentication.

3. Assess the points of vulnerability relating to cryptography in any digital system deploying it.

4. Critically analyze the selection and use of specific cryptographic techniques in digital applications such as mobile call protection, secure web browsing and cryptocurrencies.

5. Develop an informed opinion about how to address challenges arising from societal use of cryptography.

6. Rationalize future developments concerning cryptography and their likely impact on security of digital systems.

Textbook and Readings

The learning content is drawn from the key text
Keith M. Martin, Everyday Cryptography 2nd Ed., Oxford University Press, 2017

Other pieces of reading are available on the web:

- Post-Quantum Cryptography PQC
- C. Ellison and B. Schneier (2000). Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. Computer Security Journal, v 16, n 1, 2000
- Dale Walker (9th June 2020). EU inches closer to ban on end-to-end encryption.

Module outline

The module consists of ten weeks that focus on key areas of the applied cryptography.

Week 1. The Cryptographic Toolkit	**Key concepts:** Cryptography and the core security services it provides. **Learning outcomes:** • Justify the need for cryptography. • Define several fundamental security services that cryptography provides and explain how these-interrelate. • Identify cryptographic primitives associated with each security service. • Compare the different security service requirements of several applications of cryptography

Week 2. Cryptosystems	**Key concepts:** Main components of a cryptosystem and consideration how a cryptosystem could be broken. **Learning outcomes:** • Describe a basic model for a cryptosystem. • Explain the crucial roles in a cryptosystem played by algorithms and keys. • Compare symmetric and public-key cryptosystems, inferring implications about their different uses. • Justify standard assumptions about what an attacker knows about a cryptosystem. • Categorize different layers of a cryptosystem that an attacker could exploit and identify some attack techniques.
Week 3. Symmetric Encryption	**Key concepts:** Stream and block ciphers, and how to use them. **Learning outcomes:** • Explain the differences between stream and block ciphers, and differentiate their use. • Identify a number of different stream and block ciphers, and applications using them. • Compare the historical context behind the development of DES and AES, and how this influenced their properties and their standardization processes. • Justify the need for modes of operation of a block cipher • Select an appropriate mode of operation for a block cipher application.
Week 4. Public-key Encryption	**Key concepts:** The principles behind public-key encryption and the most common algorithms and their use.

	Learning outcomes: • Describe the basic principles behind public-key encryption. • Compare the basic properties and security of RSA and elliptic-curve-based public-key encryption. • Identify the main costs associated with public-key encryption, and how these influence its use. • Explain how public-key encryption is deployed in practice. • Anticipate likely future developments in public-key encryption.
Week 5. Data Integrity Mechanisms	**Key concepts:** A range of different cryptographic mechanisms supporting data integrity. **Learning outcomes:** • Compare different cryptographic primitives providing data integrity. • Describe the basic properties of hash functions, MACs, authenticated encryption primitives and digital signature schemes. • Explain the close relationship between data integrity mechanisms and those used for encryption. • Identify a range of cryptographic algorithms supporting data integrity, and applications using them. • Select an appropriate data integrity mechanism for an application of cryptography
Week 6. Entity Authentication Techniques	**Key concepts:** Different ways in which cryptography is used to support entity authentication. **Learning outcomes:** • Compare different mechanisms for randomly generating values. • Compare different techniques of providing freshness.

	• Identify the role cryptography plays in protecting, and improving upon, static passwords. • Explain why, and how, entity authentication is commonly provided alongside key establishment. • Describe Diffie-Hellman key agreement and compare it to related techniques
Week 7. Key Management	**Key concepts:** The different phases in the key management lifecycle, and how to implement them. **Learning outcomes:** • Identify some fundamental principles of key management • Explain the main phases in the lifecycle of a cryptographic key. • Compare different techniques for implementing the different phases in the key lifecycle. • Select appropriate key management techniques for specific application environments.
Topic 8. Public-key Management	**Key concepts:** Issues relating to public-key management, focusing on the use of certificates. **Learning outcomes:** • Compare the challenges associated with key management of symmetric, asymmetric private, and asymmetric public keys. • Explain the features and purpose of a public-key certificate. • Compare different techniques for implementing the different phases in the public-key certificate lifecycle. • Explain some alternative approaches to public-key management that do not involve certificates.
Topic 9. Applications of Cryptography	**Key concepts:** Some applications of cryptography and exploration of the design decisions taken.

	Learning outcomes: • Appreciate the influence of application constraints on making decisions about how to deploy cryptography. • Analyze several applications of cryptography, justifying design decisions concerning cryptographic mechanisms chosen and the management of keys. • Anticipate possible future applications of cryptography.
Topic 10. Societal Issues	**Key concepts:** Societal use of cryptography and challenges that this presents. **Learning outcomes:** • Appreciate different perspectives on the extent to which use of cryptography should, and can be, controlled. • Compare a range of strategies for controlling use of cryptography, recognizing how and why some of these have evolved over time. • Formulate an opinion on how society should address the dilemma presented by use of cryptography. • Hypothesize how future developments might affect societal use of cryptography.

Activities of this module

The module is comprised of the following elements

- Lecture videos.
    - Lectures broadly divided into ten weeks that evolve from theoretical foundation to practical application of cryptography.
- Practice (formative) Quizzes. There are two types of practice quizzes in this course:
    - ‘Check your understanding’ quiz in the end of each lesson.
    - Reflective questions with feedback provided after submission of answers.

- Formative Peer Reviewed Assignments.
    - There are three peer reviewed assignments that need to pass by providing constructive feedback to peers and discuss what you can learn from their work.
- Discussion Prompt.
    - There are many activities included in discussion prompts in every week which you will need to complete and share outputs on discission forum. It is strongly recommended that students engage in these debates with their fellow peers.
- Staff Graded Assignments.
    - There is one graded timed assignment in the end of the course.

How to pass this module

The module has one major summative assessment each worth 100% of your grade:

- In the end of the study session there will be a written examination

Activity	**Required?**	**Deadline week**	**Estimated time per module**	**% of final grade**
Written examination	Yes	12	24 hours	100%