UNIVERSITY OF LONDON | INTERNATIONAL PROGRAMMES

Royal Holloway University of London

University of London International Academy
MSc/PG Dip in Information Security
Lead College – Royal Holloway

Introduction to Cryptography IYM002 (Core)

Aims

This module takes a very specific approach to presenting cryptography:
Fundamental principles: This module is intended to be both relevant and relatively timeless. It is easy to present a module on cryptography that is quickly out of date. This module is intended to be just as relevant in ten years time as it would have been relevant ten years ago. This is because it is primarily concerned with the fundamental principles rather than technical details of current technology.
Application-focussed: This module is primarily concerned with the cryptography that a user or practitioner of information security needs to know. While there is a great deal of contemporary theoretical research on cryptography, few of these ideas make it through to real-world applications, which tend to deploy only well-tested and understood techniques. This module focuses on cryptography for everyday applications.
Widely accessible: This module is intended to be suitable as a first introduction to cryptography. It focuses on core issues and provides an exposition of the fundamentals of cryptography. This module is intended to be introductory, self-contained and widely accessible.
Students completing this module should not expect to be able to design algorithms

Pre-requisites

None

Essential Reading

- Everyday Cryptography (Martin.)

Included as study material once registered on the course.

Assessment

This module is assessed by a two hour unseen written examination.

Learning Outcomes

On completion of this module, students will have gained an understanding of the use of, and services provided by, the main types of cryptographic scheme. They should also have gained an appreciation of the need for good key management. This will include an appreciation of the general nature of: encryption techniques for providing confidentiality services (including stream ciphers, block ciphers and public key techniques), mechanisms for providing data integrity and origin authentication, including MACs and digital signatures, message exchanges to provide entity authentication and/or key establishment, and the use of Trusted Third Parties, such as Certification Authorities (CAs), to provide and support Public Key infrastructures.

Syllabus

This module is divided into four parts

Part 1: Setting the Scene

Unit 1 - Basic Principles

Unit 2 - Historical Algorithms

Unit 3 - Theoretical versus Practical Security

Units 1 to 3 provide fundamental background. The need for cryptography is motivated in Unit 1 and some of the core security services that can be provided by cryptography are identified. The basic model of a cryptosystem is introduced and the use of cryptography is discussed. We look back at a number of historical encryption algorithms in Unit 2. Most of these are unsuitable for modern practical use, but they illustrate many of the core ideas, as well as some basic encryption algorithm design principles. The differences between security in theory and practice are discussed in Unit 3. It is shown that unbreakable cryptosystems exist, but are not practical, and that most practical cryptosystems are breakable in theory. The real world is always about compromise. We argue that the study of cryptography is essentially the study of a ``toolkit'' of cryptographic primitives which can be assembled in different ways in order to achieve different security goals.

Part 2: The Cryptographic Toolkit

Unit 4 - Symmetric Encryption

Unit 5 - Public-key Encryption

Unit 6 - Data Integrity

Unit 7 - Digital Signature Schemes

Unit 8 - Entity Authentication

Unit 9 - Cryptographic Protocols

Units 4 to 9 explore the various components that make up the cryptographic toolkit. This includes cryptographic primitives and the cryptographic protocols that combine them. We begin with the provision of confidentiality. There are two types of cryptosystem, and we look at the first of these with respect to providing confidentiality in Unit 4, which deals with symmetric encryption. Different types of symmetric encryption algorithms are discussed, as are the different ways in which they can be used. In Unit 5 we look at public-key encryption. The motivation for public-key encryption is explained and two important public-key cryptosystems are studied in some detail. In Unit 6 we look at the way in which (symmetric) cryptography can be used to provide data integrity and the stronger notion of data origin authentication. We then look in Unit 7 at cryptographic techniques for providing non-repudiation, focussing on digital signature schemes. Unit 8 explains how cryptography can be used to provide entity authentication. This unit also considers random number generation, which is often required for entity authentication mechanisms. Finally, in Unit 9 we look at how these cryptographic primitives can be combined to form cryptographic protocols.

Part 3: Key Management

Unit 10- Key Management

Unit 11 - Public-Key Management

In Units 10 and 11 we explore what is arguably the most important, and often overlooked, area of cryptography from a practical perspective: key management. This underpins the security of any cryptographic system and is the aspect of cryptography where users and practitioners are most likely to become involved in decisions concerning cryptography. In Unit 10 we discuss key management in general terms, focussing on the management of secret keys. The life cycle of a cryptographic key is studied and some of the most common techniques for conducting the various phases of this life cycle are discussed. In Unit 11 we look at further issues of key management that particularly relate to public-key cryptography.

Part 4: Applications

Unit 12 - Cryptographic Applications

In Unit 12 we ``tie up'' the previous material by examining some applications of cryptography. Since many of the issues that were raised in the previous chapters require decisions that are application-dependent, we demonstrate how several important applications actually address them. In particular, we discuss why particular cryptographic primitives are used and how key management is conducted. While the cryptographic applications that we discuss are of interest in their own right, the main purpose is to link up the previously discussed ideas. This unit is, inevitably, slightly more detailed than the previous ones.