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

Advanced Cryptography IYM008 (Option)

Aims
This module follows on from the introductory cryptography module (IYM002). In that module, cryptographic algorithms were introduced according to the properties they possessed and how they might fit into a larger security architecture. In this unit we look inside some of the most popular and widely deployed algorithms and we highlight design and cryptanalytic trends over the past twenty years. This course is, by necessity, somewhat mathematical and some basic mathematical techniques will be used. However, despite this reliance on mathematical techniques, the emphasis of the module is on understanding the more practical aspects of the performance and security of some of the most widely used cryptographic algorithms

Pre-requisites
None

Essential Reading
- Handbook of Applied Cryptography (Menezes et al)

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 gain a broad familiarity of the inner-workings of many of today's most widely deployed cryptographic algorithms. Students will also develop a more detailed understanding of some of the most prominent algorithms.

Syllabus

Unit 1 **- Welcome Unit and Cryptography Basics**
In this unit we introduce some of the mathematics and notation that we will need throughout the module. We also discuss the role of cryptography and its place in the security infrastructure. As well as providing a top-level classification of different cryptographic algorithms and cryptographic attacks, we briefly recap the role of some classical ciphers.

Unit 2 **- Introduction to Block Ciphers**
This unit examines the role and importance of one particular class of cryptographic algorithms. Block ciphers play a fundamental role in providing cryptographic protection; here we consider some of the basic properties of these algorithms.

Unit 3 - **DES and DES Variant**
This unit looks at the most important block cipher (DES) in detail. The performance and security of this cipher is examined closely as are some DES-based variants.

Unit 4 - **From DES to AES**
In this unit we consider what will arguably become the most important block cipher over the next 20 years (AES). We will also consider some other ciphers that were proposed with a variety of performance and security trade-offs as the cryptographic community learnt from DES and moved towards the definition of the AES.

Unit 5 - **Block Cipher Cryptanalysis**
In this unit we consider the cryptanalysis of block ciphers and we demonstrate some of the fundamental features of the most powerful generic attack - differential cryptanalysis. The attack is illustrated with a step-by-step approach to the cryptanalysis of a toy cipher
Public-key Encryption

Unit 6 - **Stream Ciphers**
In this unit we consider a second class of symmetric encryption algorithms; stream ciphers. We consider a range of approaches to the design and analysis of these algorithms.

Unit 7 - **Hash Functions and MACs**
Hash functions and MACs play a vital role in many security solutions, yet they do not provide encryption capabilities. We look at some of the most important examples in wide-spread deployment today.

Unit 8 - **Asymmetric Techniques and RSA**
This unit moves us from symmetric cryptographic algorithms to asymmetric cryptographic algorithms. We consider the general classification of these algorithms before we move on to an in-depth study of the most widely deployed asymmetric encryption and signature algorithm; RSA.

Unit 9 - **Discrete Logarithm Cryptosystems**
This unit considers an important class of asymmetric algorithms; those based for their security on the difficulty of solving the discrete logarithm problem. Several proposals are examined with particular attention being paid to performance and security trade-offs when compared to alternative algorithms

Unit 10 - **Elliptic Curve Cryptosytems**
This unit considers another important class of asymmetric algorithms; those based for their security on the difficulty of solving the elliptic-curve discrete logarithm problem. Several proposals are examined with particular attention being paid to performance and security trade-offs when compared to alternative algorithms.

Unit 11 - **Identity-Based Encryption, Identification Schemes and Lattice Cryptosystems**
The final unit considers some alternative asymmetric techniques. First we consider identification schemes and their role in specific applications and then we turn our attention to some new and developing areas of research.