T: +44 [0]1453 860 537
E: info@kryptosec.co.uk
www.kryptosec.co.uk

cryptography specialists

Kryptosec

Fundamentals of Cryptography and Key Management

DURATION
3 DAYS

Course Overview

This course focuses on the central principles and techniques of cryptography and key management, and how they can be applied to achieve different security and trust objectives. By adopting a generic approach, it aims to deliver a core knowledge and understanding that can be applied or adapted to any situation, from system design to the implementation of a specification.

The course shows how different components work together to accomplish specific tasks. Also described are the key management requirements and solutions that are necessary to support the use of the constituent security elements, and how this may influence design decisions. This enables a balanced and complete overview and understanding of a security process.

The strengths, limitations and weaknesses of the different components are also discussed. While not aiming to turn attendees into cryptanalysts, the course conveys a basic appreciation of the nature of modern attacks.

The course concludes by looking at how these techniques are applied in some common applications and standards.

Course Objectives

The objectives of the course are:

- To understand the different cryptographic primitives, their strengths and limitations, and how they work together to achieve security objectives
- To gain a thorough overall perspective of the subject to support effective management or design decisions
- To achieve a technical competency sufficient for system design or implementation
- To provide an understanding of the different key management requirements and methodologies

Pre-Requisites

None. The course assumes no prior knowledge.

The course does use mathematical concepts and notation in places. However, the mathematical content can be varied according to choice, and all concepts and notation will be thoroughly introduced.

Course Description

The course is structured as follows:

- The role of cryptography, and the security and trust services it provides
- Generic threats, design assumptions and objectives
- Mathematical concepts (optional)
- Symmetric key ciphers: their characteristics, structure and uses, from historical examples through to modern ciphers, and including:
  - Provably secure encryption
  - Stream ciphers, including LFSRs, RC4
  - Block ciphers, including AES
  - Modes of operation
  - Data integrity, including MACs
- One way functions and Hash functions
- Asymmetric key techniques: their attributes and uses, including:
  - Diffe-Hellman key exchange
  - Public key encryption, including RSA and ElGamal
  - Digital signatures, including RSA and DSA
  - Elliptic curve cryptosystems
- Identification techniques
- Cryptographic key management: the different requirements and techniques for symmetric and asymmetric keys, including:
  - Generation and distribution
  - Storage and control
  - Update and revocation
  - The role of certificates and Certification Authorities
- Cryptographic applications, including SSL and VPNs

Course Style

The course is presented through lectures.

Price and Availability

Please contact Kryptosec for the latest pricing and availability information.