Kryptosec Limited
Fifty Eight The Street
Uley Dursley
Gloucestershire
GL11 5SJ UK
T: +44 [0]1453 860 537
E: info@kryptosec.co.uk
www.kryptosec.co.uk

SECURITY | CRYPTOGRAPHY | CONSULTANCY | TRAINING

cryptography specialists

Kryptosec

Practical Cryptography: A User's Guide

DURATION
2 DAY COURSE

Course Overview

Many applications from simple file encryption through to network security rely on the use of cryptographic techniques. This course is aimed at those who require sufficient knowledge of cryptography and key management to support the use of such techniques in a range of scenarios, but who do not require an extensive technical or mathematical understanding.

The course first introduces the core cryptographic components, describing the different security and trust services they provide, as well as the different properties, characteristics and requirements associated with the use of different cryptographic techniques. The course will then look at the complete key management lifecycle from generation through to destruction, for both symmetric and public key types. This will include Public Key Infrastructure (PKI) and the role of digital certificates and Certification Authorities. The course ends by looking at the role played by these techniques in various security applications from secure networks to SSL protected websites.

Course Objectives

The course will equip delegates to:

- Appreciate the different security services provided by cryptographic techniques, and how these techniques be applied to meet different security objectives
- Appreciate the different properties, characteristics and requirements associated with different cryptographic techniques
- Understand the key management lifecycle, including PKI and the role played by digital certificates and Certification Authorities
- Understand how these techniques are applied in various applications and standards

Course Description

The course assumes no prior knowledge, and is structured as follows:

- The security services: confidentiality, data integrity, authentication and non-repudiation
- Symmetric key ciphers, from historical examples through to modern ciphers, and including:
  - Provably secure encryption
  - Stream ciphers
  - Block ciphers, including DES and AES
  - Modes of operation
  - Data integrity techniques, including MACs
- Asymmetric key techniques, including:
  - Diffe-Hellman key exchange
  - Public key encryption, including RSA
  - Digital signatures
  - Elliptic curve cryptosystems
- Identification techniques
- Cryptographic key management:
  - The generation and distribution of keying material
  - Control of the use of keying material
  - Update, revocation and destruction of keying material
  - Storage, backup and archival of keying material
- Security applications:
  - SSL
  - Virtual private networks, including IPsec
  - Wireless security

Who Should Attend

Those who require sufficient knowledge of cryptography and key management to support the use of such techniques, but who do not require an extensive technical or mathematical understanding. Anyone wishing to develop an understanding of the core cryptographic techniques, the services they provide and the applications they support. Anyone who needs to understand cryptographic key management.

Course Style

The course is presented through lectures.

Price and Availability

Please contact Kryptosec for the latest pricing and availability information.