



Information Security and Cryptography

DURATION
4 DAY COURSE

Course Overview

Information security is a broad subject. However, common to many security applications is a reliance on the use of cryptographic techniques. The approach taken in this course is therefore to first focus on the core techniques of cryptography, such as encryption, digital signatures and key management, so as to develop a core of knowledge that is applicable across a wide range of security scenarios, and to then focus on employing these techniques in practice to enable services such as network and email security, and SSL protected websites.

In more detail, the course first develops an understanding of the different security services provided by cryptography, and then looks at the actual techniques used to achieve these services. The course then focuses on the management of cryptographic keys, including the key management principles associated with the use of different security applications and the role of certificates and PKI. Finally, the course looks at how the security techniques described can be applied in practice for different security applications. The approach taken is to discuss the relevant security standards and some of the security and implementation issues, and, in some cases, demonstrate the set up and use of a sample implementation. The solutions covered include generating and issuing certificates, and setting up and using an SSL enabled website, a Virtual Private Network and secure email.

The course aims to avoid as far as is practical showing bias towards any particular solutions vendor, and includes the use of open source solutions.

Course Objectives

The course should equip delegates to:

- Implement or evaluate a wide range of security technologies based on a proper understanding of the core security principles
- Appreciate the different cryptographic techniques, the range of services they provide and how they are constructed and used
- Understand the implications of using such techniques
- Appreciate the different key management requirements and methodologies
- Apply the relevant cryptographic techniques and security standards, along with their supporting infrastructure, to set up and use an SSL enabled website, a Virtual Private Network and secure email

Course Description*

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

- The cryptographic services:
 - Confidentiality
 - Data integrity - protection against the unauthorised alteration of data
 - Authentication - corroboration of the source of some data and of the identity of a party
 - Non-repudiation - preventing the denial of previous commitments or actions
- 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
- Asymmetric key techniques, including:
 - Diffie-Hellman key exchange
 - Public key encryption, including RSA and ElGamal
 - Digital signatures, including DSA
 - Elliptic curve cryptosystems
 - Probabilistic public-key encryption
- Identification techniques, including:
 - The use of two-factor authentication tokens
 - Zero-knowledge protocols
- Cryptographic key management, including:
 - The generation and distribution of keying material
 - Controlling the use of keying material
 - Update and revocation of keying material
 - Storage of keying material
 - The role played by Hardware Security Modules (HSMs)
 - Practical demonstrations of setting up Certification Authorities and issuing digital certificates
- The PKCS standards
- Cryptographic applications:
 - SSL and its implications, and setting up an SSL enabled Apache server
 - Virtual private networks, including IPsec and SSL VPNs
 - Setting up and using secure email, including both S/MIME and OpenPGP based solutions
 - Disk and file encryption
 - Trusted Platform Modules

Note that although the course does necessarily contain some mathematical content, this is kept to a minimum in the main part of the course, with additional optional modules available to those who are interested in exploring the mathematical concepts in greater detail.

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

cryptology specialists
Kryptosec



Information Security and Cryptography

DURATION
4 DAY COURSE

Who Should Attend

Those who have a responsibility for implementing, evaluating or designing security solutions. Anyone who needs to understand key management practices and issues. Anyone who wishes to develop a good understanding of the core cryptographic techniques and how they can be applied to solve a number of security problems.

Course Style

The course is presented through lectures, although audience participation is encouraged.

Price and Availability

The course is available as either an onsite option, delivered at a site of your choosing, or as an open scheduled course. Please contact Kryptosec for the latest pricing and availability information, or visit the website.

*Note that the course contents are subject to change

About the Presenter

Dr Mark Blunden is an information security specialist with a PhD in cryptography and a degree in mathematics, who has previously held positions in both the telecommunications and defence sectors. In his time with Kryptosec, he has worked with clients ranging from banks and other financial institutions through to software development companies.