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

Basic Cryptography: An Introduction to Encryption, Digital Signatures and Certificates

DURATION
1 DAY COURSE

Course Overview

Properly applied cryptographic techniques such as encryption and digital signatures are powerful and sometimes essential tools in establishing effective information security. This course provides an introduction to the core cryptographic techniques and the different security services they provide, together with an overview of the key management principles and techniques, such as digital certificates, that are necessary to support the use of cryptographic applications. The course ends by looking at how these techniques can be applied to enable various security applications from secure networks to SSL enabled websites.

Course Objectives

The course should enable delegates to:

- Appreciate the core techniques of cryptography and how they can be applied to meet various security objectives
- Understand both the importance of cryptographic key management, and the different key management requirements and practices associated with the use of different security techniques
- Appreciate how the techniques described are employed in practice in a variety of security applications, from SSL enabled websites through to disk encryption

Course Description*

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

- The security 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
- Introduction to the core cryptographic techniques: symmetric ciphers, public key encryption, digital signatures, data integrity techniques, message authentication techniques
- Overview of cryptographic key management: the life-cycle of cryptographic keys from generation through to destruction, and including digital certificates and Certification Authorities
- Identification techniques: from passwords to challenge response techniques
- Secure email: including the S/MIME standard
- SSL enabled websites
- Network security: methods for constructing virtual private networks
- Protection of stored information: hard disk encryption, file encryption

Who Should Attend

Those who have a technical or management responsibility for implementing security and who need to be aware of cryptography and key management techniques. Anyone who wishes to develop an understanding or appreciation of how cryptographic techniques can be used to solve a number of security problems.

Course Style

The course is presented through lectures.

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