



## Fundamentals of Cryptography and Key Management

DURATION  
3 DAY COURSE

### Course Overview

The ability to protect the confidentiality of information, to prevent unauthorised access to data or services and to prevent the unauthorised modification of data are fundamental elements of security. Similarly, the ability to know who you are talking to and where something has come from, and to be able to bind parties to previous commitments or actions, are essential for trust. In the electronic world, these services typically rely on the use of cryptographic techniques. However, it is imperative that these techniques are used in the correct fashion if they are to satisfy their objectives. In particular, it is crucial that cryptographic keys are managed in an appropriate way.

The course introduces the core techniques of cryptography around which security and trust can be constructed, and highlights the implications of using such techniques. It also looks at the entire key management lifecycle, and examines the differing requirements and methodologies for managing cryptographic keys of different types. The course ends by looking at how these techniques are applied in various applications and standards, from VPNs to secure email. The applications and techniques described are accompanied by a description of their strengths and limitations and the necessary supporting infrastructure.

### Course Objectives

The course will equip delegates to:

- Appreciate the different services provided by the various cryptographic techniques, and understand their differences and how they are constructed
- Understand the implications of using such techniques
- Appreciate the different key management requirements and methodologies
- Understand how these techniques are applied in various applications and standards, from VPNs to secure email

### Course Description

The course assumes no prior knowledge, although parts of the course do use mathematical concepts and notation. However, such concepts and notation will be explained whenever encountered. The course is structured as follows:

- The cryptographic services:
  - o Confidentiality
  - o Data integrity - protection against the unauthorised alteration of data
  - o Authentication - corroboration of the source of some data and of the identity of a party
  - o Non-repudiation - preventing the denial of previous commitments or actions

- Symmetric key ciphers, from historical examples through to modern ciphers, and including:
  - o Provably secure encryption
  - o Stream ciphers
  - o Block ciphers, including DES and AES
  - o Modes of operation
  - o Data integrity techniques
- Asymmetric key techniques, including:
  - o Diffe-Hellman key exchange
  - o Public key encryption, including RSA and ElGamal
  - o Digital signatures, including DSA
  - o Elliptic curve cryptosystems
- Identification techniques
- Cryptographic key management: the life-cycle of cryptographic keys from generation through to destruction, and including digital certificates and Certification Authorities
- Cryptographic applications:
  - o The SSL standard and its implications
  - o Virtual private networks, including IPsec and SSL VPNs
  - o Secure email, including the S/MIME standard
  - o EMV

### Who Should Attend

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. Anyone who needs to understand key management practices and issues. Those who have a technical responsibility for security.

### Course Style

The course is presented through lectures.

### Price and Availability

Please contact Kryptosec for the latest pricing and availability information