



Hands-on Cryptography and Secure Networking

A Five-Day Course

Since the days of Caesar Augustus, cryptography has been used to provide secret communications. Cryptography can also provide integrity controls and proof of authorship.

This course provides students with hands-on experience using cryptography, examining cryptographic algorithms which providing confidentiality, integrity and accountability.

We will examine key management options and key exchange protocols, in order to understand the issues of cryptographic keys.

This course provides hands-on experience with cryptanalysis, the art of breaking codes, by examining the methods and processes used to locate patterns and derive methods to break cryptography.

We will then take this knowledge of cryptography to the practical application of network privacy. We will explore VPN technologies which reside at each layer of the network stack, examining their features and the scope for the confidentiality and authentication they provide.

Course Contents

Cryptography

- Cyphers - Codes - Crypts
- One-way Hashes
- Message Digests
- Symmetric Cryptography
- DES
- AES
- Asymmetric Cryptography
- RSA
- Public Key Cryptography

Key Management Issues

- Secure Key Exchange
- Key Exchange Protocols
- Key Escrow Schemes
- Public Key Infrastructure
- Digital Certificates

Cryptoanalysis

- Pattern Analysis
- Ciphertext Only
- Known Plaintext
- Chosen Plaintext

Network Security

- Application Layer
- Transportation Layer
- Network Layer
- Physical Layer

Virtual Private Networks

- WEP - Wireless Equivalent Privacy
- SSL - Secure Socket Layer
- TLS - Transport Layer Security
- SSH - Secure Shell
- IPSEC - IP Security Protocol

Who Should Attend

IT consultants, managers, security policy developers, privacy officers, information security officers, network administrators, security device administrators and security engineers. You should have an understanding of security concepts and models with experience in administering systems and familiarity with TCP/IP.

What You'll Learn

- How cryptography provides privacy, integrity and authentication.
- Difficulties and issues with implementing cryptography.
- The differences and applicability of varying network security protocols.

What You'll Do

- Explore cryptographic methods including cyphers, code books and stenography.
- Experience the process of breaking cryptographic codes.
- Implement different virtual private networks.
- Detailed examination of network security protocols.

What You'll Take Home

- Understanding of the uses of cryptography.
- Experience implementing network security protocols.
- Your personal copy of *Network Security: Private Communication in a Public World*.