



# CISSP: Cryptography



## CISSP: Cryptography

### 1 Session –

3 Hours of Interactive Training

Cryptography is one of 10 domains comprising the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). In this CISSP certification prep course from LearnKey, expert instructor Michael Solomon covers the history, methodologies and practices of cryptography, as well as common security protocols employing cryptography. At the conclusion of this course, you will be familiar with the issues and concepts of the Cryptography domain required to pass the CISSP exam.

#### Also Available:

- Test Prep

#### About The Author

**Michael Solomon**, CISSP, TICSA, is a security consultant and trainer. Since 1987 he has worked with more than 60 organizations including Earthlink, Nike, Lucent Technologies, BellSouth, and UPS. Solomon holds Computer Science from Emory University (1998), and has contributed to or co-authored information security certification study guides for Que, Sybex and other publishers.

### Session 1

#### Section A: History and Goals

- Ancient History
- Modern History
- Confidentiality
- Integrity
- Authentication
- Nonrepudiation
- Cryptographic Uses

#### Section B: Concepts and Methodologies

- Overview
- Transposition Cipher
- Substitution Cipher
- Cipher Categories
- Cipher Process
- Symmetric Algorithms
- Asymmetric Algorithms
- Message Authentication

#### Section C: Cryptographic Algorithms

- Overview
- DES
- Triple DES
- IDEA/Blowfish/Skipjack
- AES
- RSA/EI Gamal
- Hashing Algorithms
- Other Hashing Algorithms

#### Section D: Cryptographic Practices

- Digital Signatures
- Signature Types
- Key Distribution
- Steganography
- PKI

#### Section E: System Architecture

- PEM
- MOSS
- S/MIME
- SSL
- HTTPS
- SET
- IPSec
- ISAKMP

#### Section F: Methods of Attack

- Brute Force
- Known Plaintext
- Chosen Ciphertext
- Chosen Plaintext
- Meet-in-the-Middle
- Man-in-the-Middle
- Birthday
- Replay