

Course Name:	Principle and Practice of Cryptographic Technology
Duration:	2 Day
Medium of Instruction:	Cantonese (with handout in English)
Award of Certificate:	Certificate of Attendance

Nature and Objectives:

The threat from computer crime and other information security breaches continue to rise. Information confidentiality and integrity, user authentication and non-repudiation of electronic transactions represent major challenges to this information era. Cryptography plays an important role in dealing with these challenges. The 2-day workshop provides IT professionals with a comprehensive understanding of various **cryptographic solutions**. In addition to theories and concepts, **hands-on exercises and practice** will be introduced across the workshop. Each participant will be provided with a dual-bootable Windows-Linux computer to try out the techniques taught.

Who Should Attend:

IT professionals responsible for organizational and enterprise security, system and network management and administration: System and Network Administrators / Engineers / Analysts, Technical Engineers / Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors and Managers, Network Manager, Security Consultants, and System Integrators.

Course Outline:

Foundations of Information Security

- Information Security
- The Ancient Art of Secret Messages
- Cryptography Basics
- Classic Cryptography
- Modern Cryptography

Symmetry Cryptography (Private Key)

- Stream Ciphers
- Linear Feedback Shift Register (LFSR)
- Block Cipher
- Feistel cipher, DES, 3DES, DESX, AES
- Block Cipher Modes

Asymmetry Cryptography (Public Key)

- Diffie-Hellman Key Exchange Protocol
- RSA, El-Gamal, Elliptic Curve Cryptography
- Public Key Infrastructure

Hash Functions and Message Authentication

- Non-Cryptography Hashes
- Hash Message Authentication Codes (HMAC)
- Digital Signature Standard (DSS)

Cryptographic Attacks

- Differential Cryptanalysis
- Linear Cryptanalysis

- Time-Memory Trade-Off (TMTO)

Digital Certification and Web Security

- X.509 Certification (OpenSSL)
- Secure Sockets Layer (SSL) & TLS

Secure Email

- PGP, S/MIME, GnuPG, STARTTLS
- Secure email client
- Signed and Encrypted email

Internet Protocol Security: IPsec

- IP Security and Architecture
- IKE and Key Management
- IPsec Applications
- SSL VPN

Access Controls

- Network authentication, Kerberos
- Secure Shell (SSH)

Cryptography Related Applications

- Information Hiding
- Steganography
- Digital Watermark
- Random Numbers
- Secret Sharing
- Zero Knowledge Proofs