

Course Name:	Cryptography with Java Workshop
Duration:	2.5 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 2.5 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 Windows based 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:

The JCE and the JCA

- JCA and JCE Architecture
- JCA/JCE Design Pattern
- Cryptographic Services Provider
- How to add a Services Provider
- How to Confirm a Provider has been installed; and List out the installed Provider capabilities

Symmetric Key Cryptography

- A variety of Symmetric Key Ciphers
- Paddings
- Cipher Modes of Operations
- Randomly-Generated Symmetric Key
- Key Wrapping
- JCE I/O Classes

Message Digests (MD), MACs, and HMACs

- Introduction to MD and MACs
- How to create MD and MACs

- Differences between MD and MACs
- Where to apply MD and MACs
- Digests as the basis of other functions for PBE and Masking
- Streaming support for MD

Asymmetric Key Cryptography

- Some popular asymmetric algorithms
- Key Exchange and Key Agreement
- Padding Mechanisms with Asymmetric Keys
- Create and verify Digital Signatures

Object Description in Cryptography Using ASN.1

- Introduction to ASN.1 modules related to Cryptography
- Basics about ASN.1 types and relevant ASN.1 Binary Encoding Rules
- ASN.1 Binary Encoding and Java APIs for Encoding Algorithm Parameters
- Encoding and Re-creation of Public and Private Keys using ASN.1 Objects