cSEMINAR CONTEMPORARY CRYPTOGRAPHY

Cryptography is a core security technology with several applications in communications and information systems, e-commerce and e-government in the emerging information society. Every present-day IT professional needs basic knowledge in cryptography, to understand the opportunities offered by this technology, but also the risks underlying in the different facets of its selection, application, implementation and maintenance.

Crypto AG offers a clear and concise professional 5-day seminar on Contemporary Cryptography for security or technical managers. The seminar will help participants understand the basic concepts of cryptography, and acquire the skills needed to manage encryption-based ICT systems. The Crypto cSeminar helps support the planning, implementation, deployment and management of solutions.

The contents of the cSeminar Contemporary Cryptography are managed by the highly experienced and specialised training engineers at the Crypto Academy. Theory and practice are carefully balanced; discussion of examples and case studies, and practical sessions, are given preference over academic presentation. The curriculum of the seminar is in continual evolution; therefore, the contents are regularly checked and updated. New materials or new issues are included according to the evolution of the risk scenario.

This seminar will be held at our very own Crypto Academy in Steinhausen / Zug, Switzerland, which has been awarded a "Premium Class" rating from the International Training Centre Rating Organisation. The comfortable and pleasant atmosphere and the highly qualified instructors will ensure that you will have a successful learning experience.

Course objectives

Participants will acquire the following skills and expertise: Basic knowledge on encryption fundamentals, theory and applications. The well-structured seminar has proven successful for many years and guarantees that you achieve your learning objectives. At the end of the seminar you will be able to understand in depth all major implications of cryptology, and to integrate security solutions from Crypto AG in your own organisation.

Who should attend

This seminar is open to all participants who are typically part of staff of the IT, communications, signals, or other technology-related departments. Their responsibilites include planning, implementing, operating, and maintaining encryption-based security technology, with specific regard to key generation and key management. Delegates should have a good working knowledge of IT and communications fundamentals and understand concepts such as networking, cloud computing, and IT services.

Certification

All participants receive a Certificate of Attendance to the five-day training event.

Standard seminar package

The standard seminar package includes transport, accommodation, catering and leisure activities during the entire stay organised by Crypto AG. Don't hesitate to contact us if you have any change requests or further questions.

For registration and upcoming seminar dates please visit the website www.crypto.ch/seminars

The standard seminar package costs 7,100 CHF.

CONTENT

Agenda

Day 1 – Introduction and overview

The seminar starts with a general introduction to cryptology. Different notions of security are introduced and various classes of cryptographic systems are overviewed, discussed and put into perspective on a high level of abstraction

- Introduction to cryptology
- Notions of security
- Cryptographic systems: classification

Day 2 – Secret key cryptography

This module elaborates on secret key cryptography, i.e., crypto systems that employ secret parameters that are shared among the parties involved. More specifically, it addresses symmetric encryption systems, such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), and the stream cipher RC4, message authentication systems, such as the HMAC construction, random and pseudo-random bit generators, as well as random and pseudo-random functions.

- Intro to secret key cryptography
- Symmetric key encryption systems
- Message authentication systems
- Random and pseudo-random bit generator
- Random and pseudo-random functions

Day 3 – Public key cryptography

This module provides introductory information to available public-key standards.

- Intro to public key cryptography
- Asymmetric encryption systems cryptographic hash functions
- Digital signature systems

Day 4 – Crypto Security Architecture

This module presents in particular the Crypto Security Philosophy and Architecture. It helps participants to understand how cryptography is used in different contexts.

- Crypto Security Philosophy
- Crypto Security Architecture
- Security solutions

Day 5 – Key management and applications

This module elaborates on key management, public key infrastructure (PKI), quantum cryptography, and applications, which include entity authentication, secure multi-party computation, Internet banking, e-government, Internet voting and electronic payment systems.

- Intro to key management
- Key management
- Public key infrastructure
- Quantum cryptography
- Applications of cryptography

Information and specifications are subject to change without notice.