

Seminar on Contemporary Cryptography – Get comprehensive Cryptography-know-how in just one week!



Introduced by your trusted security partner.

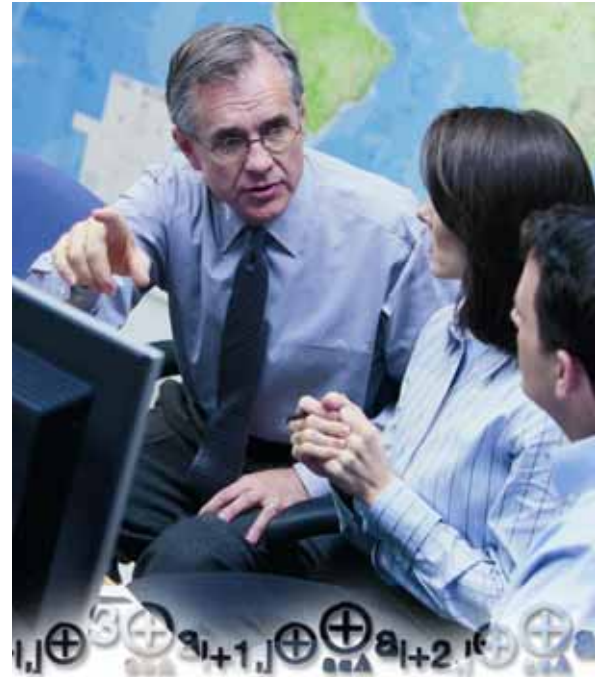


Education in information security –
made in Switzerland.



Contemporary Cryptography – Fundamentals and Applications

Cryptography is a core security technology with many applications in communications and information systems, electronic commerce and e-government in the emerging information society. Today every IT-professional needs basic knowledge in cryptography. This seminar provides an in-depth coverage of cryptography from a conceptual and application-oriented point of view. At the same time, the mathematical algorithmic and protocol aspects are explained without necessarily requiring a deep background in mathematics.



Seminar on Contemporary Cryptography

Crypto AG and its sister company InfoGuard AG have jointly developed a 5 day education programme for the needs of governmental information security professionals.

Who should attend

Delegates from government and defence entities who are responsible for initiating, implementing and maintaining information security in their organisation.

The seminar is open to everyone. On request it can be conducted as a private seminar on a date mutually agreeable. Please ask for further information.

Seminar dates

The seminar dates can be found on the enclosed booking form or on our website: www.infoguard.ch/crypto/

Seminar language

English

Seminar location

InfoGuard AG education centre, Zug/Switzerland.

Seminar Certificate

Each participant becomes an InfoGuard Contemporary Cryptography Expert, and is awarded a formal certificate.

Participants will receive introduction on all relevant topics with regard to a holistic approach to Contemporary Cryptography.



Introduction and Overview

The seminar starts with a general introduction to cryptography. Different notions of security are introduced and various classes of cryptographic systems (cryptosystems) are overviewed, discussed and put into perspective on a high level of abstraction. This module prepares the grounds for the rest of the course.

Secret Key Cryptography

This module elaborates on secret key cryptography, i.e., cryptosystems 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 pseudorandom bit generators, as well as random and pseudorandom functions.

Public Key Cryptography

This module elaborates on public key cryptography, i.e., cryptosystems that employ secret parameters that are

not shared among the parties involved. More specifically, it addresses one-way functions, asymmetric encryption systems, such as RSA, ElGamal, cryptographic hash functions, such as MD5 and SHA-1 and digital signature systems. The module also elaborates on the fundamentals and basic principles of elliptic curve cryptography (ECC).

Crypto Security Architecture

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

Key Management and Applications

This module elaborates on key management (i.e., key distribution and key establishment), public key infrastructure (PKI), quantum cryptography, and cryptographic applications. Such applications include entity authentication and secure multi-party computation, as well as more timely applications, such as Internet banking, e-government Internet voting and electronic payment systems.

Seminar Agenda

Arrival	
Introduction and Overview	
	DAY 1
Secret Key Cryptography	
	DAY 2
Public Key Cryptography	
	DAY 3
Crypto Security Architecture	
	DAY 4
Key Management and Applications	
	DAY 5
Departure	





Days 1

Introduction and Overview

- Cryptology
- Notions of security (unconditional vs. conditional security)
- Cryptographic systems (classification and overview)
 - Unkeyed cryptosystems
 - Secret key cryptosystems
 - Public key cryptosystems

Day 2

Secret Key Cryptography

- Symmetric encryption systems (e.g., DES, AES, RC4, ...)
- Message authentication systems (e.g., HMAC construction)
- Random and pseudorandom bit generators
- Random and Pseudorandom functions

Day 3

Public Key Cryptography

- One-way functions
- Asymmetric encryption systems (e.g., RSA, ElGamal, Rabin, ...)
- Cryptographic hash functions (e.g., MD5, SHA-1, ...)
- Digital signature systems
- Elliptic curve cryptography (ECC)

Day 4

Crypto Security Architecture

- Crypto Security Philosophy
- Crypto Security Architecture
- Security solutions

Day 5

Key Management and Applications

- Key management
- Public key infrastructure (PKI)
- Quantum cryptography
- Cryptographic applications
 - Entity authentication
 - Secure multi-party computation
 - Internet banking
 - Remote Internet voting
 - Electronic payment systems

Seminar environment



Tutors

The skill transfer is of high quality, both in terms of subject matter and tuition. In addition to their technical or scientific background, the tutors have many years of practical experience in their specialist fields with regard to information security and other ICT related areas. Their extensive social and cultural skills guarantee a congenial learning environment.

Seminar methodology

The seminar consists of know-how transfer sessions and discussions.

Daily schedule

5 days	Morning	9.00 – 12.00 h
Monday to Friday	Lunch	12.00 – 13.30 h
	Afternoon	13.30 – 16.30 h

Accommodation

Hotel booking can be arranged on request.



Terms and conditions

Registration

Please complete the registration form enclosed or online on our website www.infoguard.ch/crypto and fax to +41 41 749 19 10 or mail to info@infoguard.com. Your registration will be confirmed in writing.

Cancellation

- All cancellations must be submitted in writing.
- Up to two weeks before the start of the seminar, 25% of the registration fee will be charged for administration.
- Up to one week before the start of the seminar, 50% of the registration fee will be charged.
- In the week before the start of the seminar, the full registration fee will be charged.
- No charge will be made if another person participates in the seminar on behalf of the absent participant.

Substitutions/Name Changes

If you are unable to attend you may nominate, in writing, another participant to take your place at any time prior to the start of the seminar. Two or more participants may not «share» a place at a seminar. Please make separate bookings for each participant.

Alterations

- InfoGuard AG reserves the right to cancel the seminar due to an insufficient number of registrations. In such cases, any registration fees already paid will be fully refunded.
- It may become necessary for us to make alterations to the content, speakers, timing, venue or date of the event compared to the advertised programme.

Terms of Payment

- Payments are due within 10 days of the invoice date and not later than the start of the seminar.
- In the event of a registration at short notice, i.e. within one week, the person participating in the seminar may be required to submit proof of payment or to pay cash prior to the seminar start.

Place of Jurisdiction

- The place of jurisdiction is Zug, Switzerland

Enjoy your stay in Switzerland

Your stay in Switzerland will be carefully prepared. Learning will be made much easier thanks to a pleasant atmosphere and interesting, exciting leisure time. During this five day seminar we will organize a cultural outing.

The small but lively town of Zug (22'000 inhabitants) benefits from being close to the Swiss business metropolis of Zurich and its international airport, which is 35 kilometers away. It is situated right by Lake Zug, and surrounded by typical Swiss hills and mountains. The region is an excellent starting point for excursions to the country's most interesting tourist attractions.



InfoGuard AG – Education in information security «Made in Switzerland».

InfoGuard AG is the preferred education provider for information security. Its courses are geared to the needs of governmental and military organizations as well as public administrations.

Crypto AG – To Remain Sovereign.

We have developed, manufactured and implemented custom security solutions for over 55 years. You too can rely on the expertise and capabilities of Crypto AG – just like our customers in over 130 countries.

**Designed and given
by the sister company
of Crypto AG:**

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Switzerland
Phone +41 41 749 19 00
Fax +41 41 749 19 10
info@infoguard.com
www.infoguard.ch/crypto

**Introduced by your
trusted security partner:**

Crypto AG
P.O. Box 460
CH-6301 Zug/Switzerland
Phone +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch



A MEMBER OF «THE CRYPTO GROUP»