

# Information Security & Cryptography

Fundamentals and  
Applications

June 8–10, 2026  
Zurich, Switzerland

Lecturers:  
**Prof. David Basin**  
**Prof. Ueli Maurer**

# Program

Starting 09:00 on Monday, June 8<sup>th</sup>, and ending at 17:00 on June 10<sup>th</sup>, 2026.

## **Information Security: An Overview**

- Information at Risk: Threats, Security Objectives, and Security Measures
- Classification of the Fundamental Information Security Problems
- Course Overview

## **Cryptography: Basic Concepts**

- Some History
- Types and Models of Cryptographic Systems
- Cryptographic Functions, Hash Functions
- Secrecy, Authenticity, and their Duality and Independence
- Symmetric Cryptography: Block Ciphers, Stream Ciphers, MACs, etc.
- Randomness and Pseudo-Randomness
- Cryptanalytic Attacks, Assumptions, Security Definitions
- Public-Key Encryption and Secret-Key Agreement
- Digital Signatures, Certificates

## **Cryptography: Central Methods and Foundations**

- Discrete Mathematics Basics, Groups, Fields
- Theoretical Foundations of Cryptography
- Discrete Logarithms, Factoring, and other Hard Problems
- Design and Analysis of Cryptographic Systems
- RSA: Workings and Security Analysis
- Diffie-Hellman Protocol: Workings and Security Analysis
- Elliptic Curve Cryptography
- Modes of Operation for Cryptographic Systems
- Security Proofs, Indistinguishability, Reductions
- Constructive Cryptography and Universal Composability

## **System and Network Security**

- Networking Essentials
- Trade-offs in Securing Network Layers
- Security Protocols including Kerberos, SSL, IPsec
- Security Architectures
- Firewalls and Intrusion Detection

## **PKI and Key Management**

- Key Management Challenges
- PKI Certificates, Architectures, and Standards
- Key Revocation and Recovery
- Trust Models (Direct, Cross, Hierarchical, Web of Trust)
- X.509 and PGP
- Alternative PKIs: Client, CA, and Domain-Centric Options
- Certificate Handling in Web Browsers

## **Authentication, Authorization, and Access Control**

- AAA Architectures: Authentication, Authorization, and Access Control
- Authentication: Passwords, Biometrics, and Token-based
- Policies and Models
- Access Control Matrix Model
- DAC and MAC Models
- BLP, Biba, and Chinese Wall Models
- RBAC, XACML
- Single Sign-on
- Identity Management

## **Privacy and Usage Control**

- Data Protection, GDPR, and Control of Intellectual Property
- Anonymity and Privacy-enhancing Technologies
- Proxies, Mix Networks, and other Anonymity Approaches
- Usage Control Architectures
- Digital Rights Management and Trusted Computing

## **Security Engineering and Web-Application Security**

- Security Engineering in the Software Engineering Life Cycle
- Common Vulnerability Classes including: Session Management, Injection Attacks, Cross-Site Scripting, and Race Conditions
- Security Standards and Certification

## **Advanced Topics in Cryptography**

- Interactive Proofs and Identification Protocols
- Zero-Knowledge Proofs
- Proofs of Knowledge
- Secure Multi-party Computation
- Virtual System Emulation
- E-Voting
- Quantum Cryptography
- Quantum Computing

## **Blockchains and Digital Payment Systems**

- Classification of Digital Payment Systems, E-Cash
- Blockchains and Distributed Ledgers
- Smart Contracts
- Crypto-Currencies, Bitcoin

## **Certification**

Attendees will receive a professional certificate for their participation.

## Lecturers



**David Basin** is a full professor of Computer Science at ETH Zurich. He received his Ph.D. in Computer Science from Cornell University in 1989 and his Habilitation in Computer Science from the University of Saarbrücken in 1996. From 1997–2002 he held the chair of Software Engineering at the University of Freiburg in Germany. His research areas are Information Security and Software Engineering. He is the founding director of the ZISC, the Zurich Information Security Center, which he led from 2003-2011. He served as Editor-in-Chief of the ACM Transactions on Privacy and Security (2015-2020) and of Springer-Verlag's book series on Information Security and Cryptography (2008-present). He has co-founded three security companies, is on the board of directors of Anapaya Systems AG as well as various management and scientific advisory boards, and has consulted extensively for IT companies and government organizations. He is an IEEE Fellow and an ACM Fellow.



**Ueli Maurer** is a professor emeritus of Computer Science at ETH Zurich. His research interests include the theory and applications of cryptography and information security. He served as the Editor-in-Chief of the Journal of Cryptology from 2001 to 2010, and Editor-in-Chief of Springer Verlag's book series in Information Security and Cryptography from 1997 to 2012. Maurer holds several patents for cryptographic systems. He serves on several management and scientific advisory boards, has consulted extensively for the financial industry, the IT industry, and government organisations, and has co-founded several companies, including the blockchain project Concordium. He is an IEEE Fellow, an ACM Fellow, an IACR Fellow, and recipient of the 2013 Vodafone Innovation Award for Mobile Communications and the 2016 RSA Award for Excellence in the Field of Mathematics. He is a member of the Swiss Academy of Engineering Sciences (SATW) and the German National Academy of Sciences (Leopoldina).

## Seminar goals

Information Security and Cryptography are of vital importance today, with applications in communication and information systems, cyberphysical systems, and more generally, in the digitalization of businesses and services. Our seminar covers complementary topics and is aimed at different target audiences, providing an in-depth coverage of Information Security and Cryptography from both a conceptual and an application-oriented viewpoint. At the same time, the mathematical, algorithmic, protocol-specific, and system-oriented aspects are explained in a way understandable to a wide audience. This includes the foundations needed to understand the different approaches, a critical look at the state-of-the-art, coverage of modern applications such as key management and cryptocurrencies, and a perspective on future security technologies.

The seminar is aimed at all professionals who need up-to-date knowledge and expertise in this area. This includes system designers and engineers, security experts, IT-professionals, instructors, project managers, consultants, law enforcement professionals, and professional cryptographers.

The material is presented at three different levels. At the *highest level*, the basic concepts are presented in detail, but abstractly (e.g., as black boxes), without mathematics. No background is required to follow at this level. At an *intermediate level*, the most important concrete schemes, models, algorithms, and protocols are presented as well as their applications. Here some minimal mathematical and systems background is assumed. At the *deepest level*, which is not required to understand the higher levels, different special topics, requiring some mathematical background, are discussed.

## Testimonials

*"Great seminar with relevant insights, both broad and deep, led by two highly motivated 'hosts'"*

**Matti Brändli, Head Infrastructure, Swiss National Bank (SNB)**

*"The seminar strikes the balance between depth and breadth on all the topics relevant to my profession as a cryptographer. The most relevant seminar I had the chance to attend as a cryptographer."*

**Cristof Kaufmann, Security Compliance Officer PCI PIN, PostFinance AG**

*"The seminar was truly exceptional, delivering valuable insights and practical knowledge."*

**Lukas Landis, Head of Software Development TS, LEGIC Identsystems AG**

*"Profound seminar held by two real experts, participation is well invested time."*

**Sasha Freitag, Head IT Governance, Lead Architect, St. Galler Kantonalbank AG**

## Seminar Information 2026

"Information Security and Cryptography" on June 8-10, 2026, in Zurich, Switzerland

Early registration before February 28, 2026: CHF 4,400

Standard registration as from March 1, 2026: CHF 4,800

Payment to be made upon receipt of invoice by means of bank transfer.

Price includes course material, lunches, coffee breaks, and beverages during the seminar.

Course material will be provided by a download link, emailed before the seminar's start.

**To enroll:** send email to [info@infsec.ch](mailto:info@infsec.ch) with the following information: first and last name, company name, business address, invoice address (if different), phone, and email.

## Venue

The seminar will take place at the Marriott Courtyard Zurich North, Max-Bill-Platz 19, CH-8050 Zurich, Switzerland. The seminar hotel is conveniently located between downtown Zurich and the airport, easily accessible from both with public transportation.

The hotel can be booked at a special rate if you book it via the link on our website.