

eSECURITY[®]

Academy
esecurity.academy

Kryptografie

**Entstehungsgeschichte und Funktionsweise
der modernen Verschlüsselungstechnik**

Kurs in Bern

16. Januar 2025

Die Kryptografie ist die Wissenschaft der Datenverschlüsselung und hat eine lange Entstehungsgeschichte: Von der Skytale, über die Verschlüsselungsverfahren von Cäsar und Vigenère, bis hin zu elektromechanischen Rotormaschinen (z.B. Enigma) und zur Ausführung auf Computer optimierte und entsprechend standardisierte Verschlüsselungsalgorithmen (z.B. AES).

Seit in den 1940er Jahren die Informationstheorie und in den 1970er Jahren die «Public Key Kryptografie» entwickelt worden sind, stellt die moderne Kryptografie ein Teilgebiet der angewandten Mathematik dar. In der Theorie kann heute vieles mit Hilfe mathematischer Verfahren bewiesen werden. In der Praxis gibt es aber immer noch sehr viele Möglichkeiten, kryptografische Systeme anzugreifen und auszuhebeln.

Im Rahmen der eSECURITY Academy bietet Prof. Dr. Rolf Oppliger einen 1-tägigen Kurs an, um so-

wohl die Entstehungsgeschichte als auch die Funktionsweise der Kryptografie zu vermitteln. Der Kurs wird ergänzt durch das 2021 erschienene Buch «Cryptography 101: From Theory to Practice» (ISBN 978-1-63081-846-3), das – zusammen mit den verwendeten Folien - an die Kursteilnehmenden abgegeben wird.

Der 1-tägige Kurs findet am Donnerstag, 16. Januar 2025, in Bern statt (Ort und genaue Zeit werden noch bekanntgegeben).

Die Teilnahmegebühren betragen CHF 980.00 (inkl. MWST, Buch, Unterlagen und Verpflegung).

Melden Sie sich bitte bis am 16. Dezember 2024 per E-Mail an registration@esecurity.academy an.

Für Fragen stehen wir Ihnen telefonisch (079 654 84 37) oder per E-Mail (info@esecurity.academy bzw. rolf.oppliger@esecurity.ch) sehr gerne zur Verfügung.