

## GÄNGIGE VERFAHREN IM PRAXISEINSATZ

# KRYPTOGRAPHISCHE PROTOKOLLE UND DEREN ANWENDUNG

**Die Herausforderung: Kryptographische Verfahren in der Praxis nutzen.** Welche Verfahren entsprechen dem aktuellen Technikstand? Welche Parameter benötigt man für welches Verfahren, und wie wirken sie im Zusammenspiel? Solche Fragen treten bei der praktischen Anwendung Kryptographischer Verfahren immer wieder auf. Dieser Kurs stellt eine kurze Einleitung in die praktischen Anwendungsmöglichkeiten der Kryptographie und deren Umsetzung dar. Lernen Sie, selbstsicher mit kryptographischen Verfahren umzugehen.

### Inhalte des Seminars

Überblick symmetrische Verfahren

Überblick Public-Key-Kryptographie

Bewertung des Sicherheitslevels  
kryptographischer Verfahren

Gängige Schlüssellängen und andere  
Sicherheitsparameter

Nützliche nationale Standards

Internationale Normierung

Kryptographische Bibliotheken

### Ihr Nutzen

- » Nach dem Seminar können Sie kryptographische Protokolle auf ihre Sicherheit hin bewerten.
- » Sie können kryptographische Parameter sicher einschätzen.
- » Sie können den Einsatz von nationalen und internationalen Standards kryptographischer Funktionen beurteilen.
- » Sie können kryptographische Werkzeuge gekonnt einsetzen.
- » Sie können kryptographische Bibliotheken im Hinblick auf Funktionalität und Performance evaluieren.

### INFORMATIONEN IM ÜBERBLICK

Grundlagen in Computerarchitektur und Netzwerke, Kenntnis einer Programmiersprache

Administratoren\*innen und Entwickler\*innen, die sich mit dem Einsatz und der Konfiguration kryptographischer Methoden befassen

1 Tag Präsenz oder online

600,-

Weiden in der Oberpfalz

Veranstaltet durch

**Fraunhofer**  
AISEC

Referent:



Daniel Loebenberger  
Professor für  
Cybersicherheit an  
der Ostbayerischen  
Hochschule Amberg Weiden  
und Leiter der Forschungs-  
gruppe Secure Infrastructure  
am Fraunhofer AISEC



Weitere Infos und  
aktuelle Termine  
buchen unter:

[www.cybersicherheit.fraunhofer.de/kryptographische-protokolle](http://www.cybersicherheit.fraunhofer.de/kryptographische-protokolle)