

Seminar

inklusive Quizzes und  
Gruppendiskussionen

# Grundlagen der Cybersecurity - Kryptographie für Einsteiger



## Die Top-Themen:

- **Symmetrische Kryptographie und Hashfunktionen**
- **Asymmetrische Kryptographie mit Schwerpunkt auf RSA, Diffie-Hellman und Elliptischer-Kurven-Kryptographie**
- **Post-Quantum-Kryptographie im Kontext der Bedrohungen durch Quantencomputer**
- **Grundprinzipien der Kryptographie: Kerckhoffs' Prinzip und One-Time Pad**
- **Praktische Anwendungen von Kryptographie**

## Termine und Orte

09. und 10. Oktober 2025

Online

07. und 08. Mai 2026

Online

07. und 08. September 2026

Online

Einstieg in Kryptographie -  
praxisnah und anwendungsori-  
entiert!

## Ihr Trainer

Dr. Tobias Oder, Security Archi-  
tect, Alter Solutions Deutschland  
 GmbH, Düsseldorf

## Allgemeine Informationen

### Zielsetzung

**Cybersecurity ist eine der wichtigsten Herausforderungen unserer Zeit, da unsere Abhängigkeit von digitalen Systemen exponentiell wächst. Cyberangriffe können schwerwiegende wirtschaftliche, politische und persönliche Konsequenzen haben, wodurch der Schutz unserer Daten und Infrastrukturen von entscheidender Bedeutung ist, um die Stabilität und Sicherheit unserer Gesellschaften zu gewährleisten. Die ständige Entwicklung von Angriffsmethoden erfordert kontinuierliche Anstrengungen, um den Schutz vor Cyberbedrohungen aufrechtzuerhalten.**

In unserem VDI-Seminar lernen Sie, die Sicherheitsziele von Kryptographie zu verstehen, die Relevanz standardisierter Kryptographie zu erkennen und gängige kryptographische Algorithmen kennenzulernen. Sie werden in der Lage sein, Angriffe auf kryptographische Algorithmen nachzuvollziehen und zu erkennen.

Darüber hinaus zeigen wir Ihnen, wie Sie Kryptographie in der Praxis einsetzen können und vermitteln Ihnen ein Verständnis für verschiedene Anwendungsfälle. Nach dem Besuch des Trainings werden Sie in der Lage sein, zukünftige Bedrohungen, wie Quantencomputer, einzuschätzen und zu mitigieren.

**Nach jedem größeren Themenblock sind kleine Diskussionsrunden vorgesehen, in denen verschiedene Fragen gemeinsam erörtert werden.**

### Zielgruppe

Das Training richtet sich an:

- Anwender von Kryptographie
- Entwickler von sicherheitsrelevanten Produkten und Komponenten
- Systemarchitekten von vernetzten Systemen
- Anwender von Kommunikationsprotokollen



### Inhouse-Seminar

Dieses Seminar können Sie auch als firmeninterne Schulung buchen:

Wir erstellen Ihnen gerne ein individuelles Angebot. Rufen Sie uns an.

**Frau Angela Bungert/Herr Jens Wilk**

Tel.: +49 211 6214-200, E-Mail: [inhouse@vdi.de](mailto:inhouse@vdi.de)

**Herr Heinz Küsters**  

Tel.: +49 211 6214-278, E-Mail: [kuesters@vdi.de](mailto:kuesters@vdi.de)

### Veranstaltungsdokumentation

Jeder Teilnehmer erhält eine Dokumentation wie Präsentationsunterlagen, Handbuch o.ä. und eine VDI Wissensforum-Teilnahmebescheinigung.



### Seminarleitung

**Dr. Tobias Oder**, Alter Solutions Deutschland GmbH, Düsseldorf



Dr. Tobias Oder promovierte 2019 an der Ruhr-Universität Bochum im Fachbereich IT-Sicherheit. Seine aus 26 Publikationen mit über 1000 Zitierungen bestehende Forschung konzentrierte sich auf die praktische Realisierbarkeit von quanten-resistenter Kryptographie auf eingebetteten Systemen. Seit 2020 ist er

als Security Architekt in der Automobilindustrie tätig und übte zwischen 2020 und 2023 weitere Lehrtätigkeiten an der Wilhelm-Büchner Hochschule aus.

### Seminarmethoden

Wir bitten Sie um die Mitnahme eines Notebooks, da das browserbasierte Tool Mentimeter zum Einsatz kommt. Eine Installation von Software ist nicht erforderlich.

Das Training wird durch interaktive Elemente wie Quizzes und Gruppendiskussionen aufgelockert.



### Weitere interessante Veranstaltungen

#### Automotive Systems Engineering kompakt

24. und 25. November 2025, Online

28. und 29. Mai 2026, Online

29. und 30. Oktober 2026, Online

#### Datenbordnetze in Fahrzeugen

26. und 27. November 2025, München

#### Model-Based Systems Engineering kompakt

20. und 21. November 2025, Online

10. und 11. Juni 2026, Online

23. und 24. September 2026, Online

## Seminarinhalte

**1. Tag** 09:00 bis 17:00 Uhr

Symmetrische Kryptographie und Hashfunktionen

### Historische Chiffren

- Was bedeutet Kryptographie?
- Substitutionschiffren
- Enigma

### Grundprinzipien der Kryptographie

- Sicherheitsziele von Kryptographie
- Kerckhoffs' Prinzip
- One-Time Pad

### Stromchiffren

- LFSRs (Linear Feedback Shift Registers)
- ChaCha20 Algorithmus

### Blockchiffren

- Unterschiede zu Stromchiffren
- Modulararithmetik und endliche Körper
- Advanced Encryption Standard
- Modes of Operation
- Message Authentication Codes

### Symmetrische Kryptanalyse

- Wie kann man symmetrische Chiffren brechen?
- Wann gilt eine Chiffre als „gebrochen“?
- Brute-Force Angriffe
- Differenzielle Kryptanalyse
- Lineare Kryptanalyse

### Hashfunktionen

- Sicherheitseigenschaften von Hashfunktionen
- SHA-2 Algorithmus
- SHA-3 Algorithmus

**2. Tag** 08:30 bis ca. 16:30 Uhr

Asymmetrische Kryptographie

### Grundlagen der asymmetrischen Kryptographie

- Unterschiede zur symmetrischen Kryptographie
- Digitale Signaturen

### RSA

- Faktorisierungsproblem
- Mathematische Grundlagen
  - » Eulers Phi Funktion
  - » Erweiterter Euklidischer Algorithmus
- RSA-Algorithmus
- Primzahltests
- Binäre Exponentiation

### Diffie-Hellman-Schlüsselaustausch

- Diskretes Logarithmus Problem
- Vergleich mit dem Faktorisierungsproblem
- Zyklische Gruppen
- Diffie-Hellman-Protokoll

### Elliptische-Kurven-Kryptographie

- Mathematische Grundlagen von elliptischen Kurven
  - » Definition von elliptischen Kurven
  - » Arithmetische Operationen auf elliptischen Kurven
  - » Das diskrete Logarithmus Problem auf elliptischen Kurven
- Unterschiede zu RSA und Diffie-Hellman

### Post-Quantum-Kryptographie

- Quantencomputer als Bedrohung
- NIST Standardisierungsprozess
- Gitter-basierte Algorithmen
- Hash-basierte Algorithmen

### Praktische Anwendung

- Public Key Infrastructures
- Transport Layer Security



VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Deutschland

Sie haben noch Fragen?  
Kontaktieren Sie uns einfach!

**VDI Wissensforum GmbH**  
Kundenzentrum  
Postfach 10 11 39  
40002 Düsseldorf  
Telefon: +49 211 6214-201  
Telefax: +49 211 6214-154  
E-Mail: wissensforum@vdi.de  
www.vdi-wissensforum.de

Ich nehme wie folgt teil (zum Preis p. P. zzgl. MwSt.):

| Seminar  |  |  |
|--|--|--|
| <input type="checkbox"/> <b>09. und 10. Oktober 2025</b><br>Online<br>(015E197005) | <input type="checkbox"/> <b>07. und 08. Mai 2026</b><br>Online<br>(015E197006) | <input type="checkbox"/> <b>07. und 08. September 2026</b><br>Online<br>(015E197007) |
| EUR 1.840,-  | EUR 1.890,-  | EUR 1.890,-  |

www

Ich bin VDI-Mitglied und erhalte **pro Veranstaltungstag EUR 50,- Rabatt** auf die Teilnahmegebühr: VDI-Mitgliedsnummer\* \_\_\_\_\_

\*Für den VDI-Mitglieder-Rabatt ist die Angabe der VDI-Mitgliedsnummer erforderlich.

**Meine Kontaktdaten:**

Nachname \_\_\_\_\_ Vorname \_\_\_\_\_

Titel \_\_\_\_\_ Funktion/Jobtitel \_\_\_\_\_ Abteilung/Tätigkeitsbereich \_\_\_\_\_

Firma/Institut \_\_\_\_\_

Straße/Postfach \_\_\_\_\_

PLZ, Ort, Land \_\_\_\_\_

Telefon \_\_\_\_\_ Mobil \_\_\_\_\_ E-Mail \_\_\_\_\_ Fax \_\_\_\_\_

Abweichende Rechnungsanschrift \_\_\_\_\_

Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_

Teilnehmer mit einer Rechnungsanschrift außerhalb Deutschlands, Österreichs oder der Schweiz bitten wir, mit Kreditkarte zu zahlen. Bitte melden Sie sich über [www.vdi-wissensforum.de](http://www.vdi-wissensforum.de) an. Auf unserer Webseite werden Ihre Kreditkartendaten verschlüsselt übertragen, um die Sicherheit Ihrer Daten zu gewährleisten.

Die **allgemeinen Geschäftsbedingungen** der VDI Wissensforum GmbH finden Sie im Internet: [www.vdi-wissensforum.de/de/agb/](http://www.vdi-wissensforum.de/de/agb/)

**Datenschutz:** Die VDI Wissensforum GmbH verwendet die von Ihnen angegebene E-Mail-Adresse, um Sie regelmäßig über ähnliche Veranstaltungen der VDI Wissensforum GmbH zu informieren. Wenn Sie zukünftig keine Informationen und Angebote mehr erhalten möchten, können Sie der Verwendung Ihrer Daten zu diesem Zweck jederzeit widersprechen. Nutzen Sie dazu die E-Mail-Adresse [wissensforum@vdi.de](mailto:wissensforum@vdi.de) oder eine andere der oben angegebenen Kontaktmöglichkeiten.

Auf unsere allgemeinen Informationen zur Verwendung Ihrer Daten auf <https://www.vdi-wissensforum.de/datenschutz-print> weisen wir hin. Hiermit bestätige ich die AGBs der VDI Wissensforum GmbH sowie die Richtigkeit der oben angegebenen Daten zur Anmeldung.

Ihre Kontaktdaten haben wir basierend auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) zu Werbezwecken erhoben. Unser berechtigtes Interesse liegt in der zielgerichteten Auswahl möglicher Interessenten für unsere Veranstaltungen. Mehr Informationen zur Quelle und der Verwendung Ihrer Daten finden Sie hier: [www.wissensforum.de/adressquelle](http://www.wissensforum.de/adressquelle)

Im Veranstaltungshotel steht Ihnen ein begrenztes **Zimmerkontingent** zu Sonderkonditionen zur Verfügung. Bitte buchen Sie Ihr Zimmer frühzeitig per Telefon oder E-Mail direkt bei dem Hotel mit dem Hinweis auf die „VDI-Veranstaltung“. Weitere Hotels in der Nähe des Veranstaltungsortes finden Sie auch über unseren kostenlosen Service von HRS, [www.vdi-wissensforum.de/hrs](http://www.vdi-wissensforum.de/hrs)



**Leistungen:** Im Leistungsumfang sind die Pausengetränke und an jedem vollen Veranstaltungstag ein Mittagessen enthalten. Ausführliche Veranstaltungsunterlagen werden den Teilnehmern am Veranstaltungsort ausgehändigt.

**Exklusiv-Angebot:** Als Teilnehmer dieser Veranstaltung bieten wir Ihnen eine 3-monatige, kostenfreie VDI-Probenmitgliedschaft an (dieses Angebot gilt ausschließlich bei Neuaufnahme).

Mit dem FSC® Warenzeichen werden Holzprodukte ausgezeichnet, die aus verantwortungsvoll bewirtschafteten Wäldern stammen, unabhängig zertifiziert nach den strengen Kriterien des Forest Stewardship Council® (FSC). Für den Druck sämtlicher Programme des VDI Wissensforums werden ausschließlich FSC-Papiere verwendet.

