

Modulname	Kryptographie und Kryptoanalyse
Modulnummer	INF-25-Ba-W-Kryp
Verantwortliche Dozentin bzw. verantwortlicher Dozent	Dr. Elke Franz elke.franz@tu-dresden.de
Qualifikationsziele	Die Studierenden kennen die grundlegenden Typen kryptographischer Systeme und wissen, welche Schutzziele mit diesen umgesetzt werden können. Sie kennen historische Verfahren sowie moderne symmetrische und asymmetrische Verfahren und sind in der Lage, die Sicherheit dieser Verfahren anhand bekannter Angriffe einzuschätzen. Die Studierenden besitzen die Fähigkeit, diese Systeme zur Durchsetzung der verschiedenen Schutzziele dem derzeitigen Stand der Technik sicher einzusetzen und kennen verschiedene Angriffstechniken und mögliche Gegenmaßnahmen.
Inhalte	Inhalte des Moduls sind die Grundlagen der Kryptographie und Kryptoanalyse, insbesondere verschiedene Systemtypen, Angriffsarten und Sicherheitsbegriffe, historische Verfahren mit ihren Schwächen, moderne symmetrische und asymmetrische Verfahren sowie bekannte Angriffe zur Sicherheitsbewertung.
Lehr- und Lernformen	Das Modul umfasst Vorlesungen im Umfang von 2 SWS, Übungen im Umfang von 2 SWS und das Selbststudium. Die Lehrsprache der Vorlesungen und der Übungen ist Deutsch.
Voraussetzungen für die Teilnahme	Im Bachelorstudiengang Informatik werden die in den Modulen INF-25-Ba-Si Sicherheit sowie INF-25-Ba-Ma3 Algebra zu erwerbenden Kompetenzen vorausgesetzt.
Verwendbarkeit	Das Modul ist im Bachelorstudiengang Informatik ein Wahlpflichtmodul der Fachlichen Vertiefung, das nach Maßgabe der Anlage zur Prüfungsordnung zu wählen ist. Das Modul schafft die Voraussetzungen für die Module, die es unter Voraussetzungen für die Teilnahme benennen.
Voraussetzungen für die Vergabe von Leistungspunkten	Die Leistungspunkte werden erworben, wenn die Modulprüfung bestanden ist. Die Modulprüfung besteht aus einer nicht öffentlichen Mündlichen Prüfungsleistung als Einzelprüfung von 25 Minuten Dauer. Die Prüfungssprache ist Deutsch.
Leistungspunkte und Noten	Durch das Modul können 6 Leistungspunkte erworben werden. Die Modulnote entspricht der Note der Prüfungsleistung.
Häufigkeit des Moduls	Das Modul wird jedes Sommersemester angeboten.
Arbeitsaufwand	Der Arbeitsaufwand beträgt insgesamt 180 Stunden.
Dauer des Moduls	Das Modul umfasst ein Semester.

