Zusammenfassung der Vorlesung vom 16.10.2024

- Was sind besondere Eigenschaften von Informationen, aus denen sich Missbrauchsmöglichkeiten und die Notwendigkeit von Datensicherheit ergeben?
- Was sind die grundlegenden drei Schutzziele, was bedeuten sie?
- Ist ein Verlust dieser Schutzziele erkennbar / verhinderbar / kann er rückgängig gemacht werden?
- Wie grenzen sich Datenschutz und Datensicherheit ab?
- Was ist unter dem Recht auf informationelle Selbstbestimmung zu verstehen? Wie kann seine Relevanz begründet werden?
- Was sind personenbezogene Daten?
- Was verstehen Sie unter dem „Verbot mit Erlaubnisvorbehalt“? Wann ist die Verarbeitung personenbezogener Daten rechtmäßig?
- Welche Bedingungen müssen für eine gültige Einwilligung erfüllt sein?

Zusammenfassung der Vorlesung vom 23.10.2024

- Welche Grundsätze der Datenverarbeitung sind laut DSGVO einzuhalten? Was bedeuten sie?
- Welche Rechte stehen den Betroffenen bzgl. ihrer personenbezogenen Daten zu? Gibt es hierbei Einschränkungen?
- Unter welchen Umständen kann eine Löschung der Daten verlangt werden?
- Unter welchen Umständen kann Widerspruch gegen die Verarbeitung eingelegt werden?
- Was wird mit „Privacy by design“ und „Privacy by default“ gefordert?
- Welche Risiken ergeben sich für den Datenschutz durch IKT?
- Welche Klassen von Bedrohungen durch unerwünschte Ereignisse kann man unterscheiden?
- Was sind (beispielsweise) Ursachen für Sicherheitsprobleme?

Zusammenfassung der Vorlesung vom 30.10.2024

- Welche Angriffsmethoden werden beispielsweise angewendet?
- Was zeichnet Computerviren aus?
- Was sind Beispiele für Verschleierungsmethoden für Viren?
- Was sind grundlegende Antivirentechniken, welche Vor- und Nachteile haben sie?
- Was sind Beispiele für empfohlene Maßnahmen gegen die Gefährdung durch Malware?
- Was verstehen Sie unter dem Prinzip „least privilege“?
- Was beschreibt ein Angreifermodell, was sind wesentliche Inhalte?

Zusammenfassung der Vorlesung vom 06.11.2024

- Was besagt das Prinzip der Angemessenheit?
- Was kann bzgl. der erreichbaren Sicherheit ausgesagt werden?
- Warum ist Sicherheit kein Zustand, sondern ein Prozess?
- Welche Aufgaben sind der Awareness bzgl. Sicherheit zuzuordnen?
- Welche Prinzipien sind beim Sicherheitsmanagement zu beachten?
- Welche Schritte umfasst der Sicherheitsprozess?
- Was beinhalten IT-Sicherheitspolitik und IT-Sicherheitskonzept?
- Wie entstehen allgemein Risiken (Risikobildungsmodell)?
- Mit welchen zwei Faktoren werden Risiken bewertet?
- Welche Aufgaben umfasst die Risikobeurteilung?
- Welche Aufgaben umfasst die Risikobehandlung?
- Wie können Risiken mit Hilfe einer Risikomatrix bewertet werden?
- Welche Risikobehandlungsoptionen gibt es?
- Wie können die Maßnahmen klassifiziert werden? Beispiele?

Zusammenfassung der Vorlesung vom 13.11.2024

- Was beinhaltet die Validierung der Maßnahmen?
- Was unterscheidet Zugangskontrolle und Zugriffskontrolle?
- Welche prinzipiellen Möglichkeiten der Identifikation von Menschen durch IT-Systeme gibt es?
- Wie werden die Zugriffskontrollinformationen grundsätzlich verwaltet, welche vereinfachten Varianten (ACL, CL) gibt es?
- Was ist das Prinzip bei RBAC, welche Aufgaben sind zu lösen?
- Welche Vor- und Nachteile hat die redundante Speicherung?
- Wie funktionieren RAID 0, 1 und 5?
- Welche Fragen sind bei der Organisation von Backups zu klären?
- Welche Aspekte beeinflussen die Auswahl der zu sichernden Daten und die Häufigkeit der Sicherung?
- Welche Backup-Strategien unterscheidet man, wie funktionieren diese und wie erfolgt jeweils die Wiederherstellung?
- Welche Schutzziele sind bzgl. der Aufbewahrung der Kopien relevant und wie können diese umgesetzt werden?
- Was ist Zielstellung der Kanalkodierung?

Zusammenfassung der Vorlesung vom 27.11.2024

- Welche Eigenschaft sichert bei einem ungleichmäßigen Quellenkode die Dekodierbarkeit?
- Fehlererkennung bei Kanalkodierung:
  - Wie prüft der Empfänger eine empfangene Binärfolge auf Verfälschungen?
  - Was sind mögliche Ergebnisse der Fehlererkennung, und wie sind diese zu interpretieren?
- Welche beiden Möglichkeiten der Fehlerkorrektur gibt es?
- Was sind mögliche Ergebnisse der Rekonstruktion im Fehlerfall?
- Was sagt die minimale Hammingdistanz d_{min} über die Fehlererkennungs- bzw. Fehlerkorrektureigenschaften eines Kodes aus?

Zusammenfassung der Vorlesung vom 04.12.2024

- Wie funktioniert der Paritätskode (Kodierung, Fehlerprüfung, Dekodierung)? Welche Kodeparameter hat er?
- Was ist ein zyklischer Kode? Welche Fehlererkennungseigenschaften haben zyklische Kodes?
- Was ist ein Bündelfehler (Burstfehler)?
- Wie wird beim Multiplikations- und Divisionsverfahren kodiert bzw. dekodiert?
- Wie erfolgt die Fehlerprüfung?
- Was versteht man unter der Eigenschaft „systematisch“?
- Welche Kodeparameter und Fehlererkennungseigenschaften hat der zyklische HAMMING-Kode?
- Welche Kodeparameter und Fehlererkennungseigenschaften hat der ABRAMSON-Kode?

Zusammenfassung der Vorlesung vom 11.12.2024

- In welcher Reihenfolge sollten Kryptographie und Kanalkodierung angewendet werden? Warum?
- Welche Schutzziele können mit Kryptographie umgesetzt werden? Was genau kann erreicht werden?
- Was besagt das Kerkhoffs-Prinzip?
- Wie funktionieren prinzipiell symmetrische und asymmetrische Konzelations- und Authentikationssysteme (Funktionen, Input- und Outputparameter der Funktionen)?
- Warum gibt es bei der Verschlüsselungsfunktion des asymmetrischen Konzelationssystems eine Zufallszahl als weiteren Inputparameter?
- Warum kann nur mit digitalen Signatursystemen Zurechenbarkeit erreicht werden?

Zusammenfassung der Vorlesung vom 18.12.2024

- Was sind Vor- und Nachteile symmetrischer bzw. asymmetrischer Systeme?
- Wie ist das Ziel eines hybriden Systems? Wie ist der prinzipielle Ablauf bei einem hybriden Konzelationssystem?
- Welche Angriffsarten auf Kryptosysteme werden unterschieden?
- Was bedeutet informationstheoretische Sicherheit?
- Was sind relevante Anforderungen an die Schlüssel bei einer informationstheoretisch sicheren Chiffre?
- Wie funktioniert die Vernam-Chiffre?
- Warum kann es bei asymmetrischen Verfahren keine informationstheoretische Sicherheit geben?
- Wie funktionieren Transpositionen und Substitutionen?

Zusammenfassung der Vorlesung vom 08.01.2025

- Wie kann das verwendete historische Verschlüsselungsverfahren anhand eines vorliegenden Schlüsseltextes identifiziert werden?
- Wie kann die Analyse von MM-Substitutionen bzw. PM-Substitutionen erfolgen?
- Was ist unter „iterierter Blockchiffre“ zu verstehen?
- Was sind Beispiele für allgemeine Ansätze zur Analyse von Blockchiffren? Was ist jeweils das Ziel und der Ablauf?
- Was sind die charakteristischen Eigenschaften der Feistel-Chiffre?
- Was bedeutet Selbstinversität?
- Was charakterisiert den Algorithmus DES?
- Wie ist die Sicherheit des DES-Algorithmus zu bewerten?

Zusammenfassung der Vorlesung vom 15.01.2025

- Was ist das Ziel der Mehrfachverschlüsselung? Genügt eine doppelte Verschlüsselung?
- Wie ist der Ablauf des Meet-in-the-Middle-Angriffs?
- Was charakterisiert den Algorithmus AES?
- Wie erfolgt bei AES die Verschlüsselung?
- Wie werden die Teilschlüssel erzeugt?
- Wie erfolgt die Entschlüsselung?
- Was versteht man unter synchronen / selbstsynchronisierenden Chiffren?
- Wie erfolgen Ver- und Entschlüsselung bei den Betriebsarten ECB und CBC?
- Wie wirken sich additive bzw. Synchronisationsfehler bei diesen Betriebsarten aus?
- Welche dieser Betriebsarten eignet sich für die Berechnung eines MACs? Warum?
- Wie erfolgt die Berechnung bzw. das Testen des MACs? Wie sicher ist dieser MAC?

Zusammenfassung der Vorlesung vom 22.01.2025

- Wie erfolgt Ver- und Entschlüsselung bei der Betriebsart CTR?
- Wie wirken sich additive bzw. Synchronisationsfehler bei dieser Betriebsart aus?
- Was sind Eigenschaften der Betriebsarten ECB, CBC und CTR?
- Welchen Vorteil bietet der Counter Mode?
- Was bedeutet „multiplikatives Inverses“? Wie kann es bestimmt werden?
- Wie können Primzahlen erzeugt werden?
- Wie werden die öffentlichen und geheimen Parameter für RSA bestimmt?
- Wie erfolgt die Ver- bzw. Entschlüsselung?

Zusammenfassung der Vorlesung vom 29.01.2025

- Wie erfolgt bei RSA das Signieren und Testen?
- Worauf ist bei der Parameterwahl von RSA zu achten?
- Welche Angriffsmöglichkeiten bestehen bei der einfachen, unsicheren Variante von RSA?
- Wie werden diese passiven und aktiven Angriffe verhindert?
- Was ist Multimedia-Sicherheit?
- Welche Schutzziele sind für Multimedia-Sicherheit relevant, und was bedeuten sie in diesem Kontext?
- Mit welchen Schutzmechanismen können diese Ziele durchgesetzt werden?
- Wie grenzt sich Steganographie von Kryptographie ab?
- Wie ist ein steganographisches System prinzipiell aufgebaut (Funktionen mit Ein- und Ausgabewerten)?

Zusammenfassung der Vorlesung vom 05.02.2025

- Was ist bei der Auswahl des Covers zu beachten?
- Welche Klassen von Einbettungstechniken gibt es?
- Wie funktionieren LSB-Ersetzung, Inkrementieren und Dekrementieren?
- Wie ist die Sicherheit der LSB-Ersetzung zu bewerten?
- Wie funktioniert der Visuelle Angriff, wo liegen Grenzen dieses Angriffs?
- Wie funktioniert der Histogrammangriff?