Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Symmetrische kryptographische Verfahren: Grundlagen, AES

Prof. Dr. Holger Schmidt
holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

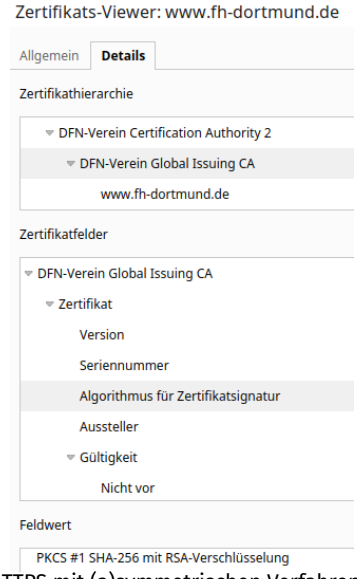
- Kerckhoffsches Prinzip
- Alice-Bob-Mallory-Modell
- Grundlegende Angriffsarten
- Schlüssellängen
- One-Time-Pad
- Advanced Encryption Standard (AES)
- PKCS7 Padding
- CBC und CTR Modi

Lernziele

Die Studierenden sind in der Lage,

- grundlegende Begriffe der symmetrischen Kryptographie zu differenzieren und zu erklären.
- AES, CTR, CBC und PKCS#7 zu erklären und anzuwenden.

Motivation



Kryptographie ist alltäglich: HTTPS mit (a)symmetrischen Verfahren, Schlüsselaustausch, Hashing

Kryptographie
Symmetrische Verschlüsselung: Grundlagen

Dieser Abschnitt basiert auf Schmeh, 2016, Teil 1 – Kapitel 4.1 und Teil 2 – Kapitel 7. Aufgrund der Präsentation als Folien und Notizen sind die Texte der Quelle typischerweise paraphrasiert.

Symmetrische Verschlüsselung

- Schutzziel: **Vertraulichkeit**
- Algorithmus in den ein geheimer Schlüssel mit einfließt
- **Ver-/Entschlüsselungsalgorithmus (Cipher, Chiffre)**

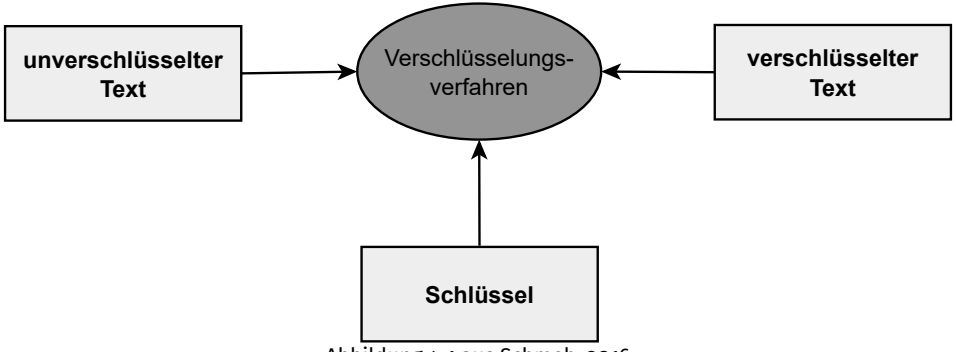


Abbildung 4-1 aus Schmeh, 2016

Kerckhoffs Prinzip

Die Sicherheit eines Verschlüsselungsalgorithmus basiert auf der Geheimhaltung des Schlüssels, nicht auf der Geheimhaltung des Algorithmus.

Gegenteil: **Security by Obscurity**

Klartext, Geheimtext, Schlüssel

- m ist der Klartext, e der Verschlüsselungsalgorithmus, d der Entschlüsselungsalgorithmus, c der Geheimtext, k der geheime Schlüssel
- Verschlüsselungsalgorithmus: $e(m, k) = c$
- Entschlüsselungsalgorithmus: $d(c, k) = m$

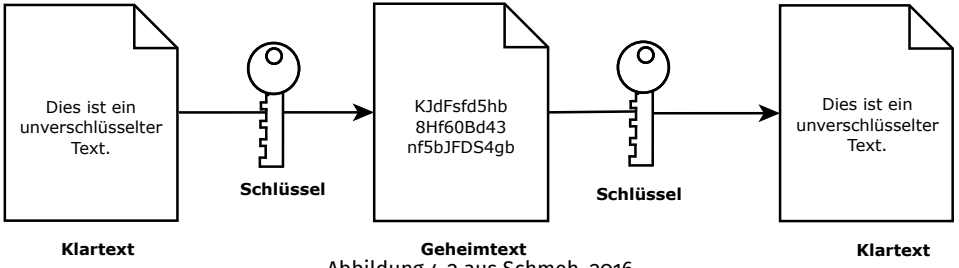
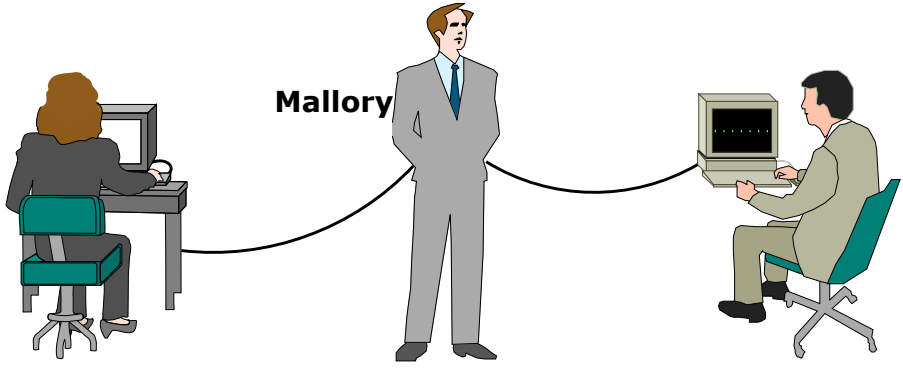


Abbildung 4-2 aus Schmeh, 2016

Alice-Bob-Mallory-Modell



Angelehnt an Abbildung 2-1 aus Schmeh, 2016

Angriffe

- Voraussetzung: Verschlüsselungsalgorithmus ist bekannt.
- Kennt Mallory den Klartext nicht, dann sprechen wir von einem **Ciphertext-Only Angriff**.
- Kennt Mallory den Klartext und versucht, für das Entschlüsseln weiterer Nachrichten den Schlüssel zu erfahren, dann sprechen wir von einem **Known-Plaintext Angriff**.
- Will Mallory den Schlüssel herausfinden und hat dabei die Möglichkeit, den Klartext selbst zu wählen, so sprechen wir von einem **Chosen-Plaintext Angriff**.
- Mallory hat die Möglichkeit den Schlüssel durch ausprobieren herauszufinden. Wir sprechen dann von einem **Brute-Force Angriff** (welcher auf einem Ciphertext-Only Angriff aufbaut).

Eigenschaften von symmetrischen kryptographischen Verfahren

- **Kerckhoffs Prinzip**
- Es darf **keinen besseren Angriff als Brute Force** geben.
- Das Verfahren muss ein **Zufallsorakel** (bzw. **Konfusion**) bilden, d. h. es darf keinen erkennbaren (statistischen) Zusammenhang zwischen Eingabe (Klartext und Schlüssel) und Ausgabe (Geheimtext) geben.
- **Avalanche-Effekt** bzw. (**Diffusion**): Änderung eines Klartext-Bits führt im Durchschnitt zur Änderung der Hälfte der Geheimtext-Bits

Schlüssellängen

- Wir betrachten einen symmetrischen Verschlüsselungsalgorithmus, bei dem Brute Force der beste Angriff ist.
- Bei 56 Bit (wie beim veralteten Data Encryption Standard (DES) (FIPS-46-3, 1999)) liegt der Brute Force Rekord bei 22 Stunden (Kumar, Paar, Pelzl, Pfeiffer, Rupp & Schimmler, 2006).
- Mit jedem Bit verdoppelt sich der Aufwand für Brute Force.
- Bei 128 Bit gibt es $2^{128} = 3,4 \cdot 10^{38}$ Schlüssel.

Mallory im Glück

Wenn Mallory 100 spezielle Computer verwendet, die jeweils 100 Milliarden Schlüssel pro Sekunde durchprobieren können (z. B. Copacobana und Rivyera von Kumar et al., 2006) und Mallory mit viel Glück nach 1% Durchprobieren von Schlüsseln erfolgreich ist, dann benötigt er $3,4 \cdot 10^{23}$ Sekunden, d. h. 10^{16} Jahre.

Wie alt ist das Universum?

Schlüssellängen / Brute-Force

Schlüssellänge	Anzahl der Schlüssel	Dauer Brute-Force
40 Bit	$1{,}1 \times 10^{12}$	1,3 Sekunden
56 Bit	$7{,}1 \times 10^{16}$	24 Stunden
64 Bit	$1{,}8 \times 10^{19}$	256 Tage
80 Bit	$1{,}2 \times 10^{24}$	45.965 Jahre
128 Bit	$3{,}4 \times 10^{38}$	$1{,}3 \times 10^{19}$ Jahre
192 Bit	$6{,}3 \times 10^{57}$	$2{,}4 \times 10^{38}$ Jahre
256 Bit	$1{,}2 \times 10^{77}$	$4{,}4 \times 10^{57}$ Jahre

- „Sicherheitsaufschlag“
- Viele Angriffe funktionieren bei kürzeren Schlüsseln besser

One-Time-Pad

- **Zufälliger Schlüssel, der genauso lang wie der Klartext ist**
- Klartext bitweise XOR-verknüpft mit Schlüssel ergibt Geheimtext
- **Das One-Time-Pad ist sicher (Shannon, 1949).**
- Praktische Probleme:
  - Schlüssellänge $=$ Klartextlänge
  - Produktion von reinem Zufall in ausreichender Menge

Strom- und Blockchiffre

Stromchiffre

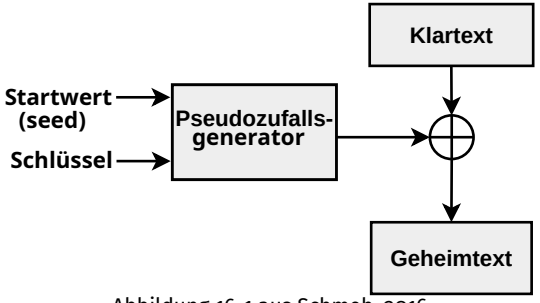


Abbildung 16-1 aus Schmeh, 2016

Blockchiffre

- zerlegt Klartext in Blöcke gleicher, fester Länge.
- verschlüsselt blockweise abhängig von **Block Modus** oder erzeugt eine Stromchiffre

Kryptographie
Advanced Encryption Standard (AES)

Dieser Abschnitt basiert auf Schmeh, 2016, Teil 2 – Kapitel 10. Aufgrund der Präsentation als Folien und Notizen sind die Texte der Quelle typischerweise paraphrasiert.

Advanced Encryption Standard (AES)

- **Blockchiffre**, **SP-Chiffre**
- Ende der 1990er von Vincent Rijmen und Joan Daemen im Rahmen eines NIST-Wettbewerbs entwickelt
- Vom NIST standardisiert (FIPS-197, 2023)
- 128 Bit Blocklänge
- 128 (10 Runden), 192 (12 Runden) oder 256 (14 Runden) Bit Schlüssellänge

Advanced Encryption Standard (AES) – Repräsentation von Bytes

- 128 Bit Klartextblock wird spaltenweise in eine 4×4-**Matrix** M überführt:

$$M = \begin{pmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{pmatrix}$$

- Jedes Byte b_{ij} wird als Element des **Galois-Körpers**[1] $\mathbb{F}_{2^8}$ und damit in der Form $a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0$ mit $a_i \in \{0, 1\} = \mathbb{F}_2$ repräsentiert.

- Die Polynomdarstellung lässt sich mithilfe der Koeffizientenwerte als Bit-Folge $a_7a_6 \ldots a_0$ repräsentieren.

[1] Ein Galois-Körper $\mathbb{F}_q$ ist ein Körper mit einer endlichen Anzahl von $q = p^n$ Elementen, mit p Primzahl und $n \in \mathbb{N}$. p heißt Charakteristik von $\mathbb{F}_q$. Grundlagen zu algebraischen Strukturen befinden sich im Anhang.

Advanced Encryption Standard (AES) – Funktionsweise

Fachhochschule Dortmund
University of Applied Sciences and Arts

1. Schlüsselaufbereitung (Erzeugung von Rundenschlüsseln)
2. *AddRoundKey* (Whitening)
3. Wiederholte (9-, 11-, 13-fache) Ausführung von
   - 3.1. *SubBytes* (Substitution via **S-Box**, verändert die b_{ij})
   - 3.2. *ShiftRows* (Zeilenweise Permutation, verändert die Struktur von M)
   - 3.3. *MixColumns* (Spaltenweise Permutation, verändert sowohl die Struktur von M als auch die b_{ij})
   - 3.4. *AddRoundKey* (**XOR** mit Rundenschlüssel, verändert die b_{ij})
4. Abschließend wird nochmal wiederholt ausgeführt (jedoch ohne *MixColumns*)

Alle Teiloperationen sind **invertierbar**, daher ist AES invertierbar.

Advanced Encryption Standard (AES) – Beispiel Eingabe

Berechnung des ersten, mit AES verschlüsselten Byte (erste Zeile, erste Spalte) ohne *AddRoundKey* am Rundenende für folgenden Block:

Klartext $\oplus$ 0. Rundenschlüssel (Whitening zu Beginn bereits angewandt):

$$\begin{pmatrix} \mathbf{1B} & 31 & 03 & 14 \\ 35 & \mathbf{38} & 44 & 54 \\ 42 & 23 & \mathbf{23} & 33 \\ 70 & 51 & 44 & \mathbf{55} \end{pmatrix}$$

Advanced Encryption Standard (AES) – Beispiel SubBytes

SubBytes entspricht einer byte-weisen Substitution via S-Box (FIPS-197, 2023, S. 16, Figure 7)

$$
\begin{aligned}
\mathit{SubBytes}(1B) &= \mathbf{AF} \\
\mathit{SubBytes}(38) &= \mathbf{07} \\
\mathit{SubBytes}(23) &= \mathbf{26} \\
\mathit{SubBytes}(55) &= \mathbf{FC}
\end{aligned}
$$

Advanced Encryption Standard (AES) – Beispiel ShiftRows

ShiftRows entspricht einer byte-weisen Zeilenrotation nach links (FIPS-197, 2023, S. 17, 5.1.2)

$$\begin{pmatrix} \mathbf{AF} & \dots & \dots & \dots \\ \mathbf{07} & \dots & \dots & \dots \\ \mathbf{26} & \dots & \dots & \dots \\ \mathbf{FC} & \dots & \dots & \dots \end{pmatrix}$$

Advanced Encryption Standard (AES) – Beispiel MixColums I

Fachhochschule
Dortmund
University of Applied Sciences and Arts

MixColums entspricht einer Multiplikation (von links) mit Spaltenmixmatrix (FIPS-197, 2023, S. 17, 5.1.3)

$$(2 \cdot \mathbf{AF}) \oplus (3 \cdot \mathbf{07}) \oplus (1 \cdot \mathbf{26}) \oplus (1 \cdot \mathbf{FC})$$

- Ergebnis ist gesuchtes, erstes AES verschlüsseltes Byte (vor abschließendem Whitening und nach Anwendung erster Runde)
- Multiplikation mit 1 entspricht Identität, also trivial

Advanced Encryption Standard (AES) – Beispiel MixColums II

Fachhochschule Dortmund
University of Applied Sciences and Arts

$$
\begin{aligned}
(2 \cdot AF) &= 00000010_2 \cdot 10101111_2 \\
&= x \cdot (x^7 + x^5 + x^3 + x^2 + x + 1) \\
&= x^8 + x^6 + x^4 + x^3 + x^2 + x
\end{aligned}
$$

- Reduktion (XOR oder Polynomdivision) mittels **irreduziblem Polynom**, da Polynomgrad > 7

$$x^8 + x^6 + x^4 + x^3 + x^2 + x \equiv x^6 + x^2 - 1 \,(mod\ x^8 + x^4 + x^3 + x + 1) \quad ^2$$

- Umrechnung des Polynoms ergibt:

$$
\begin{aligned}
x^6 + x^2 - 1 &= 01000101_2 \\
&= \mathbf{45}
\end{aligned}
$$

Advanced Encryption Standard (AES) – Beispiel MixColums III

Fachhochschule Dortmund
University of Applied Sciences and Arts

$$
\begin{aligned}
(3 \cdot 07) &= 00000011_2 \cdot 00000111_2 \\
&= (x+1) \cdot (x^2 + x + 1) \\
&= x^3 + 1 \;//\; (2x^n \; \textit{wird zu} \; 0)
\end{aligned}
$$

- Das Polynom hat Grad 3 und muss daher nicht reduziert werden.
- Umrechnung des Polynoms ergibt:

$$
\begin{aligned}
x^3 + 1 &= 00001001_2 \\
&= \mathbf{09}
\end{aligned}
$$

- Ergebnis: $\mathbf{45} \oplus \mathbf{09} \oplus \mathbf{26} \oplus \mathbf{FC} = \mathbf{96}$

[2] $a \equiv b \; (mod \; m)$ bzw. gesprochen: „a ist kongruent b modulo m“ bedeutet $a \; mod \; m = b \; mod \; m$ für $a, b \in \mathbb{Z}, m \in \mathbb{N}$

Advanced Encryption Standard (AES) – Schlüsselaufbereitung

Fachhochschule Dortmund
University of Applied Sciences and Arts

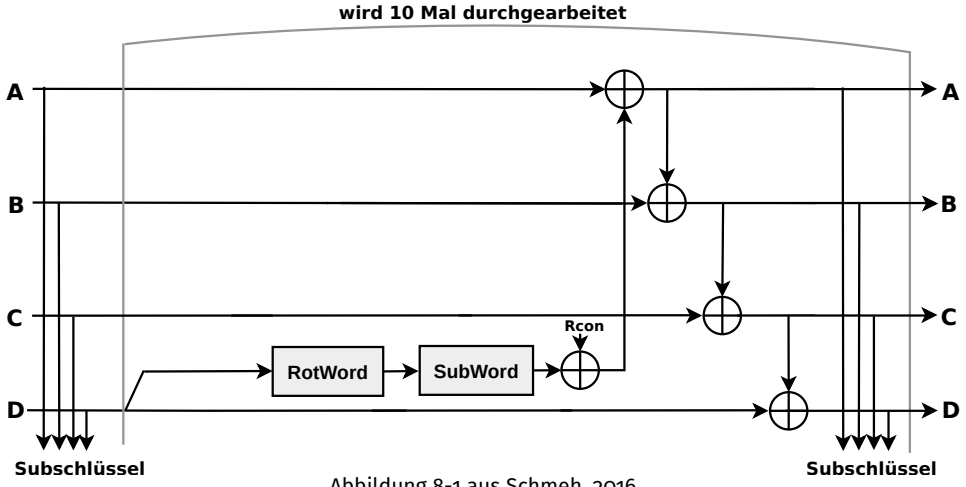


Abbildung 8-1 aus Schmeh, 2016

Advanced Encryption Standard (AES) – Kryptoanalyse

- Brute Force aufgrund von 128 Bit Schlüssellänge nicht praktikabel
- Es existieren Angriffe gegen 7 Runden bei 128 Bit, 8 Runden bei 192 Bit und 9 Runden bei 256 Bit Schlüssellänge (Ferguson, Kelsey, Lucks, Schneier, Stay, Wagner & Whiting, 2001).
- Brute Force ist nicht der beste Angriff auf AES (Bogdanov, Khovratovich & Rechberger, 2011).
- **Kein Angriff mit praktischer Bedeutung bekannt**

PKCS#7 Padding

- Problem: Klartext ggf. kein ganzzahliges Vielfaches von Blocklänge
- Lösung: Klartext wird aufgefüllt (**Padding**)
- PKCS#7 Padding ist in RFC 5652[3] standardisiert.
  - Byte-weises Padding
  - Wert der Padding-Bytes entspricht Anzahl fehlender Bytes minus 1, z. B. fehlen zwei Bytes so wird mit zwei Bytes mit Wert $01h$ aufgefüllt
  - Falls Klartext ganzzahliges Vielfaches von Blocklänge, dann wird Block mit 16 $0Fh$ Bytes angehängt

[3] https://www.rfc-editor.org/rfc/rfc5652, 28. Juni 2023

Counter (CTR) Modus

Standard (NIST SP 800-38A, 2001)

Funktionalität *iv* bestehe aus *nonce*|*counter* mit *counter* $= 0$. Dann gilt:

$$c = c_0|c_1|\cdots = e(iv, k) \oplus m_0|e(nonce|counter + 1, k) \oplus m_1|\ldots$$

bzw.

$$m = m_0|m_1|\cdots = c_0 \oplus e(iv, k)|c_1 \oplus e(nonce|counter + 1, k)|\ldots$$

Anwendungshinweise

Strombasiert, dadurch Geheim- gleich Klartextlänge und nur Verschlüsselungsfunktion für Ver-/Entschlüsselung notwendig

Wertebereich des Counter muss ausreichend groß sein

nonce (number used once) ist Zufallszahl, die nach Nutzung des Counter Wertebereichs erneuert werden muss

Cipher Block Chaining (CBC) Modus

Standard (NIST SP 800-38A, 2001)

Funktionalität Sei iv eine nonce. Dann gilt:

$$c = c_0|c_1|\cdots = e(m_0 \oplus iv, k)|e(m_1 \oplus c_0, k)|\ldots \text{ bzw.}$$
$$m = m_0|m_1|\cdots = d(c_0, k) \oplus iv|d(c_1, k) \oplus c_0|\ldots$$

Anwendungshinweise

Geheimtexte mehrerer identischer Klartextblöcke sind i. A. nicht gleich

Klartextmuster im Geheimtext nicht sichtbar

Keine Wiederverwendung von *nonce* unter gleichem Schlüssel

Padding oracle Angriffe (Vaudenay, 2002), Padre[4]

[4] https://github.com/glebarez/padre, 28. Juni 2023

Fallstricke und Anwendungshinweise

- DES (FIPS-46-3, 1999) nicht verwenden
- ECB (NIST SP 800-38A, 2001) nicht verwenden
- PKCS#5[5] und ZeroByte-Padding (ISO/IEC 9797-1, ISO/IEC 10118-1) nicht verwenden

[5] https://www.rfc-editor.org/rfc/rfc1423, 28. Juni 2023

Zusammenfassung

Zusammenfassung

- Grundlegende Begriffe der symmetrischen Kryptographie definiert
- AES, PKCS#7, CTR und CBC vorgestellt

Weiterführende Literatur

Weiterführende Literatur

- *Kryptografie – Verfahren - Protokolle - Infrastrukturen*, Kapitel 8 und 10 von Schmeh (2016)
- *IT-Sicherheit – Konzepte - Verfahren - Protokolle*, Kapitel 7.5.5 von Eckert (2023)

Literatur I

- Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011).Biclique Cryptanalysis of the Full AES. *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*, 344–371 (siehe S. 28).
- Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg. (Siehe S. 36).
- Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., & Whiting, D. (2001).Improved Cryptanalysis of Rijndael. *Fast Software Encryption: 7th International Workshop, FSE 2000 New York, NY, USA, April 10–12, 2000 Proceedings*, 213–230 (siehe S. 28).
- FIPS-197. (2023). Federal Information Processing Standards Publication (FIPS 197). Advanced Encryption Standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf (siehe S. 18, 22–24).

Literatur II

- FIPS-46-3. (1999). Federal Information Processing Standards Publication (FIPS 46-3). Data Encryption Standard (DES). https://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (siehe S. 13, 32).
- Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A., & Schimmler, M. (2006).How to Break DES for € 8,980. *International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems — SHARCS'06, Cologne, Germany* (siehe S. 13).
- NIST SP 800-38A. (2001). NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation – Methods and Techniques. https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (siehe S. 30–32).
- Schmeh, K. (2016). *Kryptografie – Verfahren - Protokolle - Infrastrukturen* (6. Aufl.). dpunkt.verlag. (Siehe S. 6, 7, 9, 10, 16, 17, 27, 36).
- Shannon, C. (1949).Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715 (siehe S. 15).

Literatur III


Vaudenay, S. (2002).Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS .... *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, 534–546 (siehe S. 31).

Anhang
Algebraische Strukturen

Gruppen

Gruppe

Eine **Gruppe** $(G, \bullet, e)$ besteht aus einer Menge G, einer Operation $\bullet : G \times G \to G$ und einem Element $e \in G$, sodass folgende Axiome erfüllt sind:

G1 $(g \bullet h) \bullet k = g \bullet (h \bullet k)$ für alle $g, h, k \in G$ (**Assoziativgesetz**),

G2 $g \bullet e = e \bullet g = g$ für alle $g \in G$ (**Neutrales Element**) und

G3 Zu jedem $g \in G$ gibt es ein $h \in G$ mit $g \bullet h = h \bullet g = e$ (**Inverses Element**).

Gilt außerdem $g \bullet h = h \bullet g$ für alle $g, h \in G$, so heißt G **abelsch** oder **kommutativ**. Ist G endlich, so heißt $|G|$ die **Ordnung** der Gruppe G.

Ringe

Ring

Ein **Ring** $(R, +, 0, \cdot, 1)$ besteht aus einer Menge R, zwei Operationen $+ : R \times R \to R$ sowie $\cdot : R \times R \to R$ und zwei Elementen $0, 1 \in R$ mit $0 \neq 1$, sodass folgende Axiome erfüllt sind:

R1 $(R, +, 0)$ ist eine abelsche Gruppe,

R2 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in R$ ($\cdot$ ist assoziativ),

R3 $x \cdot 1 = 1 \cdot x = x$ für alle $x \in R$ (Einselement von $\cdot$) und

R4 $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$ (Distributivität).

Gilt außerdem $x \cdot y = y \cdot x$ für alle $x, y \in R$, so heißt R ein **kommutativer** Ring.

Körper und Galois-Körper

Körper

Ein **Körper** (eng. *field*) ist ein kommutativer Ring, in dem jedes Element außer der 0 invertierbar ist.

Galois-Körper

Ein **Galois-Körper** $\mathbb{F}_q$ ist ein Körper mit einer endlichen Anzahl $q = p^n$ von Elementen, wobei p eine Primzahl und $n \in \mathbb{N}$ sind. p heißt Charakteristik von $\mathbb{F}_q$.