

Zusammenfassung DC

Paul Lödige
Matrikel: 15405036

SoSe 2020

Inhaltsverzeichnis

1	Substitutionsverfahren	3
1.1	Skytale	3
1.2	Monoalphabetische Substitutionsverfahren	3
1.2.1	Caesar-Verschlüsselung	4
1.2.2	Häufigkeitsanalyse	4
1.3	Polyalphabetische Substitutionsverfahren	4
1.3.1	Vignère-Verfahren	4
1.3.2	One-Time-Pad	5
1.4	algebraische Substitutionsverfahren	5
1.4.1	Hill-Verfahren	5
2	Modulare Arithmetik	6
2.1	Exkurs: Division mit Rest	6
2.2	Der Ring \mathbb{Z}_n	6
2.2.1	Addition und Multiplikation	6
2.2.2	Subtraktion	7
2.2.3	Teiler, Vielfache	7
2.2.4	Kongruenz	7
2.2.5	Matrizen	7
2.3	Der erweiterte Euklid'sche Algorithmus	7
2.3.1	Euklid'scher Algorithmus	8
2.3.2	erweiterter Euklid'scher Algorithmus	8
2.4	Euler'sche φ -Funktion	9
2.4.1	φ -Funktion und Primzahlen	9
3	IT-Sicherheit: Gefährdungen und Maßnahmen	10
3.1	Vertraulichkeit	10
3.1.1	Schutzmaßnahmen: Verschlüsselungsverfahren	10
3.2	Integrität	10
3.2.1	Schutzmaßnahme: Hashfunktionen, Whitelists	11
3.3	Authenzität der Daten	11
3.3.1	Schutzmaßnahme: Signaturen	11
3.3.2	Schutz vor Replay-Angriffen	11
3.4	Authenzität von Nutzern	11
3.4.1	Schutzmaßnahmen	11
3.5	Zugriffskontrolle	11
3.5.1	Schutzmaßname: Zugriffskontrollsystem	12
3.6	Nichtabstreitbarkeit, Verbindlichkeit	12
3.6.1	Schutzmaßname: Signaturen und PKI	12
3.7	Verfügbarkeit	12
3.7.1	Schutzmaßnahmen	12
3.8	Anonymität	12

4	Verschlüsselungsverfahren	13
4.1	Das Kerckhoffs'sche Prinzip	13
4.2	Mathematische Modellierung von Verschlüsselungsverfahren	13
4.3	Schlüsselaustausch	13
4.4	Angriffsszenarien	14
4.4.1	Ciphertext-only Angriffe	14
4.4.2	Known-plaintext Angriffe	14
4.4.3	Chosen-plaintext Angriffe	14
4.5	Brute-Force Angriffe	14
4.5.1	Beispiel: Brute-Force Angriff auf k	14
4.5.2	Beispiel: Brute-Force Angriff auf m	14
4.5.3	Anforderungen zum Schutz vor Brute-Force	14
4.6	Wörterbuchangriffe	15
4.6.1	Schutz vor Wörterbuchangriffen	15
5	Stromverschlüsselungsverfahren	16
5.1	Synchrone Stromverschlüsselungsverfahren	16
5.2	Zustandsabhängige Stromverschlüsselungsverfahren	17
5.2.1	Additive zustandsabhängige Stromverschlüsselungsverfahren	18
5.3	Schlüsselstrom vs. One-Time-Pad	19
5.4	Nonces zur Initialisierung eines Schlüsselstromgenerators	19
5.5	ChaCha20	20
5.6	Cipher-Instanzen: Verschlüsselungsalgorithmen in Java-Laufzeitumgebungen	21
6	Blockverschlüsselungsverfahren	22
6.1	Padding-Verfahren	22
6.2	Betriebsmodi	22
6.2.1	ECB (Electronic Code Book)	22
6.2.2	CBC (Cipher Block Chaining)	23
6.2.3	CBC-CS (Ciphertext Stealing for CBC Mode)	24
6.2.4	CTR (Counter)	25
6.2.5	OFB (Output Feedback)	25
6.2.6	CFB (Cipher-Feedback)	26
6.3	Konstruktionsprinzipien von Blockverschlüsselungsverfahren	27
6.4	DES	27
6.4.1	Triple-DES (3DES)	27
6.5	Meet-in-the-Middle-Angriff	28
6.6	AES (Advanced Encryption Standard)	29
6.6.1	AES-128	29
7	Endliche Körper \mathbb{F}_{p^n}	31
7.1	Polynomdivision mit Rest	31
7.2	Berechnung der Inversen	31
7.3	\mathbb{F}_2	31
7.3.1	Irreduzible Polynome über \mathbb{F}_2	31

Kapitel 1

Substitutionsverfahren

1.1 Skytale

Ein Streifen wird um einen Stock gewickelt und dann beschrieben. Nach dem abwickeln erhält man den entsprechenden Code. Durch aufwickeln auf einen Stock mit dem gleichen Umfang lässt sich die Nachricht wieder entschlüsseln.



Tipp:

Zum entschlüsseln der Nachricht am PC ist der Editor mit automatischen Zeilen-Wrap gut geeignet

1.2 Monoalphabetische Substitutionsverfahren

Jeder Buchstabe wird bijektiv durch einen anderen Buchstaben des gleichen Alphabets ersetzt.

Alphabet:	$\mathcal{Z} := \{A, B, \dots, Z\}$
Schlüsselraum:	$\mathcal{K} := \{k : \mathcal{Z} \rightarrow \mathcal{Z} k \text{ ist bijektiv}\}$
Verschlüsselung von $z \in \mathcal{Z}$:	$k(z)$
Entschlüsselung:	$E(z) := k(z)$

1.2.1 Caesar-Verschlüsselung

Alle Buchstaben des Alphabets werden um einen konstanten Wert verschoben.

Beispiel:

Code: $n = 2$

Verschlüsselung: jeder Buchstabe wird durch den übernächsten Buchstaben im Alphabet ersetzt ($E(m) = (m + 3) \bmod 26$).

Entschlüsselung: jeder Buchstabe wird durch den vor-vorherigen Buchstaben ersetzt.

1.2.2 Häufigkeitsanalyse

Monoalphabetische Substitutionsverfahren lassen sich mit moderner Technik sehr einfach durch die Verwendung von Häufigkeitsanalysen entschlüsseln. In jeder Sprache gibt es Buchstaben die deutlich häufiger vorkommen als andere. Durch einer Analyse der Häufigkeit der einzelnen Buchstaben im Geheimtext lassen sich diese den Ausgangsbuchstaben zuordnen.

1.3 Polyalphabetische Substitutionsverfahren

Damit sich ein Geheimtext nicht durch eine Häufigkeitsanalyse (1.2.2) entschlüsseln lässt wird bei polyalphabetischen Verschlüsselungsverfahren der Schlüssel regelmäßig gewechselt. Hierbei wird der Schlüsselwechsel meist selbst durch ein Schlüsselwort kodiert.

1.3.1 Vignère-Verfahren

Alphabet: $\mathcal{Z} := \{A, B, \dots, Z\}$
Menge aller Wörter: $\mathcal{W} = \mathcal{Z}^{>0} := \bigcup_{n \in \mathbb{N}} \mathcal{Z}^n = \{(m_1, m_2, \dots, m_n) | m_i \in \mathcal{Z}, n \in \mathbb{N}\}$
Schlüsselraum: $\mathcal{K} := \Sigma_{\mathcal{Z}} \times \mathcal{W}$

Ein Schlüssel $k = (f, w) \in \mathcal{K}$ besteht aus einer Permutation $f \in \Sigma_{\mathcal{Z}}$ (siehe 1.2) und einem Schlüsselwort w .

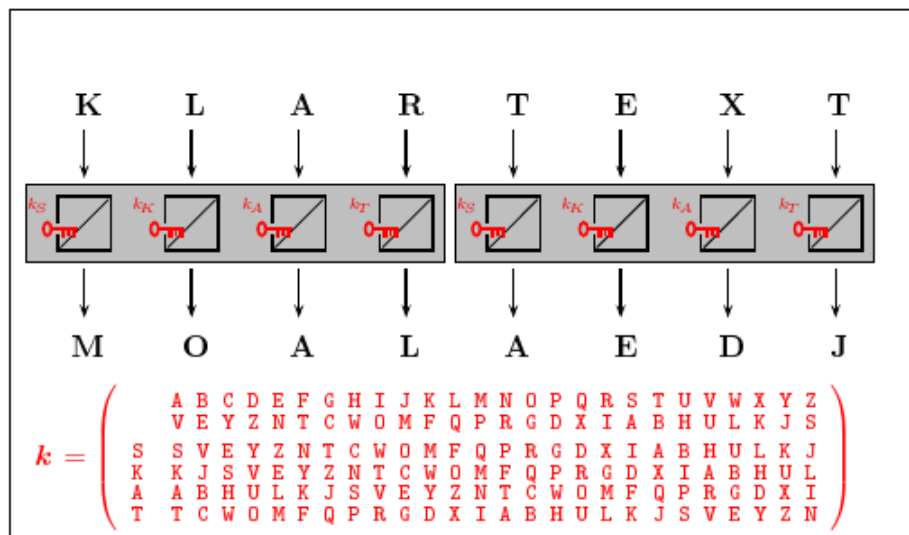
Das Vignère-Verfahren ist ein Blockverschlüsselungsverfahren, bei dem jeweils ein Block von Zeichen (im Beispiel 4) nach dem gleichen Verfahren verschlüsselt wird. Wenn die Blockgröße klein genug oder die Textlänge groß genug sind lässt sich ein solches Verfahren ebenfalls durch eine Häufigkeitsanalyse (siehe 1.2.2) knacken.

1.3.1.1 Verschlüsselung

Der Schlüssel f wird zyklisch mithilfe des Schlüsselwortes w verschoben.

Beispiel:

$f = \text{VEYZNTCWOMFQPRGDXIABHULKJS}$ und $w = \text{SKAT}$



1.3.2 One-Time-Pad

Bei dem One-Time-Pad handelt es sich um ein absolut sicheres Substitutionsverfahren (Nachrichten, bei denen sich Informationen von der Länge der Nachricht ableiten lassen müssen auf eine konstante Länge gebracht werden).

1.3.2.1 Verschlüsselung

Annahme:	Klar- und Geheimtext sind eine Folge von Zeichen der Menge $\mathcal{Z} = \mathbb{Z}$ ($n \in \mathbb{N}$)
Klartextnachricht:	$m = (m_1, m_2, \dots, m_l) \in \mathbb{Z}_n^l$
One-Time-Pad (zufällig):	$k = (k_1, k_2, \dots, k_l) \in \mathbb{Z}_n^l$
Geheimtext:	$E(m) := m + k := (m_1 + k_1, m_2 + k_2, \dots, m_l + k_l)$

1.3.2.2 Perfekte Sicherheit

Wenn die Zeichen k_i des Schlüssels mit einem perfekten Zufallsgenerator erzeugt lassen sich **keine** Rückschlüsse auf die Klartextnachricht ziehen (außer Länge).

Allerdings darf ein One-Time-Pad nur ein einziges Mal für die Verschlüsselung verwendet werden. Andernfalls könnte durch eine Berechnung der Differenz der mit dem gleichen OTP verschlüsselten Nachrichten Informationen gewonnen werden. So kann eine Häufigkeitsanalyse (siehe 1.2.2) oder sogar eine komplette Entschlüsselung (falls Klartext einer Nachricht bekannt ist) möglich werden.

1.4 algebraische Substitutionsverfahren

1.4.1 Hill-Verfahren

Das Hill-Verfahren ver- und entschlüsselt die Nachrichten mithilfe einer **invertierbaren** Matrix.

1.4.1.1 Verschlüsselung

Annahme:	$n, k \in \mathbb{N}$ sind vorgegeben
Klartextnachricht:	Menge von Blöcken $\mathcal{B} = \mathbb{Z}_n^k$
Schlüssel:	invertierbare (k, k) -Matrix K
Geheimtext:	$E_K(b) := K \cdot b \quad (b \in \mathcal{B})$

1.4.1.2 Entschlüsselung

Annahme:	gleiche Bedingungen wie bei der Verschlüsselung
Geheimtextnachricht:	Menge von Blöcken $\mathcal{C} = \mathbb{Z}_n^k$
Klartext:	$E_K(c) := K^{-1} \cdot c \quad (c \in \mathcal{C})$

Kapitel 2

Modulare Arithmetik

2.1 Exkurs: Division mit Rest

Für $a, b \in \mathbb{Z}, b \neq 0$ gibt es eindeutig bestimmte Element $q, r \in \mathbb{Z}, 0 \leq r < |b|$:

$$\begin{aligned}a &= b \cdot q + r \\a /_{\mathbb{Z}} b &:= q \\a \bmod b &:= r\end{aligned}$$

2.2 Der Ring \mathbb{Z}_n

Ein Ring \mathbb{Z}_n ist definiert durch:

$$\mathbb{Z}_n := 0, 1, \dots, n-1$$

2.2.1 Addition und Multiplikation

$$\begin{aligned}a +_{\mathbb{Z}_n} b &:= (a + b) \bmod n \\a \cdot_{\mathbb{Z}_n} b &:= (a \cdot b) \bmod n\end{aligned} \tag{2.1}$$

2.2.1.1 Inverse bezüglich der Addition

jedes $a \in \mathbb{Z}$ hat ein Inverses:

$$-a := \begin{cases} 0 & \text{für } a = 0 \\ n - a & \text{sonst} \end{cases}$$

2.2.1.2 Inverse bezüglich der Multiplikation

ein Element $a \in \mathbb{Z}_n$ ist (*multiplikativ*) *invertierbar*, falls es ein Element $b \in \mathbb{Z}_n$ gibt, für das gilt:

$$a \cdot b = 1$$

man schreibt auch:

$$a^{-1} := b$$

Die Menge der invertierbaren Elemente in \mathbb{Z}_n wird als \mathbb{Z}_n^* bezeichnet:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \cdot b = 1 \text{ für ein } b \in \mathbb{Z}_n\}$$

Zudem gilt, dass ein Element nur dann invertierbar ist, falls $\text{ggT}(a, n) = 1$:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\}$$

2.2.2 Subtraktion

Eine Subtraktion entspricht einer Addition mit der Inverse:

$$a -_{\mathbb{Z}_n} b := a +_{\mathbb{Z}_n} (-b) \mod n$$

2.2.3 Teiler, Vielfache

$b \in \mathbb{Z}$ teilt $a \in \mathbb{Z}$ falls ein $q \in \mathbb{Z}$ existiert mit:

$$a = b \cdot q$$

man schreibt auch $b|a$

2.2.3.1 Teilerregeln

1. $a|0 \forall a \in \mathbb{Z}$
2. $a|b \Leftrightarrow a|(-b)$
3. $a|b$ und $a|c \Rightarrow a|(b+c)$

2.2.4 Kongruenz

$a, b \in \mathbb{Z}$ sind *kongruent modulo n* , falls $n \in \mathbb{N} \setminus \{0\}$ und $n|(a-b)$. Man schreibt auch $a \equiv b$

2.2.5 Matrizen

2.2.5.1 Determinantenberechnung

Die Determinante $\det(A)$ der (N, N) -Matrix $A = (a_{ij})_{1 \leq i, j \leq N}$ (mit ganzzahligen Einträgen) über \mathbb{Z}_n wird definiert durch:

$$\det(A) \mod n = \det((a_{i,j} \mod n)_{1 \leq i, j \leq N})$$

Zudem gilt für die Matrizen $A = (a_{ij})_{1 \leq i, j \leq N}$ und $B = (b_{ij})_{1 \leq i, j \leq N}$ (mit ganzzahligen Einträgen):

$$\begin{aligned} \det(A \cdot B) \mod n &= (\det(A) \cdot \det(B)) \mod n \\ &= ((\det(A) \mod n) \cdot (\det(B) \mod n)) \mod n \\ &= (\det(A) \mod n) \cdot_{\mathbb{Z}_n} (\det(B) \mod n) \end{aligned}$$

2.2.5.2 Inverse Matrix

Die Inverse einer quadratischen Matrix A über \mathbb{Z}_n lässt sich mithilfe der Adjunkten berechnen:

$$A^{-1} = (\det(A))^{-1} \cdot \text{adj}(A)$$

Die Adjunkte lässt sich über \mathbb{Z}_n berechnen, da lediglich Summen und Differenzen von Produkten berechnet werden müssen.

2.3 Der erweiterte Euklid'sche Algorithmus

Der Euklid'sche Algorithmus ist ein sehr effizienter Weg den ggT zweier Zahlen zu ermitteln. Der Euklid'sche Algorithmus lässt sich auch über \mathbb{Z}_n verwenden. Man spricht dann von dem erweiterten Euklid'schen Algorithmus.

2.3.1 Euklid'scher Algorithmus

gegeben: $a_0, b_0 \in \mathbb{Z}$

1. $a := a_0$ und $b := b_0$
2. falls $b = 0$ gebe $|a|$ aus und beende
3. $r := a \bmod b$
4. $a := b$
5. $b := r$
6. goto 2.

2.3.2 erweiterter Euklid'scher Algorithmus

gegeben: $a_0, b_0 \in \mathbb{N}_0$

gesucht: $\alpha \cdot a_0 + \beta \cdot b_0 = g = ggT(a_0, b_0)$

1. $a := a_0, \alpha_a = 1, \beta_b = 0, b := b_0, \alpha_b := 0, \beta_b := 1$
2. falls $b = 0$ gebe $g := a, \alpha := \alpha_a$ und $\beta := \beta_a$ aus
3. $q := a /_{\mathbb{Z}} b$
4. $r := a - q \cdot b, \alpha_r := \alpha_a - q \cdot \alpha_b, \beta_r := \beta_a - q \cdot \beta_b$
5. $a := b, \alpha_a := \alpha_b, \beta_a := \beta_b$
6. $b := r, \alpha_b := \alpha_r, \beta_b := \beta_r$
7. goto 2.

2.3.2.1 Beispiel

Eingabe:

$$a_0 = 1224 \text{ und } b_0 = 156$$

Berechnung:

1224	156	a,b	q
1	0	1224	
0	1	156	7
1	-7	132	1
-1	8	24	5
6	-47	12	2
		0	

Ergebnis:

$$6 \cdot 1224 + (-47) \cdot 156 = 12$$

2.4 Euler'sche φ -Funktion

Die Euler'sche φ -Funktion bezeichnet die Anzahl invertierbarer Elemente in \mathbb{Z}_n

$$\varphi(n) := \begin{cases} |\mathbb{Z}_n^*| & \text{für } n \in \mathbb{N}, n \geq 2 \\ 1 & \text{für } n = 1 \end{cases}$$

Für $a, b \in \mathbb{N}$ mit $\text{ggT}(a, b) = 1$ gilt:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Zudem gilt für ein $n \in \mathbb{N}$ dessen Primzahlzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$:

$$\varphi(n) = n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

2.4.1 φ -Funktion und Primzahlen

für eine Primzahl p gilt:

$$\varphi(p) = p - 1$$

Für Primzahlpotenzen gilt zudem:

$$\varphi(p^e) = p^{e-1}(p - 1)$$

Kapitel 3

IT-Sicherheit: Gefährdungen und Maßnahmen

Im Folgenden wird auf mehrere Schutzziele eingegangen, welche für die IT-Sicherheit wichtig sind.

3.1 Vertraulichkeit

Bei dem Kriterium der Vertraulichkeit geht es darum, dass Daten nicht an unbefugte gelangt



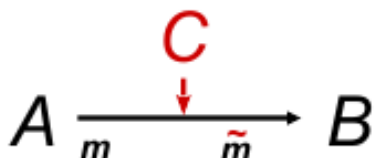
3.1.1 Schutzmaßnahmen: Verschlüsselungsverfahren

Durch die Verschlüsselung der Daten kann eine Gefährdungen der Vertraulichkeit verhindert werden. Allerdings muss hierbei auf folgende Punkte geachtet werden:

- Schlüsselerzeugung:
Schlüssel müssen mit einem kryptographisch sicheren Zufallsgenerator erzeugt werden
- Schlüsselspeicherung:
Schlüssel müssen sicher gespeichert sein
- Schlüsselaustausch:
Damit zwei Systeme Informationen austauschen können müssen zunächst Schlüssel ausgetauscht werden. Bei synchronen Verschlüsselungsverfahren muss dieser Austausch auf einem sicheren Weg geschehen.

3.2 Integrität

Bei dem Kriterium der Integrität geht es darum, dass die Daten, die verschickt werden auch unverändert empfangen werden.

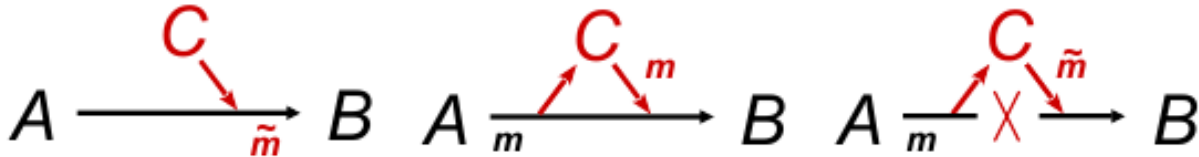


3.2.1 Schutzmaßnahme: Hashfunktionen, Whitelists

zur Sicherung der Integrität werden mithilfe von Hashfunktionen Prüfsummen errechnet und in einer Whitelist abgespeichert.

3.3 Authentizität der Daten

Bei dem Kriterium der Authentizität geht es darum, sicherzustellen, dass die empfangenen Daten auch tatsächlich vom angegebenen Absender stammen.



3.3.1 Schutzmaßnahme: Signaturen

Um die Authentizität sicherzustellen gibt es mehrere Möglichkeiten:

1. es wird ein zweiter Kommunikationsweg für die Authentifikation verwendet (2-Factor-Authentication)
2. **Signaturverfahren:**
Eine Signatur wird (mit dem Signaturverfahren S) berechnet und mithilfe eines privaten Schlüssels k_{pri} verschlüsselt. Der Empfänger nutzt den öffentlichen Schlüssel k_{pub} und das zu S gehörigen Verifikationsverfahren V um die Nachricht zu authentifizieren.
3. **MAC-Verfahren:**
Sender und Empfänger einigen sich auf einen geheimen Schlüssel k . Anschließend nutzt der Sender diesen Schlüssel um den MAC(Message Authentication Code)-Wert der Nachricht zu verschlüsseln. Wenn der Empfänger den MAC-Wert entschlüsselt kann er die Nachricht authentifizieren.

3.3.2 Schutz vor Replay-Angriffen

Um einen Replay-Angriff zu verhindern muss dafür gesorgt werden, dass jede Nachricht nur ein einziges Mal akzeptiert wird. Mögliche Verfahren hierfür sind Zählwerte, die mit jeder Nachricht inkrementiert werden oder Zeitstempel.

3.4 Authentizität von Nutzern

In vielen Fällen ist es nötig einen Nutzer zu authentifizieren (z.B. Anmeldung auf einer Webseite). Diese Authentifikation ist eine spezielle Form der Nachrichtenauthentifikation, bei der der Inhalt der übertragenen Daten nicht relevant ist.

3.4.1 Schutzmaßnahmen

- Nutzen eines gemeinsamen Geheimnisses (z.B. WLAN-Passwort)
- Nutzen eines Schlüssels, den nur eine Seite besitzt (siehe 3.3.1)
- Nutzen von einmaligen Eigenschaften (z.B. Fingerabdruck)

3.5 Zugriffskontrolle

Bei Systemen, die eine Aktion ausführen ist es wichtig abzusichern, dass nur erlaubte Aktionen angefragt werden können.

3.5.1 Schutzmaßname: Zugriffskontrollsystem

Es werden Listen (Access Control Lists) darüber geführt, welcher Nutzer welche Aktionen veranlassen darf. Hierbei werden die Rechte häufig in Form von Rollen vergeben (Role Based Access Control).

3.6 Nichtabstreitbarkeit, Verbindlichkeit

Eine Form der Authentifikation oder Authentifizierung, die auch gegenüber dritten unwiderlegbar ist. Dies ist vor allem für Kommunikationen wichtig, bei denen es für eine Partei vorteilhaft wäre sie abzustreiten (z.B. Verträge).

3.6.1 Schutzmaßname: Signaturen und PKI

Signaturen (siehe 3.3.1) können auch als Beweis für die Nichtabstreitbarkeit verwendet werden, falls der öffentliche Schlüssel der dritten Partei bekannt ist. Hierfür wird eine öffentliche Infrastruktur (Public Key Infrastruktur), welche von Zertifizierungsstellen zur Verfügung gestellt wird (z.B. ITU (für X.509)).

3.7 Verfügbarkeit

Bei dem Kriterium der Verfügbarkeit geht es darum, dass die Daten und IT-Systeme wie angedacht erreichbar sind. Mögliche Bedrohungsszenarien hierfür sind:

- Datenverlust durch defekte Daten
- Datenverlust durch Schadsoftware
- Nichterreichbarkeit von Diensten aufgrund von Netzwerkproblemen
- Nichterreichbarkeit von Webdiensten aufgrund erfolgreicher Denial-of-Service-Angriffen

3.7.1 Schutzmaßnahmen

- redundante örtlich verteilte Datenspeicherung
- Virens Scanner und Paketfilter zum Schutz vor Malware
- Firewalls

3.8 Anonymität

Es gibt viele Gründe, wegen denen es sinnvoll ist, dass eine Datenübertragung sicher aber ohne den Versand persönlicher Daten funktioniert.

Kapitel 4

Verschlüsselungsverfahren

4.1 Das Kerckhoffs'sche Prinzip

„Ein Verschlüsselungssystem darf nicht der Geheimhaltung bedürfen und soll ohne Schaden in Feindeshand fallen können.“

Folglich ist für die Entschlüsselung der Nachricht nicht die Kenntnis über das Verfahren, sondern der Schlüssel die relevante Information.

„Es soll nicht möglich sein, einen Geheimtext ohne Kenntnis des hierfür vorgesehenen Schlüssels **effizient** zu entschlüsseln.“

4.2 Mathematische Modellierung von Verschlüsselungsverfahren

Klartextnachrichten und Geheimtextnachrichten sind Elemente einer Menge \mathcal{M} .

Schlüssel sind Elemente einer Menge \mathcal{K} , die als Schlüsselraum bezeichnet wird.

Die Verschlüsselungsverfahren bestehen aus einem Paar von Funktionen zur Verschlüsselung (E) und Entschlüsselung (D):

$$E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$$

$$D : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$$

Hierbei sind die definierten Abbildungen bijektiv ($D_k := E_k^{-1}$):

$$E_k : \mathcal{M} \rightarrow \mathcal{M}, E_k(m) := E(k, m)$$

$$D_k : \mathcal{M} \rightarrow \mathcal{M}, D_k(m) := D(k, m)$$

Die Nachrichtenmenge \mathcal{M} besteht in Realität aus einer endlichen Folgen (Tupeln) von Bit- oder Bytewerten. Diese können entweder die gleiche Länge besitzen (Blockverschlüsselung) oder von beliebiger Länge sein (Stromverschlüsselung).

$$\mathcal{M} = \mathcal{Z}^n = \{(z_1, z_2, \dots, z_n) \mid z_i \in \mathcal{Z}\} \text{ für ein festes } n \in \mathbb{N} \text{ (Blockverschlüsselung)}$$

$$\mathcal{M} = \mathcal{Z}^{>0} = \bigcup_{n \in \mathbb{N}} \mathcal{Z}^n = \{(z_1, z_2, \dots, z_n) \mid z_i \in \mathcal{Z}, n \in \mathbb{N}\} \text{ (Stromverschlüsselung)}$$

4.3 Schlüsselaustausch

Um mithilfe eines symmetrischen Schlüssels Daten austauschen zu können muss der Schlüssel auf eine Sichere Art und Weise ausgetauscht werden. Dies ist zwar offline möglich, stellt allerdings kein praktikables Verfahren für die Kommunikation im Internet dar. Daher werden für einen sicheren Schlüsselaustausch über eine unsichere Infrastruktur asymmetrische Verschlüsselungsverfahren benötigt.

4.4 Angriffsszenarien

Da für eine effiziente Entschlüsselung einer Geheimtextnachrichten die Kenntnis des Schlüssels essentiell ist, versuchen die meisten Angriffe diesen herauszufinden.

4.4.1 Ciphertext-only Angriffe

Vorraussetzung: ein oder mehrere Geheimtexte $c_i = E_k(m_i)$ bekannt

Angriffsziel: Bestimmung von m oder von k

4.4.2 Known-plaintext Angriffe

Vorraussetzung: Geheimtext $c = E_k(m)$ und eine Reihe von bekannten Paaren $(m_i, E_k(m_i))$ sind bekannt

Angriffsziel: Bestimmung von m oder von k

4.4.3 Chosen-plaintext Angriffe

Vorraussetzung: Geheimtext $c = E_k(m)$ und für eine Reihe von beliebig vorgegebenen Klartextnachrichten m_i kann

Angriffsziel: Bestimmung von m oder von k

4.5 Brute-Force Angriffe

Da die Vorraussetzung für ein gutes Verschlüsselungsverfahren ist, dass es nicht **effizient** entschlüsselt werden kann (siehe 4.1) muss die **Effizienz** definiert sein. An dieser Stelle setzen Brute-Force Angriffe an. Sie versuchen wie der Name schon sagt mit roher Rechenleistung den Schlüssel zu ermitteln.

4.5.1 Beispiel: Brute-Force Angriff auf k

Unter der Annahme, dass ein known-plaintext Angriff (siehe 4.4.2) vorliegt lässt sich der Schlüssel bestimmen, indem alle möglichen Schlüssel k des Schlüsselraums \mathcal{K} „ausprobiert“ werden. Hierbei können für die einzelnen bekannten Klartextnachrichten mehrere Schlüssel passen:

$$\mathcal{K}_i := \{\tilde{k} \in \mathcal{K} \mid E_{\tilde{k}}(m_i) = c_i\}$$

Bei einer ausreichenden Menge bekannter Klartextnachrichten lässt sich der Schlüssel aus der Schnittmenge der möglichen Schlüssel bestimmen:

$$\bigcap_{i=1}^N \mathcal{K}_i = \{k\}$$

4.5.2 Beispiel: Brute-Force Angriff auf m

Liegen die Vorraussetzungen für einen chosen-plaintext Angriff vor, so kann die Klartextnachrichten herausgefunden werden, indem alle möglichen Klartextnachrichten $\tilde{m} \in \mathcal{M}$ „ausprobiert“ werden:

$$E_k(\tilde{m}) = c = E_k(m) \implies \tilde{m} = m$$

4.5.3 Anforderungen zum Schutz vor Brute-Force

1. Es soll keinen Angriff auf den Schlüssel k geben, der durchschnittlich weniger als $\frac{|\mathcal{K}|}{2}$ Ver- oder Entschlüsselungsoperationen braucht.
2. Es soll keinen Angriff auf die Klartextnachricht m geben, der durchschnittlich weniger als $\min\left\{\frac{|\mathcal{K}|}{2}, \frac{|\mathcal{M}|}{2}\right\}$ Ver- oder Entschlüsselungsoperationen braucht.

4.6 Wörterbuchangriffe

Nachrichtenpaare (Geheim- und Klartext), die mithilfe eines Schlüssels k verschlüsselt wurden können in einem Wörterbuch abgespeichert werden. Mithilfe des Wörterbuchs können diese Paare jederzeit entschlüsselt werden. Zudem kann für einen chosen-plaintext Angriff (siehe 4.4.3) ein Wörterbuch mit häufig vorkommenden Wörtern erstellt werden, sodass eine Entschlüsselung in wesentlich kürzerer Zeit möglich wird.

4.6.1 Schutz vor Wörterbuchangriffen

Um einem Wörterbuchangriff vorzubeugen ist es wichtig, dass sich der Geheimtext bei jeder Verschlüsselung des gleichen Klartextes unterscheidet. Dies wird meist dadurch erreicht, dass die Klartextnachricht vor Anwendung des Verschlüsselungsverfahrens abgeändert wird. Meist wird hierfür eine Nonce (Number used Once) verwendet. Die Nonce kann ein Zähler, ein Zeitstempel oder eine Zufallszahl sein. Der Nonce-Wert muss beiden Seiten bekannt sein. Hierbei kann er entweder mitverschlüsselt übertragen werden oder besteht aus einem Wert (z.B. Zähler), der beiden Seiten bekannt ist.

4.6.1.1 Nonce-Verschlüsselung

Ein Nonce-Wert $v \in \mathcal{M}$ wird dazu genutzt die Klartextnachricht $m \in \mathcal{M}$ abzuändern:

$$\tilde{m} = m + v$$

Anschließend wird die veränderte Nachricht verschlüsselt:

$$c = E_k(\tilde{m})$$

Für die Entschlüsselung wird der Schlüssel k und der Nonce-Wert v benötigt:

$$m = D_k(c) + v$$

Kapitel 5

Stromverschlüsselungsverfahren

Bei einem Stromverschlüsselungsverfahren wird eine Nachricht zeichenweise verschlüsselt. Die Menge der verschlüsselten Zeichen \mathcal{M} ist als endliche Folge von Elementen einer Zeichenmenge \mathcal{Z} definiert.

$$\mathcal{M} = \mathcal{Z}^{>0} := \bigcup_{l \in \mathbb{N}} \mathcal{Z}^l = \{(m_1, m_2, \dots, m_l) \mid m_i \in \mathcal{Z}, l \in \mathbb{N}\}$$

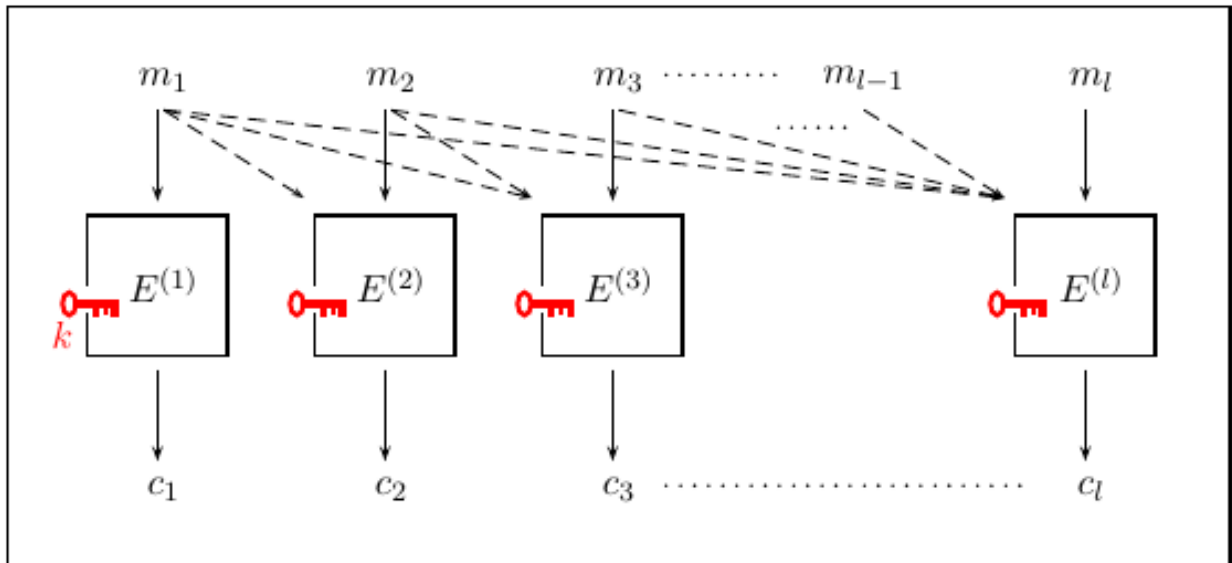
Die Verschlüsselungsfunktion E_k lässt sich zeichenweise beschreiben:

$$E^{(i)} : \mathcal{K} \times \mathcal{Z}^i \rightarrow \mathcal{Z}^i \text{ für alle } i \in \mathbb{N}$$

mit:

$$E_k((m_1, m_2, \dots, m_l)) = (E^{(1)}(k, (m_1)), E^{(2)}(k, (m_1, m_2)), \dots, E^{(l)}(k, (m_1, m_2, \dots, m_l)))$$

Bei manchen Verfahren können bei der Berechnung des i -ten Geheimtextzeichens $c_i = E^{(i)}(k, (m_1, m_2, \dots, m_i))$ auch die vorherigen Zeichen miteinfließen.



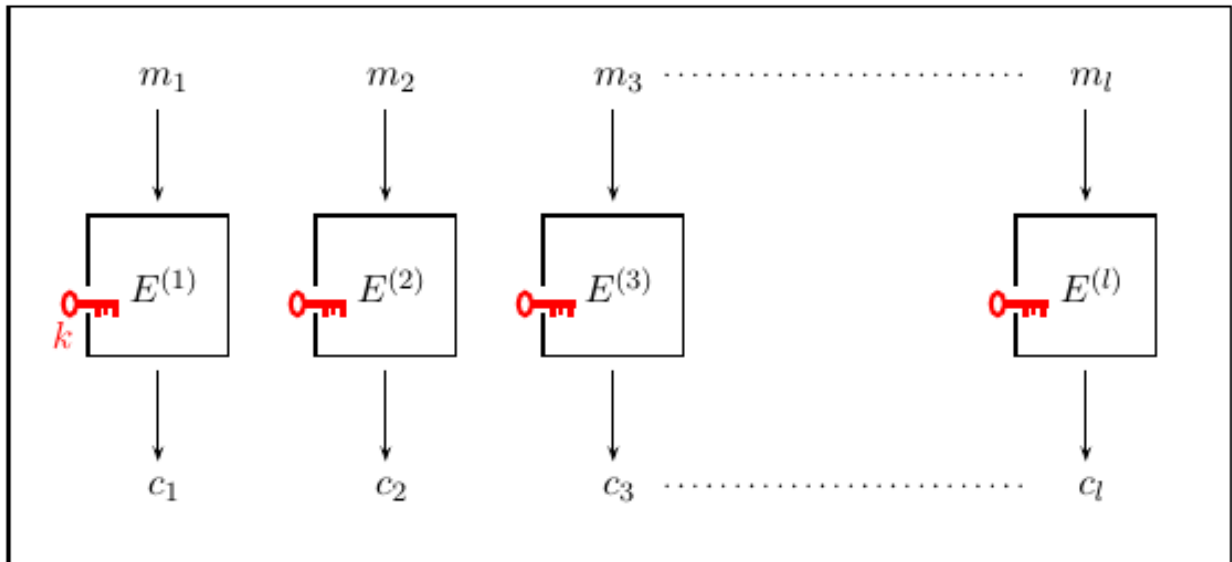
5.1 Synchrone Stromverschlüsselungsverfahren

Bei synchronen Stromverschlüsselungsverfahren hängen die Zeichen einer Geheimtextnachricht nicht von den vorherigen ab. So ist es möglich die einzelnen Zeichen des Klartextes gleichzeitig (synchron) zu verschlüsseln. Ein Beispiel hierfür sind monoalphabetische Verschlüsselungsverfahren (siehe 1.2).

$$E^{(i)} : \mathcal{K} \times \mathcal{Z} \rightarrow \mathcal{Z}$$

wobei gelten muss:

$$E_k((m_1, m_2, \dots, m_l)) = (E^{(1)}(k, m_1), E^{(2)}(k, m_2), \dots, E^{(l)}(k, m_l))$$



5.2 Zustandsabhängige Stromverschlüsselungsverfahren

Bei einer zustandsabhängigen Stromverschlüsselung werden die Zeichen mithilfe eines Zustands verschlüsselt, der sich abhängig vom vorherigen Zeichen ändert. Hierzu werden benötigt:

\mathcal{S} : Menge der Zustände

$s_0 : \mathcal{K} \rightarrow \mathcal{S}$

$s : \mathcal{S} \times \mathcal{Z} \rightarrow \mathcal{S}$

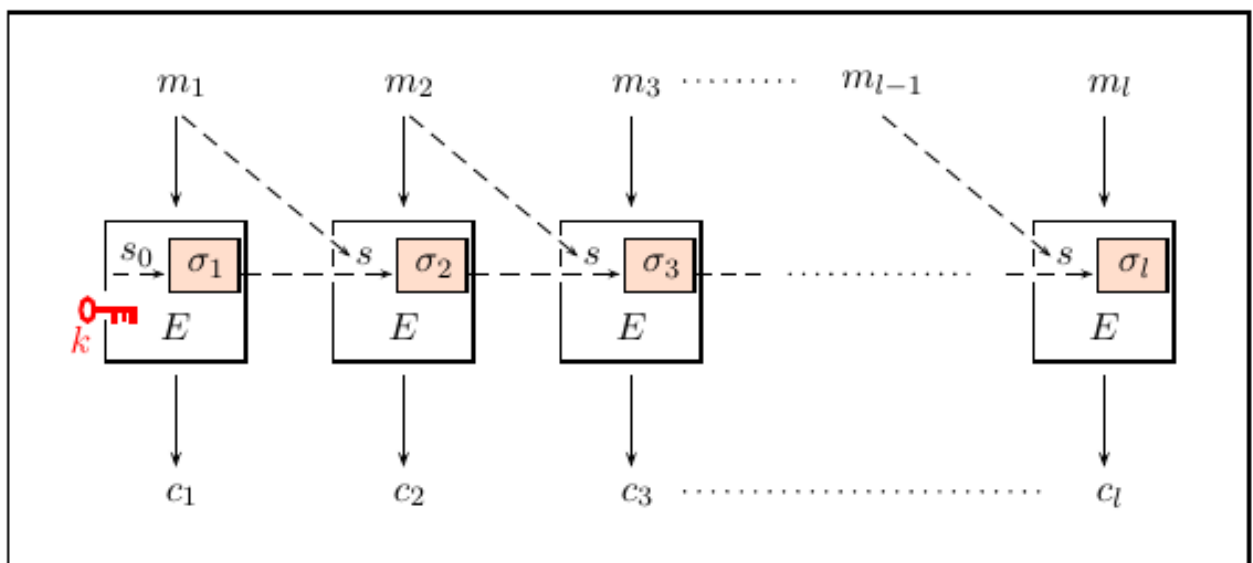
$E : \mathcal{S} \times \mathcal{Z} \rightarrow \mathcal{Z}$ (bijektiv)

Mithilfe von s_0 und einem Schlüssel k wird ein Startzustand $\sigma_1 := s_0(k)$ festgelegt. Die folgenden Zustände σ_i werden mithilfe der Abbildung s errechnet:

$$\sigma_i := s(\sigma_{i-1}, m_{i-1})$$

Die einzelnen Zeichen lassen sich dann mithilfe von E in Abhängigkeit von dem jeweiligen Zustand bestimmen:

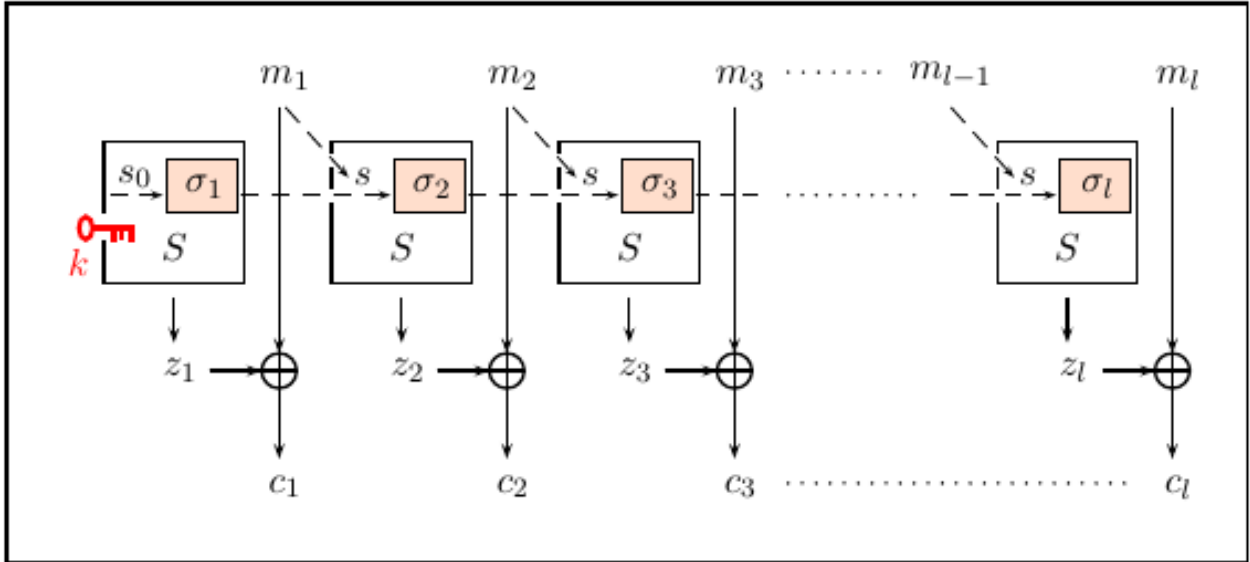
$$c_l := E(\sigma_l, m_l)$$



5.2.1 Additive zustandsabhängige Stromverschlüsselungsverfahren

Additive zustandsabhängige Stromverschlüsselungsverfahren sind zustandsabhängige Stromverschlüsselungsverfahren, mit einer Funktion $S : \mathcal{S} \rightarrow \mathcal{Z}$. Die Verschlüsselungsfunktion ist hierbei durch $E(\sigma, m) = S(\sigma) + m$ definiert, wobei hierbei eine modulare Addition (siehe 2.2.1) über \mathcal{Z} stattfindet. s_0, s und S bilden den Schlüsselstromgenerator, der den folgenden Schlüsselstrom erzeugt:

$$z_i := S(\sigma_i) = S(s(\sigma_{i-1}, m_{i-1}))$$



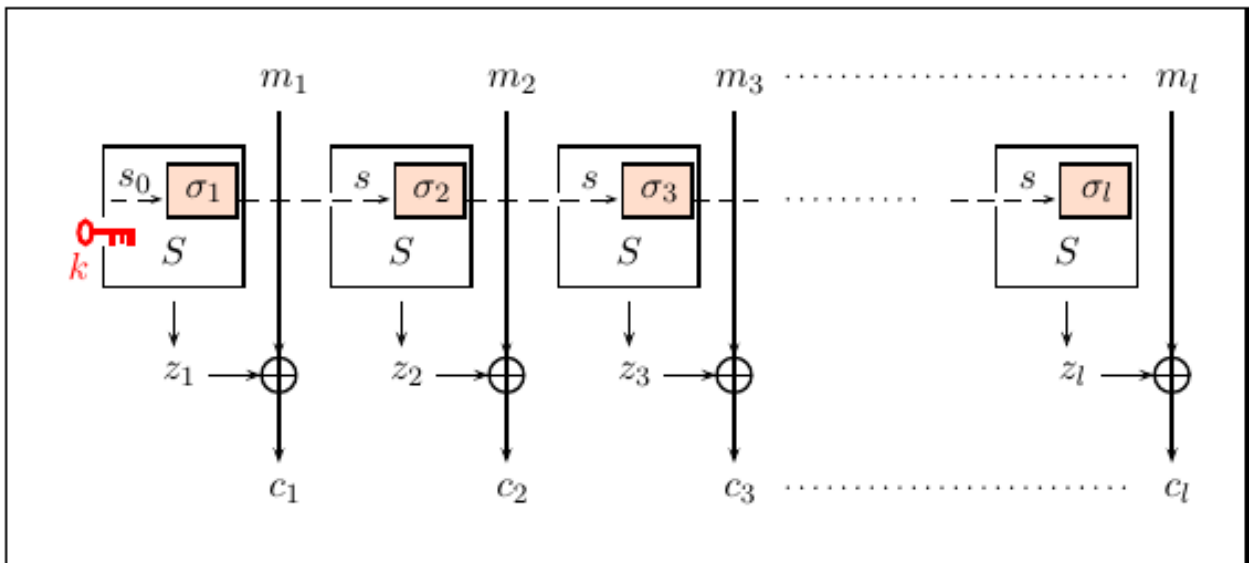
5.2.1.1 Synchrone additive Stromverschlüsselungsverfahren

eine additive Stromverschlüsselung lässt sich synchron durchführen, falls die Übergangsfunktion s nicht von den Zeichen des Klartextes abhängt.

$$\sigma_{i+1} = s(\sigma_i) \text{ mit } s : \mathcal{S} \rightarrow \mathcal{S}$$

Hierdurch definiert sich der Schlüsselstrom:

$$z_i = S(s^{i-1}(s_0(k))) \quad (i \in \mathbb{N})$$



5.3 Schlüsselstrom vs. One-Time-Pad

Ein One-Time-Pad (siehe 1.3.2) ist eine spezielle Form einer additiven Stromverschlüsselung, wobei die Schlüsselstromzeichen $S\sigma_i$ direkt aus dem Schlüssel k entnommen werden. Aufgrund dieser Tatsache kann ein Schlüsselstrom als Ersatz für ein One-Time-Pad betrachtet werden. Hierbei ist allerdings darauf zu achten, dass folgende Bedingungen erfüllt sind:

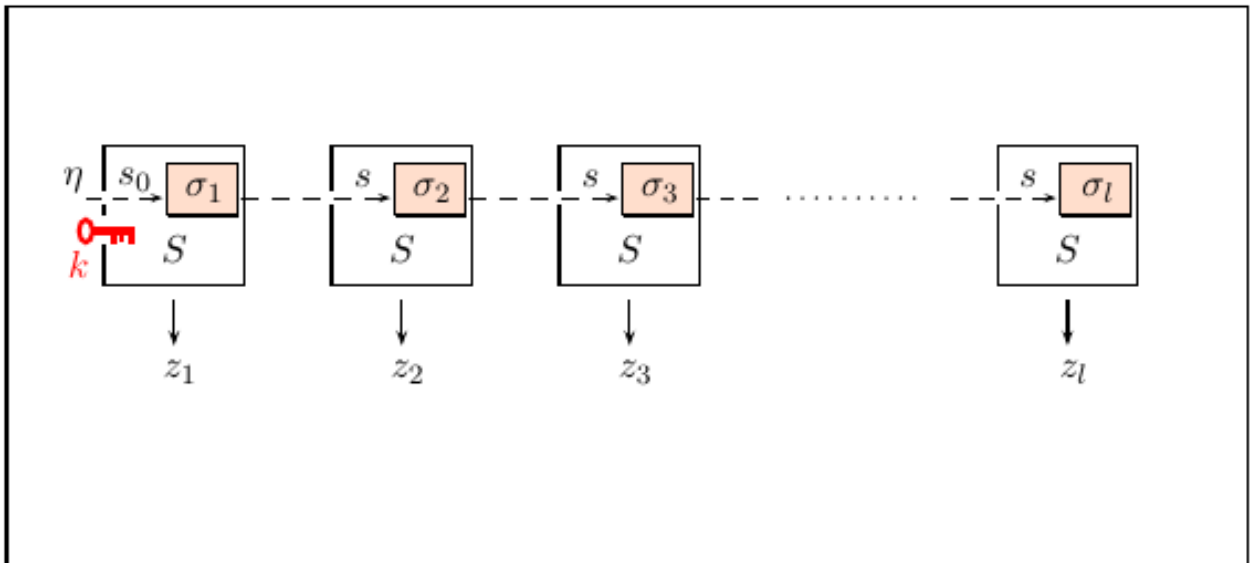
- Schlüsselstromzeichen dürfen keinen Aufschluss über die nachfolgenden Zeichen geben
 - Schlüsselstromzeichen müssen statistisch gleichverteilt und unkorreliert sein
 - ein Schlüssel $k \in \mathcal{K}$ dient gut zur Initialisierung eines Pseudozufallsgenerators
- die Bestimmung des Schlüssels k darf nicht effizienter als mit einer Brute-Force-Suche (siehe 4.5) im Schlüsselraum \mathcal{K} möglich sein.

5.4 Nonces zur Initialisierung eines Schlüsselstromgenerators

Wie bei einem One-Time-Pad (siehe 1.3.2) sollte ein Schlüsselstrom nur einmalig verwendet werden. Da der Austausch von Schlüsseln bei synchronen Verschlüsselungsverfahren allerdings sehr aufwendig ist, wird versucht den Schlüssel weiter zu verwenden. Hierfür gibt es mehrere Möglichkeiten:

- Der Schlüsselstrom wird nicht neu initialisiert und durchgehend weiterverwendet (Schlüsselstrom muss zwischen Sender und Empfänger synchron bleiben).
- Der verwendete Schlüssel wird durch einen Nonce-Wert η_m verändert.
 - η_m muss mit übertragen werden und zwischen Sender und Empfänger synchron gehalten werden
 - Der Schlüsselraum wird kleiner, da er sich in einen Raum \mathcal{K}_{eff} , in dem k liegt und einen Bereich \mathcal{N} für den Nonce-Wert aufteilt
- Die Funktion s_0 (siehe 5.2) wird so erweitert, dass sowohl Werte aus \mathcal{K} , als auch aus \mathcal{N} einfließen:

$$s_0 : \mathcal{K} \times \mathcal{N} \rightarrow \mathcal{S}$$



5.5 ChaCha20

Der ChaCha20-Schlüsselstromgenerator nutzt für die Initialisierung des Zustands s_0 einen Schlüsselwert $k \in \mathcal{K}$ und einen Nonce-Wert $\eta \in \mathcal{N}$. Für die Beschreibung des Algorithmus werden die folgenden Mengen benötigt:

$$\begin{aligned} (\text{byte-basiert}) \quad \mathcal{Z} &= \mathbb{Z}_{2^8} \\ (\text{int-basiert}) \quad \mathcal{K} &= (\mathbb{Z}_{2^{32}})^8 \\ (\text{int-basiert}) \quad \mathcal{S} &= (\mathbb{Z}_{2^{32}})^{16} \times (\mathbb{Z}_{2^{32}})^{16} \times \mathbb{Z}_{2^{38}+1} \\ (\text{int-basiert}) \quad \mathcal{N} &= (\mathbb{Z}_{2^{32}})^3 \end{aligned}$$

Elemente im Zustandsraum \mathcal{S} bestehen aus 3-Tupeln:

$$(s^0, s, c) = (\mathbb{Z}_{2^{32}})^{16} \times (\mathbb{Z}_{2^{32}})^{16} \times \mathbb{Z}_{2^{38}+1}$$

In s^0 werden der Schlüssel k und der Nonce-Wert η mit fest definierten Konstanten nach der Initialisierung abgespeichert. Bei der Initialisierung und nach Ausgabe von jeweils 64 Bytes wird der Wert von s^0 nach s kopiert und in einen Block von 64 Schlüsselstrombytes überführt. c speichert die Anzahl der bereits verwendeten Schlüsselstrombytes (nach Spezifikation max. 2^{38} Bytes)

Initialisierung:

$$s_0 : \mathcal{K} \times \mathcal{N} \rightarrow \mathcal{S}$$

daraus ergibt sich:

$$\begin{aligned} s_0((k, \eta)) &= s_0(((k_1, \dots, k_8), (n_1, n_2, n_3))) \\ &:= s(((c_1, c_2, c_3, c_4, k_1, \dots, k_8, 0, n_1, n_2, n_3), (0, \dots, 0), 0)) \\ &= s((s^0, 0, 0)) \end{aligned}$$

wobei c_i die folgende Konstanten sind:

$$\begin{aligned} c_1 &= 0x61707865 \\ c_2 &= 0x3320646e \\ c_3 &= 0x79622d32 \\ c_4 &= 0x6b206574 \end{aligned}$$

und

$$s^0 := (c_1, c_2, c_3, c_4, k_1, \dots, k_8, 0, n_1, n_2, n_3)$$

Update-Funktion: $s : \mathcal{S} \rightarrow \mathcal{S}$

Solange $c < 2^{38}$ gilt:

$$s((s^i, s, c)) := \begin{cases} (s^i, s, c+1) & \text{falls } c \bmod 64 \neq 0 \\ (s^{i+1}, s^i \oplus f_{ib}^{10}(s^i), c+1) & \text{falls } c \bmod 64 = 0 \end{cases}$$

f_{ib} wird 10 mal wiederholt und bildet die folgende Abbildung:

$$f_{ib} : (\mathbb{Z}_{2^{32}})^{16} \rightarrow (\mathbb{Z}_{2^{32}})^{16}$$

Die Funktion ist in RFC 8439 definiert.

Extraktion der Schlüsselstromzeichen: $S; \mathcal{S} \rightarrow \mathcal{S}$

Mit der Funktion S werden die Bytewerte, aus denen die Zahlen s_0, s_1, \dots, s_{15} der zweiten Komponente eines Elements aus \mathcal{S} zusammengesetzt sind, extrahiert:

Für

$$(s^0, s, c) = (s^0, (s_0, s_1, \dots, s_{15}), c) \in \mathcal{S}$$

werden Hierzu

$$\begin{aligned} i &= \lfloor c/4 \rfloor \bmod 16 \\ j &= c \bmod 4 \end{aligned}$$

berechnet und

$$S((s^0, (s_0, s_1, \dots, s_{15}), c)) := \lfloor \frac{s_i}{2^{8j}} \rfloor \bmod 2^8$$

gesetzt.

5.6 Cipher-Instanzen: Verschlüsselungsalgorithmen in Java-Laufzeitumgebung

siehe Skript2 1.5 (Seite 19).

Kapitel 6

Blockverschlüsselungsverfahren

Ein Verschlüsselungsverfahren wird als Blockverschlüsselungsverfahren bezeichnet, wenn die Menge der Nachrichten \mathcal{M} durch die Menge der Blöcke einer festen Länge $n \in \mathbb{N}$ gegeben ist:

$$\mathcal{M} := (\mathbb{Z}_2^8)^n = \{(z_1, z_2, \dots, z_n) \mid z_i \in \mathbb{Z}_2^8\}$$

Wichtig

- Häufig wird für Blöcke die aus n Bytewerten die Blocklänge in Bits (Blocklänge = $n \cdot 8$) angegeben
- Die Menge der Blöcke \mathcal{M} kann als Vektorraum über \mathbb{Z}_2 aufgefasst werden. Hierbei wird die Summe von zwei Blöcken $m_1, m_2 \in \mathcal{M}$ durch eine bitweise Addition definiert, welcher einer Bitweisen XOR-Verknüpfung (\oplus) entspricht.
- Da sich die Vektoren aus \mathbb{Z}_2^{8n} in Zahlen aus $\mathbb{Z}_{2^{8n}}$ umrechnen lassen könnte man sie auch auf diese Art addieren. Hierbei erhält man allerdings ein deutlich anderes Ergebnis als bei XOR-Addition. Aus diesem Grund wird in diesem Fall das Symbol \boxplus verwendet.

6.1 Padding-Verfahren

Damit Daten beliebiger Länge mit einem Blockverschlüsselungsverfahren verschlüsselt werden können muss die Nachricht auf ein Vielfaches der Blocklänge aufgestockt werden. Man spricht von Padding. Um dem Empfänger mitzuteilen, welche übertragenen Daten zum Padding und nicht zur Nachricht gehören gibt es mehrere Möglichkeiten:

- Die Anzahl der Padding-Bytes wird mit übertragen
- Als Paddingbytes werden Zeichen verwendet, die nicht in die Kodierung passen (z.B. 0x00 bei ASCII)
- Es findet immer Padding statt (bei passender Nachrichtenlänge ist der ganze letzte Block Padding), wobei im Padding die Paddinglänge kodiert ist.

6.2 Betriebsmodi

Es gibt eine Vielzahl von Betriebsmodi, die für die Blockverschlüsselung verwendet werden. Auf diese wird im Folgenden eingegangen

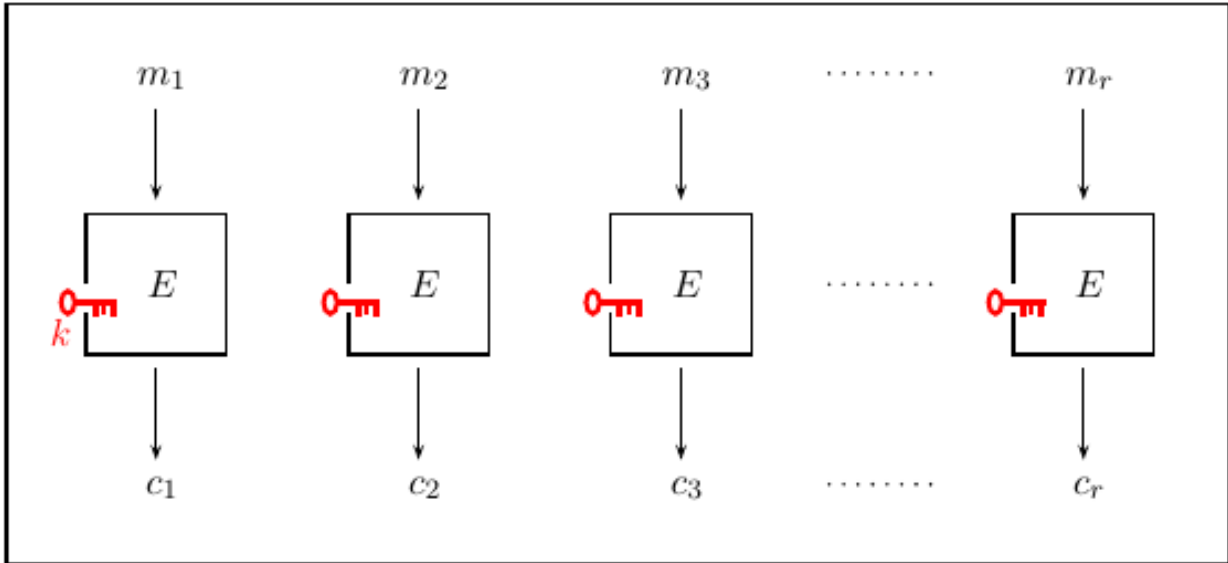
6.2.1 ECB (Electronic Code Book)

Im ECB-Modus wird mit dem Verschlüsselungsverfahren E jedes Tupel von Blöcken blockweise verschlüsselt:

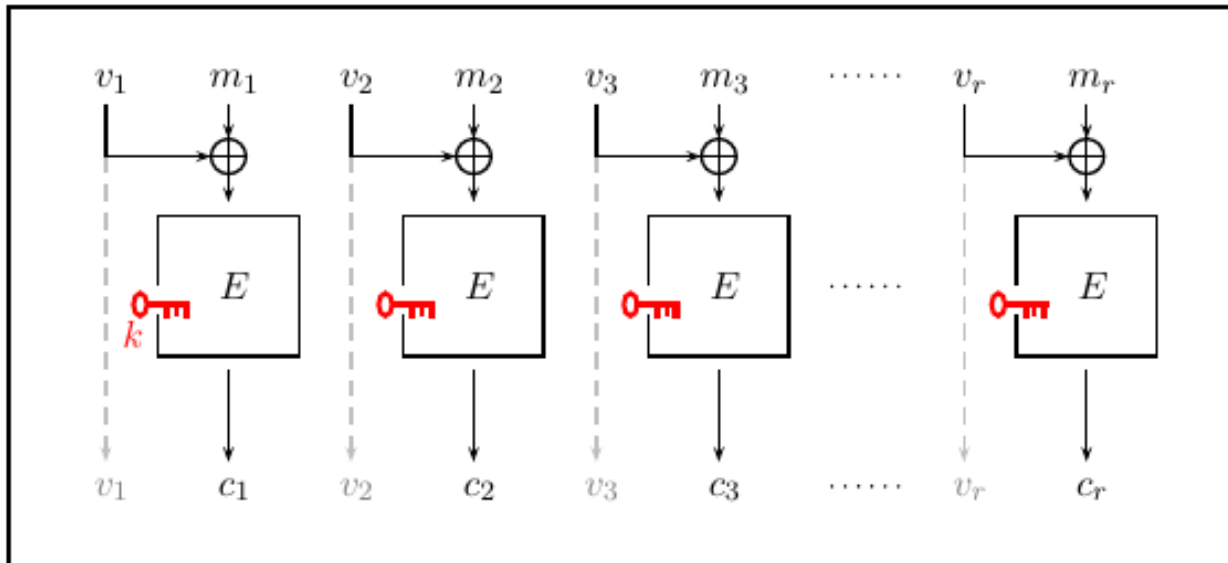
$$E_k((m_1, \dots, m_r)) := (E_k(m_1), \dots, E_k(m_r))$$

eine auf diese Weise verschlüsselte Nachricht kann ebenfalls Blockweise entschlüsselt werden:

$$D_k((c_1, \dots, c_r)) := (D_k(c_1), \dots, D_k(c_r))$$



Da diese Modus anfällig für Wörterbuchangriffe ist wird häufig ein Nonce-Wert verwendet, der jeweils mit dem Klartextblock addiert (\oplus) wird:

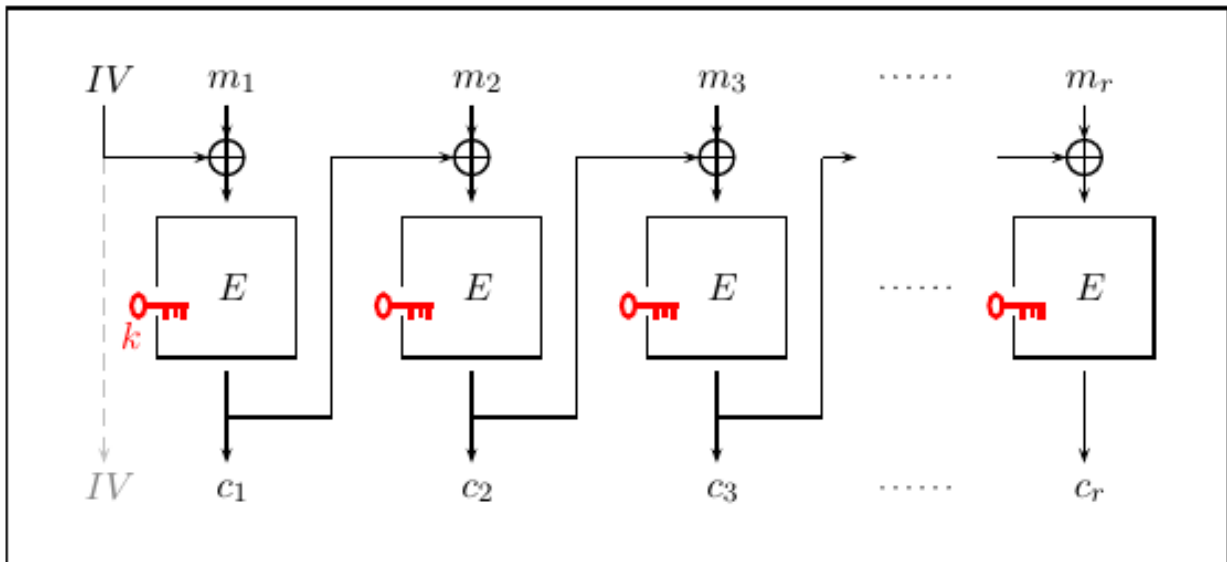


6.2.2 CBC (Cipher Block Chaining)

Der CBC-Modus ist eine spezielle Form des ECB-Modus, bei dem der errechnete Geheimtextblock als Nonce-Wert für die Verschlüsselung des nächsten Blocks verwendet wird. Hierbei wird der erste Nonce-Wert c_0 durch einen Initialisierungsvektor $IV \in \mathcal{M}$ gegeben.

$$c_i := E_k(m_i + c_{i-1})$$

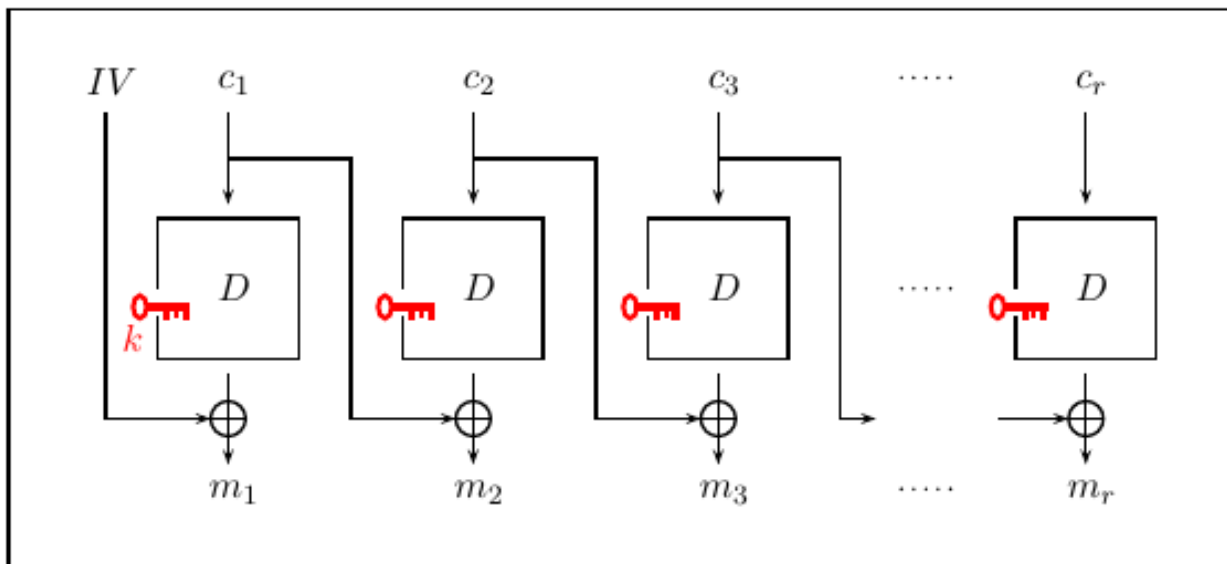
$$E_{k,IV}(m_1, \dots, m_r) := (c_1, \dots, c_r)$$



Bei der Entschlüsselung wird wie folgt vorgegangen:

$$m_i := D_k(c_i) + c_{i-1}$$

$$D_{k,IV}(c_1, \dots, c_r) := (m_1, \dots, m_r)$$



6.2.3 CBC-CS (Chiphertext Stealing for CBC Mode)

Der CBC-CS-Modus wird auch als CTS-Modus (Chiphertext Stealing Mode) bezeichnet. Dieser Modus basiert auf dem CBC-Modus (siehe 6.2.2), erlaubt aber eine Verschlüsselung von Nachrichten mit beliebiger Länge (ohne Padding). Um das Padding zu umgehen gibt es mehrere Varianten:

6.2.3.1 CBC-CS1

Bei der Variante 1 der CBC-CS-Verschlüsselung wird der letzte Block m_r^* der Nachricht mit 00-Bytes auf die Blocklänge aufgefüllt (00-Padding). Anschließend wird die Nachricht inkl. dem gepaddeten Block m_r mit dem CBC-Verfahren (siehe 6.2.2) verschlüsselt. Um wieder auf die ursprüngliche Länge der Nachricht zu kommen werden aus dem vorletzten Block c_{r-1} des Geheimtextes die gleiche Anzahl Bytes entfernt, die zu m_r^* hinzugefügt wurden. Hierdurch ergibt sich die Geheimtextnachricht $c_1, \dots, c_{r-2}, c_{r-1}^*, c_r$, die die gleiche Länge wie m hat.

Wenn die Länge der Nachricht m ein Vielfaches des Blocklänge l ist wird das normale CBC-Verschlüsselungsverfahren angewandt.

6.2.3.2 CBC-CS2

Bei der Variante 2 der CBC-CS-Verschlüsselung wird auf die gleiche Weise vorgegangen, wie bei Variante 1. Allerdings werden, **falls** ein Padding notwendig ist nach der Verschlüsselung und dem Stealing die letzten beiden Blöcke vertauscht.

$$E - CBC - CS2_{k,IV}(m_1, \dots, m_{r-1}, m_r^*) := (c_1, \dots, c_r, c_{r-1}^*)$$

Wenn die Länge der Nachricht m ein Vielfaches des Blocklänge l ist wird das normale CBC-Verschlüsselungsverfahren angewandt.

6.2.3.3 CBC-CS3

Die Variante 3 der CBC-CS-Verschlüsselung unterscheidet sich nur darin von der Variante 2, dass immer die letzten beiden Blöcke vertauscht werden. Dies geschieht ungeachtet davon, ob die Länge der Nachricht m ein Vielfaches der Blocklänge l ist.

6.2.4 CTR (Counter)

Im CTR-Modus wird ein Blockverschlüsselungsverfahren E mit einem Schlüssel k und einem Nonce-Wert $Ctr \in \mathcal{M}$ wie folgt verwendet:

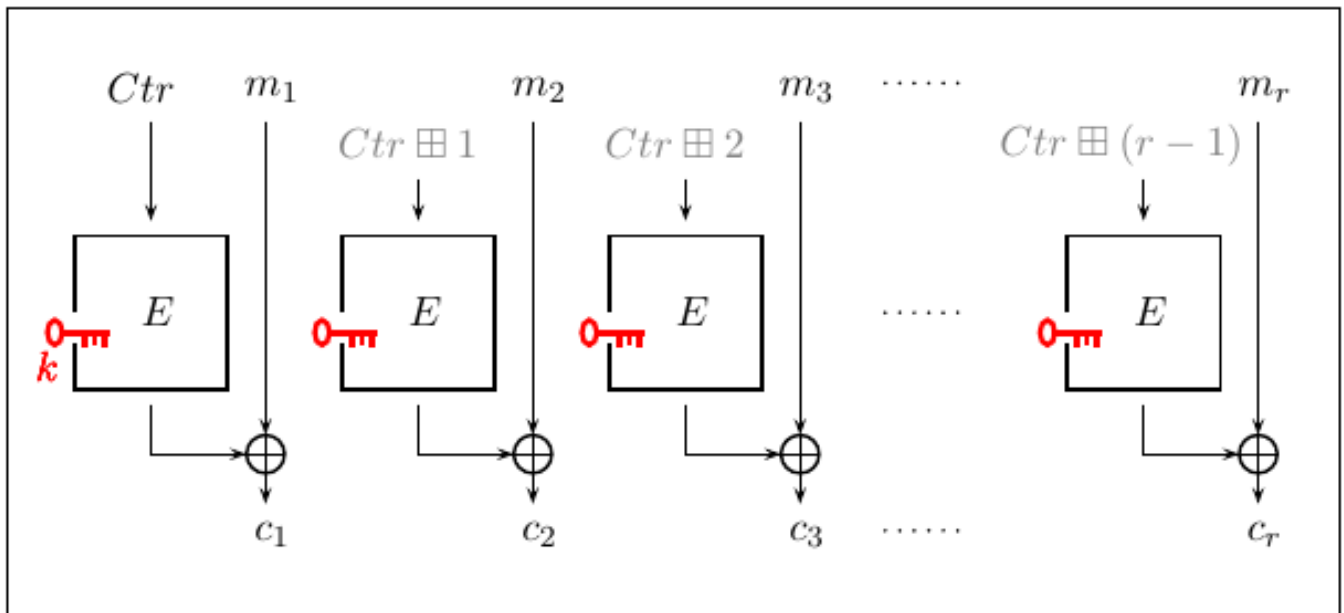
$$c_i := m_i + E_k(Ctr \boxplus (i - 1))$$

$$E - CTR_{k,Ctr}(m_1, \dots, m_r) := (c_1, \dots, c_r)$$

Der CTR-Modus definiert ein synchrones additives Stromverschlüsselungsverfahren (siehe 5.2.1.1). Die Menge der $z_i = E_k(Ctr \boxplus (i - 1))$ definiert hierbei den Schlüsselstrom.

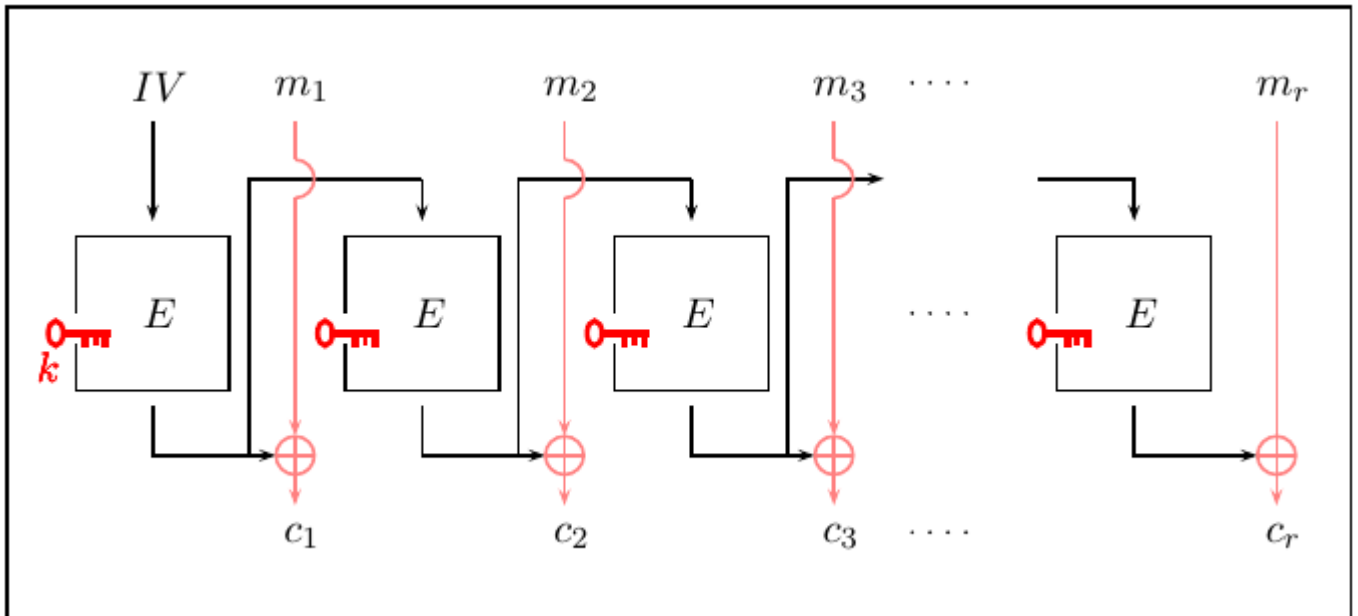
Aufgrund dessen ist die Entschlüsselungsfunktion D gleich der Verschlüsselungsfunktion E :

$$D - CTR_{k,Ctr}(c_1, \dots, c_r) = E - CTR_{k,Ctr}(c_1, \dots, c_r)$$



6.2.5 OFB (Output Feedback)

Bei der Konstruktion im OFB-Modus handelt es sich um ein synchrones Stromverschlüsselungsverfahren (siehe 5.1). Hierbei wird die Ausgabe der Verschlüsselungsfunktion jeweils als Eingabe für die nächste Verschlüsselungsfunktion genutzt:

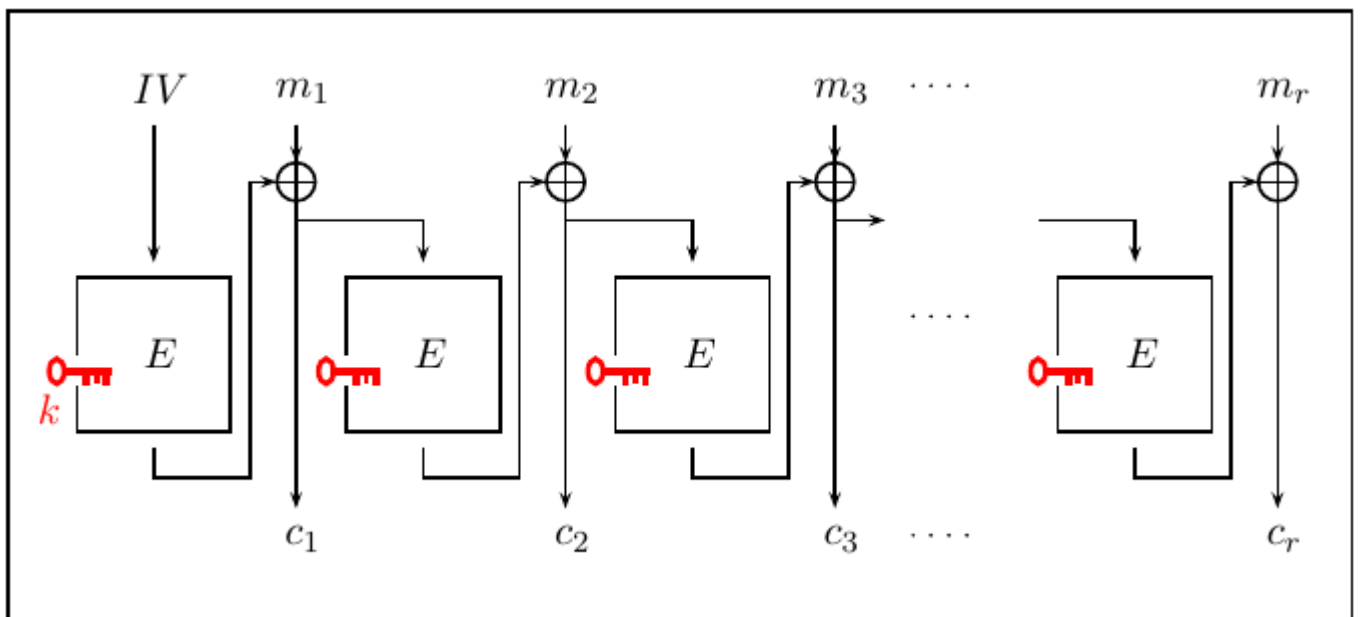


6.2.5.1 OFB- $8n$

bei dieser Variante des des OFB-Modus werden immer nur $n \in \mathbb{N}$ Bytes des verschlüsselten Blocks in der XOR-Verknüpfung genutzt. Der Rest des Klartextblocks wird in den folgenden Schritten verschlüsselt. n darf hierbei maximal so groß wie die Blocklänge l der Verschlüsselungsfunktion E sein.

6.2.6 CFB (Cipher-Feedback)

Der CFB-Modus hat viele Ähnlichkeiten mit dem OFB-Modus (siehe 6.2.5). Allerdings wird hierbei immer der verschlüsselte Block als Eingabe für die jeweils nächste Verschlüsselungsfunktion genutzt. Anders als beim OFB-Modus handelt es sich beim CFB-Modus aufgrund der Nutzung der Geheimtextblöcke nicht um eine synchrone Stromverschlüsselung.



6.2.6.1 CFB- $8n$

Diese Sonderfunktion des CFB-Modus stellt das Pendant zum OFB- $8n$ -Modus im OFB-Modus (siehe 6.2.5) dar.

6.3 Konstruktionsprinzipien von Blockverschlüsselungsverfahren

Alle Blockverschlüsselungsverfahren führen innerhalb des jeweiligen Blocks Permutationen aus. Diese Permutationen werden in Schleifen (Runden) angewandt. Die Permutationen können in folgende elementare Operationen zusammengefasst werden:

- *Transpositionen* von Bitwerten innerhalb eines Blocks
- *Substitution* von Werten innerhalb kleinerer Teilblöcke. Hierbei handelt es sich um eine Abbildung, welche durch eine Rechenvorschrift oder eine Wertetabelle gegeben werden kann. Wertetabellen werden in diesem Zusammenhang auch als *S-Boxen* bezeichnet.

Zudem findet der Schlüssel k ebenfalls eine Berücksichtigung. Aus ihm werden Rundenschlüssel k_i mit $i \in \{1, \dots, r\}$ abgeleitet, welche bei jeder Runde mit in die Berechnung einfließen. Bei einer Entschlüsselung wird das durch die Runden beschriebene Verfahren einfach rückwärts angewandt.

6.4 DES

Das einfache DES wurde 1977 veröffentlicht und 2005 zurückgezogen. Sowohl die Blöcke als auch die Schlüssel setzen sich jeweils aus 8 Bytes zusammen:

$$\begin{aligned}\mathcal{M} &= (\mathbb{Z}_2^8)^8 = \{(m_1, \dots, m_8) \mid m_i \in \mathbb{Z}_2^8\} \\ \mathcal{K} &= \{(k_1, \dots, k_8) \mid k_i \in \mathbb{Z}_2^8, \text{parity}(k_i) = 1\} \subseteq (\mathbb{Z}_2^8)^8\end{aligned}$$

Die Parität ist definiert durch:

$$\mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2 \quad \text{parity} \left(\sum_{i=0}^7 b_i \cdot 2^i \right) = \left(\sum_{i=0}^7 b_i \right) \mod 2$$

Mit anderen Worten: „Die Anzahl der 1-Bits im Byte muss ungerade sein“

Durch die Parität ist der Wert des achten Bits schon festgelegt. Aufgrund dessen hat der Schlüsselraum eine Bitlänge von $8 \cdot 7 = 56$. Da dies für moderne PCs mithilfe eines Brute-Force-Angriffs (siehe 4.5) in trivialer Zeit zu knacken ist sollte DES nicht mehr verwendet werden.

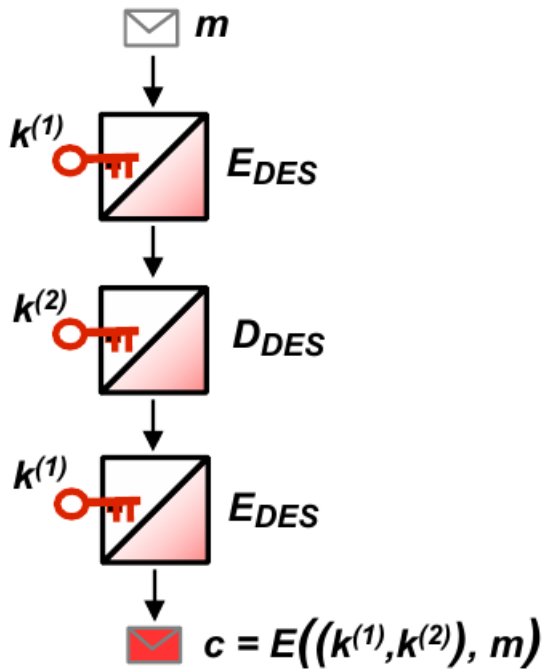
6.4.1 Triple-DES (3DES)

Beim Triple-DES wird das DES Verfahren 3mal hintereinander ausgeführt. Üblicherweise im EDE-Modus (Encrypt-Decrypt-Encrypt) mit 16 Byte langen Schlüsseln. Dadurch ergibt sich für den Schlüsselraum eine effektive Länge von 112 Bits. Die Menge der 8-Byte-langen Blöcke und der Schlüsselraum definieren sich wie folgt:

$$\begin{aligned}\mathcal{M} &= (\mathbb{Z}_2^8)^8 = \{(m_1, \dots, m_8) \mid m_i \in \mathbb{Z}_2^8\} \\ \mathcal{K} &= \{(k_1, \dots, k_8) \mid k_i \in \mathbb{Z}_2^8, \text{parity}(k_i) = 1\}^2\end{aligned}$$

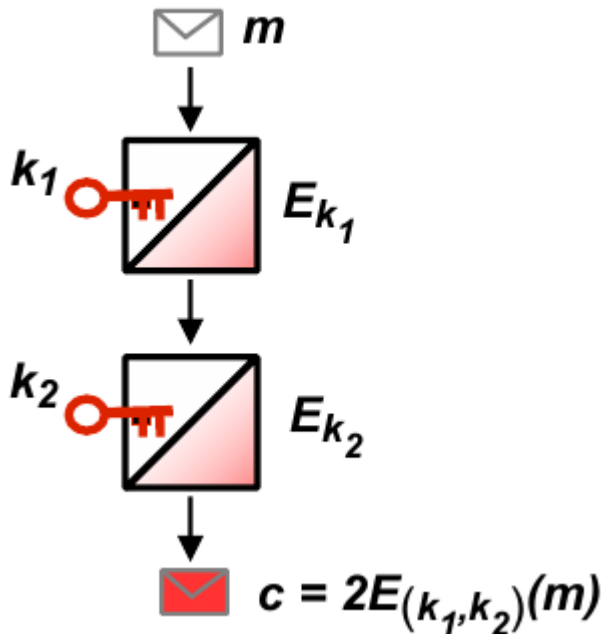
Die 3-DES Entschlüsselungsfunktion definiert sich durch:

$$E((k^{(1)}, k^{(2)}, m)) := E_{DES} \left(k^{(1)}, D_{DES} \left(k^{(2)}, E_{DES} \left(k^{(1)}, m \right) \right) \right)$$



6.5 Meet-in-the-Middle-Angriff

Aufgrund des Meet-in-the-Middle-Angriffs führt eine **zweifache** Hintereinanderreihung von Verschlüsselungsfunktionen nur zu einer kleinen Vergrößerung des Schlüsselraums. Bei diesem Angriff handelt es sich um einen known-plaintext-Angriff (siehe 4.4.2). Es wird angenommen, dass es ein $2E_{k_1, k_2}$ verfahren gibt, dass sich wie folgt definiert:



Es wird zudem angenommen, dass genügend Speicher zur Verfügung steht um alle $\tilde{k}_1 \in \mathcal{K}$ zusammen mit den jeweiligen $c_{\tilde{k}_1}(m_1) := E(\tilde{k}_1, m_1)$ in eine Tabelle zu schreiben:

\tilde{k}_1	$c_{\tilde{k}_1}(m_1) := E(\tilde{k}_1, m_1)$
0101010101010101	8A549EC56733AB66
0101010101010102	653148AE6B688132
\vdots	\vdots
FEFEFEFEFEFEFEFEFE	CE55464B6485684E

Anschließend wird die Tabelle nach der zweiten Spalte sortiert. Beim Ausprobieren alle Möglichkeiten von $\tilde{k}_2 \in \mathcal{K}$ kann für $D_{\tilde{k}_2}(c_1)$ nachgeschlagen werden, ob sich dieser in der Tabelle befindet. Hierdurch ergeben sich dann $(\tilde{k}_1, \tilde{k}_2)$ Paare, für die gilt:

$$2E_{\tilde{k}_1, \tilde{k}_2}(m_1) = c_1$$

Durchschnittlich ist mit $1 + \frac{|\mathcal{K}|}{|\mathcal{M}|}$ solcher Paare zu rechnen. Die Paare können nun durch Ausprobieren der anderen bekannten Nachrichten $\{m_i \setminus m_1\}$ schnell ausgeschlossen werden.

6.6 AES (Advanced Encryption Standard)

Der AES ist für Schlüssel mit den Bitlängen 128, 192 und 256 definiert. Im folgenden wird AES-128 als Synonym für alle möglichen Schlüssellängen verwendet.

6.6.1 AES-128

Sowohl die Blöcke als auch die Schlüssel setzen sich aus jeweils 16 Bytes zusammen:

$$\mathcal{M} = (\mathbb{Z}_2^8)^{16} = \{(m_1, \dots, m_{16}) \mid m_i \in \mathbb{Z}_2^8\}$$

$$\mathcal{K} = (\mathbb{Z}_2^8)^{16} = \{(k_1, \dots, k_{16}) \mid k_i \in \mathbb{Z}_2^8\}$$

Blöcke werden in Form von Matrizen dargestellt, die als State-Array bezeichnet werden:

$$S = \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix} := \begin{pmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \\ m_4 & m_8 & m_{12} & m_{16} \end{pmatrix}$$

Im AES gibt es 4 elementare Operationen auf den State-Arrays:

1. SubBytes()

Es wird auf Basis der folgenden Tabelle eine Substitution von jedem Element des State-Arrays durchgeführt.

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2. ShiftRows()

auf dem S-Array wird die folgende Transposition durchgeführt:

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix} \mapsto \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,0} & s_{3,1} & s_{3,2} \end{pmatrix}$$

3. MixColumns()

auf dem S-Array wird eine Substitution ausgeführt, die durch die folgende Multiplikation definiert ist:

$$S \mapsto M \cdot S \quad \text{mit } M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 02 & 01 & 02 \end{pmatrix}$$

Hierbei ist wichtig anzumerken, dass die Multiplikation nicht in \mathbf{Z}_{256} berechnet wird. Stattdessen wird sind die Elemente als Elemente des Körpers \mathbf{F}_{256} aufzufassen (siehe 7)

4. AddRoundKey()

Es wird eine XOR-Operation der Einträge des S-Arrays mit den entsprechenden Einträgen aus \mathbf{K} durchgeführt. Dies entspricht einer Matrixaddition in \mathbb{F}_{256} :

$$\mathbf{S} \mapsto \mathbf{K} + \mathbf{S}$$

AES-128 führt die zuvor beschriebenen Schritte nach dem folgenden Algorithmus aus:

```
AES_ENCRYPT(S, K0, ..., K10) {
  AddRoundKey(S, K0)
  for( int i = 1; i < 10; ++i) {
    SubBytes(S);
    ShiftRows(S);
    MixColumns(S);
    AddRoundKey(S, Ki)
  }
  SubBytes(S);
  ShiftRows(S);
  AddRoundKey(S, K10)
}
```

Kapitel 7

Endliche Körper \mathbb{F}_{p^n}

$\mathbb{F}_p := \mathbb{Z}_p$ (p ist eine Primzahl) ist ein Körper. Zudem können Körper auch für beliebige Primzahlpotenzen p^n mit $n \in \mathbb{N}, n > 0$ mithilfe der Polynome aus \mathbb{F}_p vom Grad $< n$ konstruiert werden:

$$\begin{aligned}\mathbb{F}_{p^n} &:= \{a(x) \mid a(x) \in \mathbb{F}_p[x], \text{grad}(a(x)) < n\} \\ &= \{a_{n-1}x^{n-1} + \dots + a_1x + a_0 \mid a_i \in \mathbb{F}_p\}\end{aligned}$$

Die normale Polynomaddition stellt bereits eine Addition in \mathbb{F}_{p^n} dar. Die normale Polynommultiplikation ist allerdings in \mathbb{F}_{p^n} nicht abgeschlossen. Das heißt es gibt häufig Produkte mit Polynomen vom Grad $> n$. Hierbei lässt sich allerdings analog zu \mathbb{Z} (siehe 2.2) durch eine Polynomdivision mit Rest durch $p(x)$ ein Wert in \mathbb{F}_{p^n} erzeugen.

7.1 Polynomdivision mit Rest

Ist \mathbb{F} ein Körper und $a(x), b(x) \in \mathbb{F}[x], b(x) \neq 0$, so gibt es eindeutig bestimmte Polynome $q(x), r(x) \in \mathbb{F}$ mit:

$$a(x) = b(x) \cdot q(x) + r(x) \text{ und } 0 \leq \text{grad}(r(x)) < \text{grad}(b(x))$$

Alternativ wird für den Rest $r(x)$ auch „ $a(x) \bmod b(x) = r(x)$ “ geschrieben.

7.2 Berechnung der Inversen

Der größte gemeinsame Teiler (das Polynom mit den höchsten Grad, dass $a(x)$ und $b(x)$ teilt) kann mithilfe des Euklid'schen Algorithmus (siehe 2.3.1) berechnet werden. Ist \mathbb{F}_{p^n} bezüglich eines irreduziblen Polynoms $p(x)$ definiert, lässt sich mithilfe der Anwendung des erweiterten Euklid'schen Algorithmus (siehe 2.3.2) auf die Polynome $a(x)$ und $b(x)$ eine Inverse von $a(x)$ in \mathbb{F}_{p^n} bestimmen.

7.3 \mathbb{F}_2

7.3.1 Irreduzible Polynome über \mathbb{F}_2

- Polynome von Grad 1 (lineare Polynome) sind immer irreduziblen. Für \mathbb{F}_2 sind dies:

$$\begin{aligned}p_{1,1}(x) &= x \\ p_{1,2}(x) &= x + 1\end{aligned}$$

- Es gibt in \mathbb{F}_2 4 paarweise verschiedene Polynome von Grad 2. 3 davon haben eine Nullstelle und lassen sich daher in Linearfaktoren zerlegen. Das einzige irreduzible Polynom von Grad 2 ist:

$$p_2(x) = x^2 + x + 1$$

- Ein Polynom von Grad 3 ist genau dann irreduzible, falls $p(x)$ keine Nullstellen hat. Dies trifft für die folgenden zwei Polynome zu:

$$p_{3,1}(x) = x^3 + x + 1$$

$$p_{3,2}(x) = x^3 + x^2 + 1$$

- Ein Polynom von Grad 4 ist genau dann irreduzible, wenn $p(x)$ keine Nullstelle hat und auch nicht das Quadrat von $p_2(x)$ ($x^4 + x^2 + 1$) ist:

$$p_{4,1}(x) = x^4 + x + 1$$

$$p_{4,1}(x) = x^4 + x^3 + 1$$

$$p_{4,1}(x) = x^4 + x^3 + x^2 + x + 1$$