TECHNISCHE UNIVERSITÄT BERGAKADEMIE FREIBERG

Die Ressourcenuniversität. Seit 1765.

Fakultät für Mathematik und Informatik (Fakultät 1)
Institut für Diskrete Mathematik und Algebra
Lehrstuhl für Algebra

Seminararbeit

Advanced Encryption Standard

Michael von Wenckstern

Angewandte Mathematik
Vertiefung: Informatik

Matrikel: 50 455

24. November 2012

Betreuer/1. Korrektor:
Prof. Dr. rer. nat. habil. Hebisch
Raum 1.09
Prüferstraße 1
09596 Freiberg

1 Kryptographie und ihre Einteilung

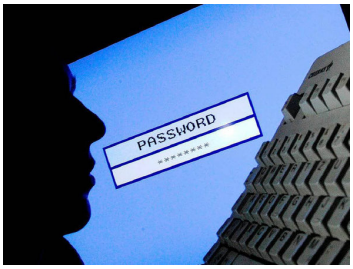

Abb. 1: Verschlüsselte Beweise: Passwörter vom "Maskenmann" schwer zu knacken
Hinweise auf weitere Morde oder einen Pädophilenring? Die Ermittler können nur spekulieren, was sich auf dem Computer des mutmaßlichen Kindermörders Martin N. befindet. Denn das Passwort ist bisher nicht geknackt.
Quelle: Badische Zeitung
http://tinyurl.com/cedap4f

Die Ziele der Kryptographie (vom griechischen: verborgen schreiben) sind die Geheimhaltung, sowie die Authentizität und die Integrität von Nachrichten. Deswegen findet die Kryptographie Verwendung in unserem alltäglichen Leben:

- geheime Firmen- und Regierungsunterlagen
- Onlineshops wie Amazon, Ebay
- Kreditkarten, Paypal
- LTE, WLAN
- Pay TV

Die Grundidee der Geheimhaltung ist die folgende: Person A will an seinen Freund F eine Information schicken, welche nur dieser lesen soll, nicht aber ein anderer Angreifer X. Also muss A den sogenannten **Klartext** so in einen **Geheimtext** ändern, dass F diese übermittelten Daten leicht entschlüsseln kann, aber X nicht. Daraus folgt aber schon, dass F mehr wissen muss als jeder Angreifer, da sonst bei Chancengleichheit die Entschlüsselung entweder für F unmöglich oder für X zu leicht wäre. Diese Zusatzinformation von F, die X nicht besitzt, nennt man den **Schlüssel** für die übermittelte Nachricht. Kann der Angreifer den Klartext aus dem Geheimtext ohne Kenntnis des Schlüssels gewinnen, dann ist das verwendete Verschlüsselungsverfahren **unsicher**. Lässt sich dagegen voraussagen, dass es dem Angreifer nicht gelingen wird den Klartext zu rekonstruieren, dann ist das Verfahren **perfekt** bzw. sicher. Es gibt aber auch Alternativen zur Kryptographie, so lässt sich beispielsweise die Authentizität von Geldscheinen durch chemisch-physikalische Merkmale wie Spezialpapier, Silberdraht oder Wasserzeichen garantieren. Aber die Kryptographie bietet 'objektivere' Sicherheit, da die sie größtenteils auf mathematischen Theorien beruht, d.h. im Idealfall ist die Sicherheit eines Algorithmus beweisbar. Zurzeit gibt es aber noch keine hunderprozentige Sicherheit, da der Schlüssel heute meistens aus einer bestimmten Anzahl von Bits besteht und somit theoretisch erraten werden kann. Aber bei einem 256-Bit Schlüssel, den die USA für die Geheimhaltungsstufe Top Secret vorschreibt, ist man praktisch gegen das systematische Erraten der $2^{256} \approx 1.2 \cdot 10^{77}$ Schlüssel gefeit, denn aus genau so vielen Teilchen besteht das Universum. Zum Vergleich: eine neue 400 Euro Grafikkarte schafft heute ungefähr 4 TerraFlops, also ca. $4 \cdot 10^{12}$ Rechenoperationen pro Sekunde, deswegen ist ein 56-Bit Schlüssel ($2^{56} \approx 7 \cdot 10^{16}$) wie ihn der DES verwendet zu kurz. Bild 3 stellt die Einteilung der Chiffrierverfahren dar. Direkte Chiffrierverfahren erzeugen aus Klartext und Schlüssel einen Ausgabetext, den man sofort als Geheimtext identifiziert. Im Gegensatz dazu manipulieren indirekte Verfahren bestimmte Teile des Klartextes so, dass das Ergebnis keine geheimen Informationen vermuten lässt. Die symmetrischen Verfahren benutzen zum Ver- und Entschlüsseln den gleichen Schlüssel. Bei den Public-Key-Verfahren wird der Klartext mit öffentlichen Schlüssel in einen Geheimtext umgewandelt, und der Empfänger rekonstruiert mithilfe des Privatschlüssels den Klartext aus dem Geheimtext. Die SSL-Verschlüsselungen im Internet benutzen heute am Anfang ein Public-Key-Verfahren (meistens RSA) um den Schlüssel für symmetrische Verfahren auszutauschen. Der öffentliche Schlüssel findet sich im Zertifikat (s. Bild 2) wieder. Der Grund für den

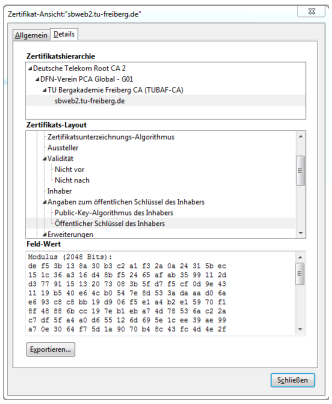

Abb. 2: Zertifikat von
https://sbweb2.tu-freiberg.de

Verschlüsselungswechsel von asymmetrisch zu symmetrisch liegt im Geschwindigkeitsvorteil für symmetrische Verfahren. Zum Beispiel benötigt der RSA-Algorithmus zum Verschlüsseln von 435 KB ca. 24.4 Sekunden und AES ist mit 2.6 Sekunden fast zehnmal so schnell(Quelle: [SMS07]). Bei Substitutionsverfahren werden Klartextelemente unter Beibehaltung ihrer Ordnung im Orginaltext durch Geheimtextelemente ersetzt. Bei Permutationsverfahren wird die Zeichenreihenfolge im Text verändert, aber die Zeichen werden nicht durch andere ersetzt. Bei Stromverfahren, auch Stromchiffre genannt, werden einzelne Zeichen des Klartextes mit denen des Schlüssels verknüpft, z.B. bei einem Bitstrom verwendet man die $\oplus$ Operation. Frequenzsprungverfahren verwendent die Bundeswehr zur Übertragung von geheimen Informationen, dabei wird in Sekundenbruchteilen immer die Frequenz gewechselt. Bei den Chaffling-Verfahren wird die Information in mehrere Pakete aufgeteilt und zwischen diesen werden auch noch beliebige Zufallspakete versendet, um den Empfänger zu verwirren.

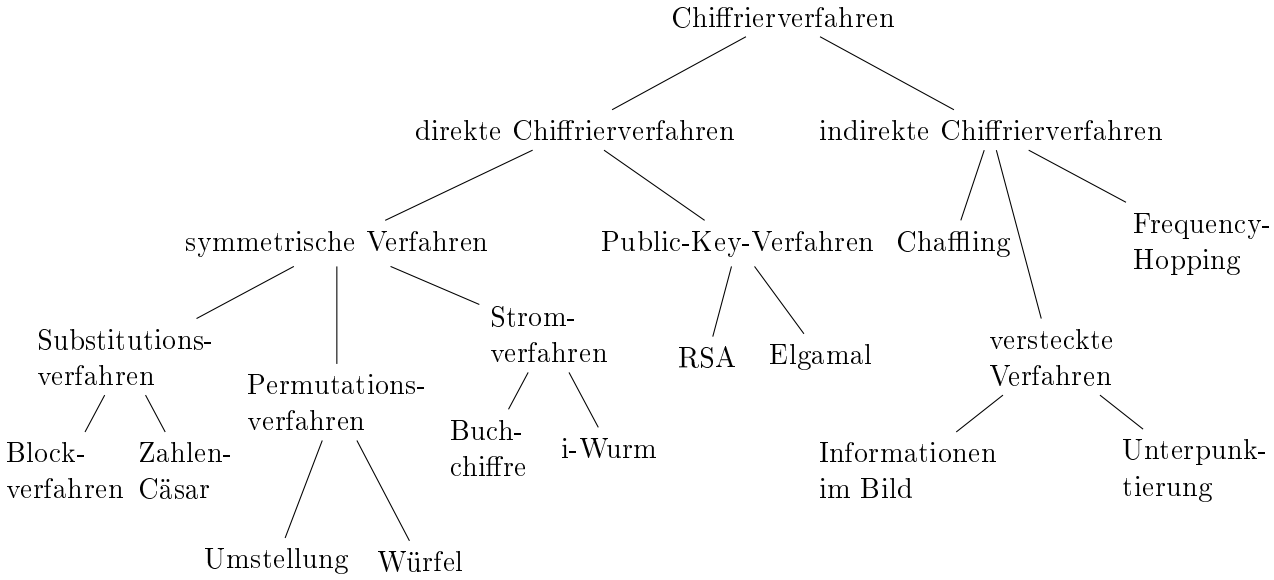

Abb. 3: Einteilung von Chiffrierverfahren. Quelle: [Spe, S. 21]

2 Auswahlverfahren zum Nachfolger von DES

Der Advanced Encryption Standard (kurz AES genannt) ist der Nachfolger vom Data Encryption Standard (mit DES abgekürzt). Bis zum Jahre 1990 wurde der DES zum Verschlüsseln von geheimen US-Regierungsdokumenten genutzt. Da in der Mitte der neunziger Jahre alle 2^{56} Schlüssel des DES durchprobiert werden konnten, wurde kurz danach als Übergangslösung der Triple-DES eingeführt, d.h. eine Nachricht wird mit 3 verschiedenen DES-Schlüsseln verschlüsselt, was ein Knacken der Verschlüsselung mit der Brutforce-Methode erstmal unmöglich machte. 1997 schrieb das US-Handelsministerium öffentlich eine Suche nach einem Nachfolgeralgorithmus aus. Das National Institute of Standards and Technology (kurz NIST genannt) führte diese Ausschreibung durch. Die öffentliche Diskussion über einen Nachfolger beeindruckte viele Menschen, da der DES im Geheimen entwickelt worden ist und viele Menschen damals befürchteten, dass die NSA im DES-Algorithmus eine Hintertür zum Entschlüsseln für sich eingebaut hatte. Der Sieger des DES-Nachfolgers sollte AES genannt werden und musste folgende Kriterien erfüllen:

1. symmetrischer Algorithmus, genauer Blockchiffre
2. AES muss 128 Bit, 192 Bit und 256 Bit lange Blöcke verwenden können
3. AES muss mit 128 Bit, 192 Bit oder 256 Bit langen Schlüssel umgehen können, daher auch die Namen AES-128 bzw. AES-256
4. AES soll gegen alle bekannten Kryptoanalysemethoden resistent sein, besonders gegen Power- und Timing-Attacken
5. AES soll leicht in Software und Hardware programmierbar sein und auch überdurchschnittliche Leistungsfähigkeit besitzen, damit die Verschlüsselung auch auf mobilen Endgeräten verwendet werden kann
6. AES muss von jeder Person unentgeltlich benutzt werden dürfen, muss also patentfrei sein

Die Anforderungen 1. bis 4. gehören zur Hauptkategorie Sicherheit. Die letzten zwei Kriterien gehören zur Kategorie Kosten, also Lizensierungsansprüche und rechnerische Effizenz für günstige Hardware. Zwei weitere wünschenswerte Kriterien waren erstens eine hohe Geschwindigkeit auf diversen Plattformen und zweitens eine vorhandene Flexibilität, d.h. AES sollte auch sicher und effizient als Stromchiffre und kryptologische Hashfunktion zu implementieren sein. Bis zur Deadline am 15. Juni 1998 wurden fünfzehn Vorschläge aus aller Welt eingereicht. Da die fünf Verfahren MARS, RC6, Serpent, Twofish und Rijandael die obengenannten Kriterien erfüllten, wurden weitere herangezogen:

- Überprüfung auf theoretische Schwachstellen
- Sortierung nach Leistungs- und Ressourcenverbrauch

Am 2. Oktober 2000 stand der belgische Algorithmus Rijandael (nach seinen Erfindern Vincent Rijmen und Joan Daemen) als Sieger fest. Rijandael wurde wegen seiner Eleganz (schöne mathematische Theorie), Einfachheit (Referenzimplementierung umfasst weniger als 500 Zeilen C-Code), Sicherheit und Geschwindigkeit ausgewählt, obwohl er ein europäischer Algorithmus ist.

Zusammenfassung von [Wik12a].

3 Der Körper GF(2^8)

Theorem 1 (Endlicher Körper p^n)**.** *Sei p eine Primzahl und $n \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^n$ Elementen, und dieser wird mit GF(p^n) bezeichnet. (GF steht für galois field und bedeutet endlicher Körper)*
Quelle: [wik10]

Wenn nicht anders vermerkt, stammen die nun folgenden Informationen aus dem offiziellen AES-Veröffentlichungspaper [Dae09].

Viele Operationen im AES-Algorithmus arbeiten mit ganzen Bytes (also 8 Bit), Die 256 Möglichkeiten auf Bytelevel repräsentieren den Körper GF(2^8). Es gibt verschiedene Darstellungen des endlichen Körpers, die aber nach Theorem 1 alle isomorph zueinander sind. Allerdings hat die gewählte Darstellung Einfluss auf die Komplexität der AES-Implementierung. Rijndael hat die klassische Polynomrepräsentation ausgewählt:
Ein Byte b bestehend aus der Bitfolge $b_7b_6b_5b_4b_3b_2b_1b_0$ wird als Polynom mit den Koeffizienten $x \in \{0, 1\}$ angesehen: $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$

Beispiel 1. *Das Byte mit dem Hexadezimalwert $0x8B$ (Binärdarstellung: 10001011) entspricht dem Polynom: $x^7 + x^3 + x + 1$.*

3.1 Addition

In der Polynomdarstellung ist die Summe zweier Elemente ein Polynom, dessen Konstanten durch die Summe modulo 2 der Koeffizienten beider Terme gegeben ist.

Beispiel 2. $0x8B + 0xC4 = 0x4F$ *oder*
Polynomschreibweise: $(x^7 + x^3 + x + 1) + (x^7 + x^6 + x^2) = x^6 + x^3 + x^2 + x + 1$
binäre Schreibweise: 1000 1011 + 1100 0100 = 0100 1111

Wie man schon im Beispiel sieht kann man die Addition auch durch das bitweise EXOR $\oplus$ auf dem Bytelevel ausdrücken.

Lemma 2 (Die Addition der Polynome bildet eine abelsche Gruppe)**.** *Die Addition der Polynome bildet eine abelsche Gruppe mit dem neutralen Element $0x00$.*

Beweis.
- Abgeschlossenheit: Ist durch bitweises modulo 2 gegeben.
- Assoziativität: Jeder Faktor ist assoziativ mit den Faktoren der anderen Summanden der gleichen Potenz.
- Neutrales Element: Für jeden Faktor gilt: $b_i + 0 = b_i$, also ist das Nullpolynom das neutrale Element
- Inverses Element: Da $1 + 1 = 0$ und $0 + 0 = 0$ gilt, sind die Elemente zu sich selbst invers.
- Kommutativität: Ist offensichtlich durch Addition modulo 2 faktorweise gegeben.

□

3.2 Multiplikation

In der Polynomialdarstellung entspricht die Multiplikation in GF(2^8) der Mulitplikation eines Polynoms modulo eines irreduziblen Polynoms vom Grad 8. Ein Polynom ist irreduzibel, wenn es keine anderen Teiler außer eins und sich selber besitzt. Im AES-Algorithmus wird das Polynom $m(x) = x^8 + x^4 + x^3 + x + 1$ oder $0x011B$ in Hexdarstellung verwendet.

Lemma 3 ($m(x)$ ist irreduzibel)**.** *Das AES-Polynom $0x011B$ ist irreduzibel.*

Beweis. $(a_8x^8 + a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) \cdot (b_8x^8 + b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0) =$
$a_8b_8x^{16} + a_8b_7x^{15} + a_8b_6x^{14} + a_8b_5x^{13} + a_8b_4x^{12} + a_8b_3x^{11} + a_8b_2x^{10} + a_8b_1x^9 + a_8b_0x^8 +$
$a_7b_8x^{15} + a_7b_7x^{14} + a_7b_6x^{13} + a_7b_5x^{12} + a_7b_4x^{11} + a_7b_3x^{10} + a_7b_2x^9 + a_7b_1x^8 + a_7b_0x^7 +$
$a_6b_8x^{14} + a_6b_7x^{13} + a_6b_6x^{12} + a_6b_5x^{11} + a_6b_4x^{10} + a_6b_3x^9 + a_6b_2x^8 + a_6b_1x^7 + a_6b_0x^6 +$
$a_5b_8x^{13} + a_5b_7x^{12} + a_5b_6x^{11} + a_5b_5x^{10} + a_5b_4x^9 + a_5b_3x^8 + a_5b_2x^7 + a_5b_1x^6 + a_5b_0x^5 +$
$a_4b_8x^{12} + a_4b_7x^{11} + a_4b_6x^{10} + a_4b_5x^9 + a_4b_4x^8 + a_4b_3x^7 + a_4b_2x^6 + a_4b_1x^5 + a_4b_0x^4 +$
$a_3b_8x^{11} + a_3b_7x^{10} + a_3b_6x^9 + a_3b_5x^8 + a_3b_4x^7 + a_3b_3x^6 + a_3b_2x^5 + a_3b_1x^4 + a_3b_0x^3 +$
$a_2b_8x^{10} + a_2b_7x^9 + a_2b_6x^8 + a_2b_5x^7 + a_2b_4x^6 + a_2b_3x^5 + a_2b_2x^4 + a_2b_1x^3 + a_2b_0x^2 +$
$a_1b_8x^9 + a_1b_7x^8 + a_1b_6x^7 + a_1b_5x^6 + a_1b_4x^5 + a_1b_3x^4 + a_1b_2x^3 + a_1b_1x^2 + a_1b_0x^1 +$
$a_0b_8x^8 + a_0b_7x^7 + a_0b_6x^6 + a_0b_5x^5 + a_0b_4x^4 + a_0b_3x^3 + a_0b_2x^2 + a_0b_1x^1 + a_0b_0x^0 \stackrel{!}{=}$
$x^8 + x^4 + x^3 + x + 1$
Machen jetzt Koeffizientenvergleich → Boolesches Gleichungssystem:
$a_0 \cdot b_0 = 1,$
$a_0 \cdot b_1 \oplus a_1 \cdot b_0 = 1,$
$a_0 \cdot b_2 \oplus a_1 \cdot b_1 \oplus a_2 \cdot b_0 = 0,$
$a_3 \cdot b_0 \oplus a_2 \cdot b_1 \oplus a_1 \cdot b_2 \oplus a_0 \cdot b_3 = 1,$
$a_4 \cdot b_0 \oplus a_3 \cdot b_1 \oplus a_2 \cdot b_2 \oplus a_1 \cdot b_3 \oplus a_0 \cdot b_4 = 1,$
$a_5 \cdot b_0 \oplus a_4 \cdot b_1 \oplus a_3 \cdot b_2 \oplus a_2 \cdot b_3 \oplus a_1 \cdot b_4 \oplus a_0 \cdot b_5 = 0,$
$a_6 \cdot b_0 \oplus a_5 \cdot b_1 \oplus a_4 \cdot a_2 \oplus a_3 \cdot b_3 \oplus a_2 \cdot b_4 \oplus a_1 \cdot b_5 \oplus a_0 \cdot b_6 = 0,$
$a_7 \cdot b_0 \oplus a_6 \cdot b_1 \oplus a_5 \cdot b_2 \oplus a_4 \cdot b_3 \oplus a_3 \cdot b_4 \oplus a_2 \cdot b_5 \oplus a_1 \cdot b_6 \oplus a_0 \cdot b_7 = 0,$
$a_8 \cdot b_0 \oplus a_7 \cdot b_1 \oplus a_6 \cdot b_2 \oplus a_5 \cdot b_3 \oplus a_4 \cdot b_4 \oplus a_3 \cdot b_5 \oplus a_2 \cdot b_6 \oplus a_1 \cdot b_7 \oplus a_0 \cdot b_8 = 1,$
$a_8 \cdot b_1 \oplus a_7 \cdot b_2 \oplus a_6 \cdot b_3 \oplus a_5 \cdot b_4 \oplus a_4 \cdot b_5 \oplus a_3 \cdot b_6 \oplus a_2 \cdot b_7 \oplus a_1 \cdot b_8 = 0,$
$a_8 \cdot b_2 \oplus a_7 \cdot b_3 \oplus a_6 \cdot b_4 \oplus a_5 \cdot b_5 \oplus a_4 \cdot b_6 \oplus a_3 \cdot b_7 \oplus a_2 \cdot b_8 = 0,$
$a_8 \cdot b_3 \oplus a_7 \cdot b_4 \oplus a_6 \cdot b_5 \oplus a_5 \cdot b_6 \oplus a_4 \cdot b_7 \oplus a_3 \cdot b_8 = 0,$
$a_8 \cdot b_4 \oplus a_7 \cdot b_5 \oplus a_6 \cdot b_6 \oplus a_5 \cdot b_7 \oplus a_4 \cdot b_8 = 0,$
$a_8 \cdot b_5 \oplus a_7 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_5 \cdot b_8 = 0,$
$a_8 \cdot b_6 \oplus a_7 \cdot b_7 \oplus a_6 \cdot b_8 = 0,$
$a_8 \cdot b_7 \oplus a_7 \cdot b_8 = 0,$
$a_8 \cdot b_8 = 0$

Lösen jetzt das Gleichungssystem mit XBoole und erhalten als Lösung:

Protokoll | 4-fache Ansicht | 1-fache Ansicht | Räume/Objekte

« » O TVL 1 (ODA) | 18 Var. | 2 Z. | R. 1

	a0	a1	a2	a3	a4	a5	a6	a7	a8	b0	b1	b2	b3	b4	b5	b6	b7	b8
1:	1	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	1
2:	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0

Dies bedeutet folgende Polynome miteinander multipliziert ergeben das Ausgangspolynom $m(x)$:

- $(1) \cdot (1 + x + x^3 + x^4 + x^8)$ und
- $(1 + x + x^3 + x^4 + x^8) \cdot (1)$

Diese Polynome sind aber gerade das Einspolynom und das Ausgangspolynom selber, damit ist bewiesen, dass $m(x)$ irreduzibel ist. □

Beispiel 3. $0x8B \bullet 0xC4 = 0xCC$

binäre Schreibweise: 1000 1011 • 1100 0100 = 1100 1100
Polynomschreibweise: $(x^7+x^3+x+1)\cdot\ (x^7+x^6+x^2) = x^{14}+x^{13}+x^9+$
$x^{10}+x^9+x^5 \quad + \quad x^8+x^7+x^3 \quad + \quad x^7+x^6+x^2 =$
$x^{14}+x^{13}+x^{10}+x^8+x^6+x^5+x^3+x^2$
$x^{14}+x^{13}+x^{10}+x^8+x^6+x^5+x^3+x^2$ *modulo* $x^8+x^4+x^3+x+1 = x^7+x^6+x^3+x^2$

Offensichtlich sieht man, dass durch die Modulo-Anwendung von $m(x)$ immer ein Polynom vom Grad echt kleiner als 8 herauskommt. Die Multiplikation ist assoziativ und besitzt das neutrale Element $0x01$.

Definition 1 (größter gemeinsamer Teiler)**.** *$d(x)$ ist größter gemeinsamer Teiler von $a(x)$ und $b(x)$ genau dann wenn:*

1. $a(x)\ mod\ d(x) = 0$
2. $b(x)\ mod\ d(x) = 0$

Aus 1. und 2. folgt, dass $d(x)$ sowohl $a(x)$ als auch $b(x)$ teilt. Außerdem muss auch noch $\forall_{d'\in GF(2^8)\wedge a(x)\ mod\ d'(x)=0\wedge b(x)\ mod\ d'(x)=0} : d(x)\ mod\ d'(x) = 0$.

Theorem 4 (Euklidischer Algorithmus)**.**

1. *Wenn $b(x) = 0$ ist, dann ist $ggt(a(x), b(x)) = a(x)$.*
2. *Wenn $b(x) \neq 0$ ist, dann ist $ggt(a(x), b(x)) = ggt(b(x), a(x)\ mod\ b(x))$.*

Beweis. Erstens ist offensichtlich wahr. Zweitens: Sei $b(x) \neq 0$, dann gibt es $q(x) \in GF(2^8)$ mit $a(x) = q(x) \bullet b(x) + (a(x) \bmod b(x))$ und $q(x)$ ist Ergebnis der Polynomdivision. Daher teilt der größte gemeinsame Teiler von $a(x)$ und $b(x)$ auch den größten gemeinsamen Teiler von $b(x)$ und $a(x) \bmod b(x)$, denn: $d(x) = \text{ggt}(a(x), b(x)) \rightarrow (1)\ a(x) \bmod d(x) = 0 \wedge\ (2)\ b(x) \bmod d(x) = 0 \rightarrow \exists_{k_1(x),k_2(x)\in GF(2^8)} :\ (1)\ k_1(x) \bullet d(x) = a(x) \wedge\ (2)\ k_2(x) \bullet d(x) = b(x) \rightarrow\ (1) + (2)\ (k_1(x) + k_2(x)) \bullet d(x) = a(x) + b(x) \rightarrow (a(x) + b(x)) \bmod d(x) = 0 \rightarrow d(x)$ teilt nun auch $a(x) + b(x)$, analog mit $d(x) \bmod (d'_1(x) + d'_2(x)) = 0$.
Quelle: [Buc04, S. 12]. □

Theorem 5 (Erweiterter Euklidischer Algorithmus)**.** *Der erweiterte Euklidische Algorithmus berechnet nicht nur den größten gemeinsamen Teiler wie der einfache Euklidische Algorithmus, sondern auch noch die Koeffizienten $s(x), t(x) \in GF(2^8)$, so dass gilt:*

$$ggt(a(x), b(x)) = s(x) \bullet a(x) + t(x) \bullet b(x)$$

Für jedes binäre Polynom $b(x)$ vom Grad echt kleiner als acht, kann man die Polynome $a(x)$ und $c(x)$ mit dem erweiterten Euklidalgorithmus berechnen, so dass gilt:

$$ggt(b(x), m(x)) = 1 \rightarrow b(x)\cdot\boxed{a(x)}+m(x)\cdot c(x) = 1 \rightarrow b^{-1}(x)\cdot b(x)\cdot a(x)+m(x)\cdot b^{-1}(x)\cdot c(x) = b^{-1}(x)\cdot 1$$

Der größte gemeinsame Teiler ist eins, da $m(x)$ irreduzibel ist und somit nur durch 1 und durch $m(x)$ teilbar ist, da aber $deg(b(x)) < deg(m(x))$, können beide nur den gemeinsamen Teiler 1 besitzen. Damit gilt dann $a(x) \bullet b(x)\ mod\ m(x) =\ 1$ oder $b^{-1}(x) = \boxed{a(x)}\ mod\ m(x)$. Außerdem gilt auch noch: $e(x) = a(x) \bullet (b(x) + d(x)) = a(x) \cdot (b(x) + d(x))\ mod\ m(x) \iff \exists c(x) : e(x) + c(x) \cdot m(x) = a(x) \cdot (b(x) + d(x)) = a(x) \cdot b(x) + a(x) \cdot d(x) \iff e(x) = a(x) \cdot b(x) + a(x) \cdot d(x)\ mod\ m(x) = a(x) \cdot b(x)\ mod\ m(x)\ +\ a(x) \cdot d(x)\ mod\ m(x) = a(x) \bullet b(x) + a(x) \bullet d(x)$.

Lemma 6. *Die $256 = 2^8$ Bytemöglichkeiten bilden einen Körper, den Körper GF(2^8).*

Beispiel 4. *Sei $b(x) = (0,0,0,0,0,0,1,1)^T$, wollen nun $b^{-1}(x)$ bestimmen: $ggt(b(x), m(x)) = ggt(1+x, 1+x+x^3+x^4+x^8) = (1+x)\cdot\boxed{(x^7+x^6+x^5+x^4+x^2+x)}+(1+x+x^3+x^4+x^8)\cdot 1 \rightarrow b^{-1}(x) = (1,1,1,1,0,1,1,0)^T$*
Rechnung: $\underline{1+x+x^3+x^4+x^8} = (x^7+x^6+x^5+x^4+x^2+x)\cdot\underline{(1+x)}+\underline{1}$
$\underline{1+x} = (x+1)\cdot\underline{1}+\underline{0} \rightarrow$ da der Rest Null ist, folgt daraus, dass $ggT = 1$ ist.
Stellen jetzt die Restdarstellung in den vorhergehenden Zeilen rekursiv ein, bei uns gibt es nur noch eine vorige Zeile:
$1 = 1\cdot(1+x+x^3+x^4+x^8) - (x^7+x^6+x^5+x^4+x^2+x)\cdot(1+x)$
Und in diesem Körper ist Minus das gleiche wie Plus, also erhält man:
$1 = ggt(1+x, m(x)) = 1\cdot(1+x+x^3+x^4+x^8) + (x^7+x^6+x^5+x^4+x^2+x)\cdot(1+x)$.

Nebenrechnung:

$(x^8$				$+x^4$	$+x^3$		$+x$	$+1$	$/(x+1) = x^7+x^6+x^5+x^4+x^2+x$
$\oplus x^8$	$\oplus x^7$								
	x^7			$+x^4$	$+x^3$		$+x$	$+1$	
	$\oplus x^7$	$\oplus x^6$							
		$+x^6$		$+x^4$	$+x^3$		$+x$	$+1$	
		$\oplus x^6$	$\oplus x^5$						
			$+x^5$	$+x^4$	$+x^3$		$+x$	$+1$	
			$\oplus x^5$	$\oplus x^4$					
					$+x^3$		$+x$	$+1$	
					$\oplus x^3$	$\oplus x^2$			
						x^2	$+x$	$+1$	
						$\oplus x^2$	$\oplus x$		
							1		

Beispiel 5. *Sei $b(x) = (0,1,1,1,1,1,0,0)^T$, wollen nun $b^{-1}(x)$ bestimmen: $ggt(b(x), m(x)) = ggt(x^6+x^5+x^4+x^3+x^2, 1+x+x^3+x^4+x^8) = (x^6+x^5+x^4+x^3+x^2)\cdot\boxed{(x^7+x^5+1)}+(1+x+x^3+x^4+x^8)\cdot(x^3+x+1) \rightarrow b^{-1}(x) = (1,0,1,0,0,0,0,1)^T$*
Rechnung: $\underline{1+x+x^3+x^4+x^8} = (x^2+x)\cdot\underline{(x^6+x^5+x^4+x^3+x^2)}+\underline{x^4+x+1}$
$\underline{x^6+x^5+x^4+x^3+x^2} = (x^2+x+1)\cdot\underline{(x^4+x+1)}+\underline{x^2+1}$
$\underline{x^4+x+1} = (x^2+1)\cdot\underline{(x^2+1)}+\underline{x}$
$\underline{x^2+1} = (x)\cdot\underline{x}+\underline{1}$
$\underline{x} = (x)\cdot\underline{1}+\underline{0} \rightarrow$ da der Rest Null ist, folgt daraus, dass $ggT = 1$ ist.
Stellen jetzt die Restdarstellung in den vorhergehenden Zeilen rekursiv ein:
$1 = x^2+1-(x)\cdot\boxed{(x)} = x^2+1-x\cdot\boxed{(x^4+x+1-(x^2+1)\cdot(x^2+1))} = \boxed{(x^2+1)}\cdot(1+x^3+x)-x\cdot(x^4+x+1)$
$= \boxed{(x^6+x^5+x^4+x^3+x^2-(x^2+x+1)\cdot(x^4+x+1))}\cdot(1+x^3+x)-x\cdot(x^4+x+1)$
$= (x^6+x^5+x^4+x^3+x^2)\cdot(1+x^3+x)-\boxed{(x^4+x+1)}\cdot(+x^5+x+x^4+1)$
$= (x^6+x^5+x^4+x^3+x^2)\cdot(1+x^3+x)-\boxed{(1+x+x^3+x^4+x^8-(x^2+x)\cdot(x^6+x^5+x^4+x^3+x^2))}\cdot(+x^5+x+x^4+1)$
$= (x^6+x^5+x^4+x^3+x^2)\cdot(1+x^3+x+(x^2+x)\cdot(+x^5+x^4+x+1))-(1+x+x^3+x^4+x^8)\cdot(x^3+x+1)$
$= (x^6+x^5+x^4+x^3+x^2)\cdot(1+x^3+x+x^7+x^6+x^3+x^2+x^6+x^5+x^2+x)-(1+x+x^3+x^4+x^8)\cdot(x^3+x+1)$
$= (x^6+x^5+x^4+x^3+x^2)\cdot(1+x^7+x^5)-(1+x+x^3+x^4+x^8)\cdot(x^3+x+1)$

Nebenrechnung 1:

$$\begin{array}{cccccccc|l}
(x^8 & & & & +x^4 & +x^3 & +x & +1) & /(x^6+x^5+x^4+x^3+x^2) = x^2+x \\
\oplus x^8 & \oplus x^7 & \oplus x^6 & \oplus x^5 & \oplus x^4 & & & & \\
\hline
 & x^7 & +x^6 & +x^5 & & +x^3 & +x & +1 & \\
 & \oplus x^7 & \oplus x^6 & \oplus x^5 & \oplus x^4 & \oplus x^3 & & & \\
\hline
 & & & & +x^4 & & +x & +1 &
\end{array}$$

Nebenrechnung 2:

$$\begin{array}{ccccccc|l}
(x^6 & +x^5 & +x^4 & +x^3 & +x^2) & & & /(x^4+x+1) = x^2+x+1 \\
\oplus x^6 & & & \oplus x^3 & \oplus x^2 & & & \\
\hline
 & x^5 & +x^4 & & & & & \\
 & \oplus x^5 & & & \oplus x^2 & \oplus x & & \\
\hline
 & & +x^4 & & +x^2 & +x & & \\
 & & \oplus x^4 & & & \oplus x & \oplus 1 & \\
\hline
 & & & & x^2 & & +1 &
\end{array}$$

Nebenrechnung 3:

$$\begin{array}{cccc|l}
(x^4 & & +x & +1) & /(x^2+1) = x^2+1 \\
\oplus x^4 & \oplus x^2 & & & \\
\hline
 & +x^2 & +x & +1 & \\
 & \oplus x^2 & & \oplus 1 & \\
\hline
 & & x & &
\end{array}$$

Nebenrechnung 4:

$$\begin{array}{ccc|l}
(x^2 & +1) & /(x) = x \\
\oplus x^2 & & \\
\hline
 & +1 &
\end{array}$$

Beispiel 6. *Sei* $b(x) = (0,1,1,1,1,1,1,1)^T$, *wollen nun* $b^{-1}(x)$ *bestimmen:*
$ggt(b(x), m(x)) = ggt(x^6+x^5+x^4+x^3+x^2+x+1, 1+x+x^3+x^4+x^8) = (x^6+x^5+x^4+x^3+x^2)\cdot$
$\boxed{(x^7+x^3+x^2+x)} + (1+x+x^3+x^4+x^8)\cdot(x^5+x^4+x^3+x^2+1) \rightarrow b^{-1}(x) = (1,0,0,0,1,1,1,0)^T$
Rechnung: $\underline{1+x+x^3+x^4+x^8} = (x^2+x)\cdot(x^6+x^5+x^4+x^3+x^2+x+1) + \underline{x^4+x^3+1}$
$\underline{x^6+x^5+x^4+x^3+x^2+x+1} = (x^2+1)\cdot\underline{(x^4+x^3+1)} + \underline{x}$
$\underline{x^4+x^3+1} = (x^3+x^2)\cdot\underline{x} + \underline{1}$
$\underline{x} = (x)\cdot\underline{1} + \underline{0} \rightarrow$ *da der Rest Null ist, folgt daraus, dass ggT = 1 ist.*
Stellen jetzt die Restdarstellung in den vorhergehenden Zeilen rekursiv ein:
$1 = x^4+x^3+1-(x^3+x^2)\cdot\boxed{(x)}$
$= x^4+x^3+1-(x^3+x^2)\cdot\boxed{(x^6+x^5+x^4+x^3+x^2+x+1-(x^2+1)\cdot(x^4+x^3+1))}$
$= (x^4+x^3+1)\cdot(1+(x^3+x^2)\cdot(x^2+1)) - (x^6+x^5+x^4+x^3+x^2+x+1)\cdot(x^3+x^2)$
$= \boxed{(x^4+x^3+1)}\cdot(x^5+x^4+x^3+x^2+1) - (x^6+x^5+x^4+x^3+x^2+x+1)\cdot(x^3+x^2)$
$= \boxed{(1+x+x^3+x^4+x^8-(x^2+x)\cdot(x^6+x^5+x^4+x^3+x^2+x+1))}\cdot(x^5+x^4+x^3+x^2+1) - (x^6+$
$x^5+x^4+x^3+x^2+x+1)\cdot(x^3+x^2)$
$= (1+x+x^3+x^4+x^8)\cdot(x^5+x^4+x^3+x^2+1) - (x^6+x^5+x^4+x^3+x^2+x+1)\cdot((x^2+x)\cdot(x^5+$
$x^4+x^3+x^2+1)+(x^3+x^2))$
$= (1+x+x^3+x^4+x^8)\cdot(x^5+x^4+x^3+x^2+1) - (x^6+x^5+x^4+x^3+x^2+x+1)\cdot(x^7+x^3+x^2+x)$

Nebenrechnung 1:

$$\begin{array}{cccccccccc|l}
(x^8 & & & & +x^4 & +x^3 & & +x & +1) & /(x^6+x^5+x^4+x^3+x^2+x+1) = x^2+x \\
\oplus x^8 & \oplus x^7 & \oplus x^6 & \oplus x^5 & \oplus x^4 & \oplus x^3 & \oplus x^2 & & & \\
\hline
 & x^7 & +x^6 & +x^5 & & & +x^2 & +x & +1 & \\
 & \oplus x^7 & \oplus x^6 & \oplus x^5 & \oplus x^4 & \oplus x^3 & \oplus x^2 & \oplus x & & \\
\hline
 & & & & +x^4 & +x^3 & & & +1 &
\end{array}$$

Nebenrechnung 2:

$$\begin{array}{llllllll} (x^6 & +x^5 & +x^4 & +x^3 & +x^2 & +x & +1) & /(x^4+x^3+1) = x^2+1 \\ \oplus x^6 & \oplus x^5 & & & \oplus x^2 & & & \\ \hline & & +x^4 & +x^3 & & +x & +1 & \\ & & \oplus x^4 & \oplus x^3 & & & \oplus 1 & \\ \hline & & & & & +x & & \end{array}$$

Nebenrechnung 3:

$$\begin{array}{llll} (x^4 & +x^3 & +1) & /(x) = x^3+x^2 \\ \oplus x^4 & & & \\ \hline & +x^3 & +1 & \\ & \oplus x^3 & & \\ \hline & & 1 & \end{array}$$

3.2.1 Multiplikation mit x

In Hardware kann die Multiplikation mit x in nur 4 Operationen (Linksshift, b_7 aus $b(x)$ eliminieren, b_7 mit $0x1B$ verknüpfen und Linksshift mit vorigem Ergebnis addieren) ausgeführt werden.

Lemma 7. $x \bullet b(x) = \ b(x) << 1 \oplus b_7 \dots \ b_7 \ \& \ 0x1B$

Beweis. Wenn man nun $b(x)$ multipliziert mit dem Polynom x, dann bekommt man als Ergebnis

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

$x \bullet b(x)$ erhält man, indem man das Ergebnis mit modulo $m(x)$ reduziert, ist $b_7 = 0$, dann ist die Reduktion der Einheitsoperator, für $b_7 = \ 1$ muss $m(x)$ von $b(x)$ abgezogen werden, z.B. indem man $b(x) \oplus m(x)$ rechnet.

$b(x)$ auf Bytelevel ist: $\boxed{b_7}\boxed{b_6}\boxed{b_5}\boxed{b_4}\boxed{b_3}\boxed{b_2}\boxed{b_1}\boxed{b_0}$

$b(x) << 1$ auf Bytelevel ist: $\boxed{b_6}\boxed{b_5}\boxed{b_4}\boxed{b_3}\boxed{b_2}\boxed{b_1}\boxed{b_0}\boxed{0}$

$b(x) << 1 \oplus b_7 \dots \ b_7 \ \& \ 0x1B$ auf Bytelevel ist:

$\boxed{b_6}\boxed{b_5}\boxed{b_4}\boxed{b_3}\boxed{b_2}\boxed{b_1}\boxed{b_0}\boxed{0} + \boxed{b_7 \cdot 0}\boxed{b_7 \cdot 0}\boxed{b_7 \cdot 0}\boxed{b_7 \cdot 1}\boxed{b_7 \cdot 1}\boxed{b_7 \cdot 0}\boxed{b_7 \cdot 1}\boxed{b_7 \cdot 1}$ □

Diese Multiplikation mit x wird als xtime Funktion bezeichnet. Multiplikation mit höheren Polynomen von x kann man auf die wiederholte Anwendung der xtime Funktion zurückführen. Wenn man dann noch die Zwischenergebnisse aufaddiert, kann man somit die Multiplikation mit jeder Konstanten effizient implementieren.

Beispiel 7. $0x57 \bullet 0x13 = 0x57 \bullet (0x01 \oplus 0x02 \oplus 0x10)$
$0x57 \bullet 0x02 = xtime(0x57) = xtime(01010111) = 10101110 = 0xAE$
$0x57 \bullet 0x04 = xtime(0xAE) = xtime(10101110) = 0101\ 1100 \oplus 0001\ 1011 = 0100\ 0111 = 0x47$
$0x57 \bullet 0x08 = xtime(0x47) = xtime(01000111) = 10001110 = 0x8E$
$0x57 \bullet 0x10 = xtime(8E) = xtime(10001110) = 0001\ 1100 \oplus 0001\ 1011 = 0000\ 0111 = 0x07$
(Anmerkung $0x10$ ist dezimal 16)
$\rightarrow 0x57 \bullet 0x13 = 0x57 \oplus 0xAE \oplus 0x07 = 0101\ 0111 \oplus 1010\ 1110 \oplus 0000\ 0111 = 1111\ 1110 = 0xFE$

4 Polynome mit Koeffizienten in GF(2^8)

Wenn man nun Polynome mit Koeffizienten in GF(2^8) definiert, entspricht ein 4-Byte-Vektor einem Polynom vom Grad echt kleiner als 4. Da Polynome addiert werden, indem man einfach ihre gleichgradigen Koeffizienten addiert, kann eine Addition von einem Polynom durch bitweises $\oplus$ im Bytevektor durchgeführt werden. Die Multiplikation ist etwas schwieriger: Angenommen man hat zwei Polynome über GF(2^8): $a(x) = \ a_3x^3 + a_2x^2 + a_1x + a_0$ und $b(x) = b_3x^3 + b_2x^2 +$

$b_1x + b_0$ *Das Produkt* $c(x) = a(x) \cdot b(x)$ *ist dann gegeben durch:*
$c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$ *mit (Verwenden* $\bullet$ *als Multiplikation mit die Koeffizienten* c_i *in GF(2^8) liegen und nicht in GF(2^{16}) und damit außerhalb unseres Körpers).*
$c_0 = a_0 \bullet b_0$, $c_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1$, $c_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2$, $c_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3$,
$c_4 = a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3$, $c_5 = a_3 \bullet b_2 \oplus a_2 \bullet b_3$, $c_6 = a_3 \bullet b_3$
Offensichtlich benötigt man nun einen 7-Byte-Vektor um $c(x)$ *darzustellen. Um wieder einen 4-Byte-Vektor zu bekommen, reduziert man* $c(x)$ *modulo einem Polynom vom Grad 4. In AES verwendet man dazu das Polynom* $M(x) = x^4 + 1$.

Lemma 8. *Sei* $d(x) = c(x)$ *modulo* $M(x)$*, dann gilt:*
$d(x) = d_3x^3 + d_2x^2 + d_1x + d_0$ *mit*
$d_0 = a_0 \bullet b_0 \oplus a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3$
$d_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1 \oplus a_3 \bullet b_2 \oplus a_2 \bullet b_3$
$d_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \oplus a_3 \bullet b_3$
$d_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3$

Beweis. Führen Polynomdivision durch: (Anmerkung in diesem Körper sind die Elemente zu sich selbst invers $\rightarrow a - b = a + (-b) = a + b = a \oplus b$)

$(c_6x^6$	$+c_5x^5$	$+c_4x^4$	$+c_3x^3$	$+c_2x^2$	$+c_1x$	$+c_0)$	$/(x^4+1) = c_6x^2 + c_5x + c_4$
$\oplus c_6x^6$				$\oplus c_6x^2$			
	c_5x^5	$+c_4x^4$	$+c_3x^3$	$+(c_2 \oplus c_6)x^2$	$+c_1x$	$+c_0$	
	$\oplus c_5x^5$				$\oplus c_5x$		
		$+c_4x^4$	$+c_3x^3$	$+(c_2 \oplus c_6)x^2$	$+(c_1 \oplus c_5)x$	$+c_0$	
		$\oplus c_4x^4$				$\oplus c_4$	
			$+c_3x^3$	$+(c_2 \oplus c_6)x^2$	$+(c_1 \oplus c_5)x$	$+(c_0 \oplus c_4)$	

Damit bekommt man jetzt folgende Beziehung
$d_3 = c_3$, $d_2 = c_2 \oplus c_6$, $d_1 = c_1 \oplus c_5$ und $d_0 = c_0 \oplus c_4$ □

Wir schreiben ab jetzt $d(x) = a(x) \otimes b(x)$*. Wenn man sich die Struktur von* d_0 *bis* d_3 *genauer anschaut, stellt man fest, dass sich diese auch in Vektorschreibweise darstellen lassen:*

$$\begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \bullet \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

Lemma 9. *Das Polynom* $M(x)$ *ist nicht irreduzibel. Daraus folgt, dass nicht jedes Polynom über GF(2^8) modulo* $M(x)$ *invertierbar ist. Aber das in AES verwendete Polynom* $p(x) = 0x03\ x^3 + 0x01\ x^2 + 0x01\ x + 0x02$ *ist invertierbar und besitzt das inverse Polynom* $p^{-1}(x) = 0x0B\ x^3 + 0x0D\ x^2 + 0x09\ x + 0x0C$.

Beweis. $(x^2 + 1) \cdot (x^2 + 1) = x^4 \oplus x^2 \oplus x^2 \oplus 1 = x^4 + 1 = M(x)$
Rechnen jetzt nach, dass $p(x) \otimes p^{-1}(x) = 1$
Bilden zuerst $xtime(0x03)$,$xtime(0x01)$ und $xtime(0x02)$:
$0x03 \bullet 0x02 = xtime(0x03) = xtime(00000011) = 00000110 = 0x06$
$0x03 \bullet 0x04 = xtime(0x06) = xtime(00000110) = 00001100 = 0x0C$
$0x03 \bullet 0x08 = xtime(0x0C) = xtime(00001100) = 00011000 = 0x18$
$0x03 \bullet 0x10 = xtime(0x18) = xtime(00011000) = 00110000 = 0x30$

$0x01 \bullet 0x02 = xtime(0x01) = xtime(00000001) = 00000010 = 0x02$
$0x01 \bullet 0x04 = xtime(0x02) = xtime(00000010) = 00000100 = 0x04$
$0x01 \bullet 0x08 = xtime(0x04) = xtime(00000100) = 00001000 = 0x08$

$0x01 \bullet 0x10 = xtime(0x08) = xtime(00001000) = 00010000 = 0x10$

$0x02 \bullet 0x02 = xtime(0x02) = xtime(00000010) = 00000100 = 0x04$
$0x02 \bullet 0x04 = xtime(0x04) = xtime(00000100) = 00001000 = 0x08$
$0x02 \bullet 0x08 = xtime(0x08) = xtime(00001000) = 00010000 = 0x10$
$0x02 \bullet 0x10 = xtime(0x10) = xtime(00010000) = 00100000 = 0x20$

$d_0 = \ 0x02 \bullet 0x0E \oplus 0x03 \bullet 0x09 \oplus 0x01 \bullet 0x0D \oplus 0x01 \bullet 0x0B$
$= 0x02 \bullet (0x02 \oplus 0x04 \oplus 0x08) \oplus 0x03 \bullet (0x01 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x04 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x02 \oplus 0x08)$
$= (0x04 \oplus 0x08 \oplus 0x10) \oplus (0x03 \oplus 0x18) \oplus (0x01 \oplus 0x04 \oplus 0x08) \oplus (0x01 \oplus 0x02 \oplus 0x08)$
$= 0x1C \oplus 0x1B \oplus 0x0D \oplus 0x0B = 0x01$
$d_1 = \ 0x01 \bullet (0x02 \oplus 0x04 \oplus 0x08) \oplus 0x02 \bullet (0x01 \oplus 0x08) \oplus 0x03 \bullet (0x01 \oplus 0x04 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x02 \oplus 0x08)$
$= (0x02 \oplus 0x04 \oplus 0x08) \oplus (0x02 \oplus 0x10) \oplus (0x03 \oplus 0x0C \oplus 0x18) \oplus (0x01 \oplus 0x02 \oplus 0x08)$
$= 0x0E \oplus 0x12 \oplus 0x17 \oplus 0x0B = 0x00$
$0x01 \bullet 0x0E \oplus 0x02 \bullet 0x09 \oplus 0x03 \bullet 0x0D \oplus 0x01 \bullet 0x0B$
$d_2 = \ 0x01 \bullet 0x0E \oplus 0x01 \bullet 0x09 \oplus 0x02 \bullet 0x0D \oplus 0x03 \bullet 0x0B$
$= 0x01 \bullet (0x02 \oplus 0x04 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x08) \oplus 0x02 \bullet (0x01 \oplus 0x04 \oplus 0x08) \oplus 0x03 \bullet (0x01 \oplus 0x02 \oplus 0x08)$
$= (0x02 \oplus 0x04 \oplus 0x08) \oplus (0x01 \oplus 0x08) \oplus (0x02 \oplus 0x08 \oplus 0x10) \oplus (0x03 \oplus 0x06 \oplus 0x18)$
$= 0x0E \oplus 0x09 \oplus 0x1A \oplus 0x1D = 0x00$
$d_3 = \ 0x03 \bullet 0x0E \oplus 0x01 \bullet 0x09 \oplus 0x01 \bullet 0x0D \oplus 0x02 \bullet 0x0B$
$= 0x03 \bullet (0x02 \oplus 0x04 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x08) \oplus 0x01 \bullet (0x01 \oplus 0x04 \oplus 0x08) \oplus 0x02 \bullet (0x01 \oplus 0x02 \oplus 0x08)$
$= (0x06 \oplus 0x0C \oplus 0x18) \oplus (0x01 \oplus 0x08) \oplus (0x01 \oplus 0x04 \oplus 0x08) \oplus (0x02 \oplus 0x04 \oplus 0x10)$
$= 0x12 \oplus 0x09 \oplus 0x0D \oplus 0x16 = 0x00$ □

4.1 Multiplikation mit x

Wenn man $b(x)$ mit einem Polynom x multipliziert erhält man:

$$b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

$x \otimes b(x)$ erhält man indem man das obige Ergebnis mit modulo $x^4 + 1$ reduziert.

$$\begin{array}{llll} (b_3x^4 & +b_2x^3 & +b_1x^2 & +b_0x) \qquad /(x^4+1) = b_3 \\ \oplus b_3x^4 & & & \oplus b_3 \\ \hline & b_2x^3 & +b_1x^2 & +b_0x \quad +b_3 \end{array}$$

Die Multiplikation mit x ist equivalent zur Multiplikation mit der obigen Matrix, wobei alle $a_i = 0x00$ außer $a_1 = 0x01$. Wenn $c(x) = x \otimes b(x)$, dann gilt

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0x00 & 0x00 & 0x00 & 0x01 \\ 0x01 & 0x00 & 0x00 & 0x00 \\ 0x00 & 0x01 & 0x00 & 0x00 \\ 0x00 & 0x00 & 0x01 & 0x00 \end{pmatrix} \bullet \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

Wenn $b(x) = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$, *dann ist* $x \otimes b(x) = \begin{pmatrix} b_3 \\ b_0 \\ b_1 \\ b_2 \end{pmatrix}$

Dies bedeutet, dass Multiplikationen mit Potenzen von x einfach durch eine Bytepermutation ausgedrückt werden können, oder in der PC-Hardware durch einfache zyklische Shiftoperationen.

5 Designentscheidung

Die folgenden Kriterien sollte das Design des AES erfüllen:

- *Resistent gegen alle bekannten Kryptographieattacken*
- *Hohe Ausführungsgeschwindigkeit und Codekompaktheit auf den meisten Hardwareplattformen*
- *Das Design sollte einfach sein*

Definition 2 (Feistel-Struktur). *Sei F die Rundenfunktion und $K_0, K_1, \ldots K_n$ die Rundenschlüssel für die Runden $0, 1, \ldots, n$. Dann macht der Feistel-Algorithmus folgendes:*
Teile den Klartextblock in zwei gleichlange Blöcke (L_0, R_0) auf.
Für jede Runde $i = 0, 1, \ldots, n$ berechne:
$L_{i+1} = R_i$
$R_{i+1} = L_i \oplus F(R_i, K_i)$
Der kodierte Text ist dann (R_{n+1}, L_{n+1}).
Die Entschlüsselung funktioniert 'rückwärts' für $i = n, n-1, \ldots, 0$:
$R_i = L_{i+1}$
$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$
Der dekodierte Text ist dann (L_0, R_0).

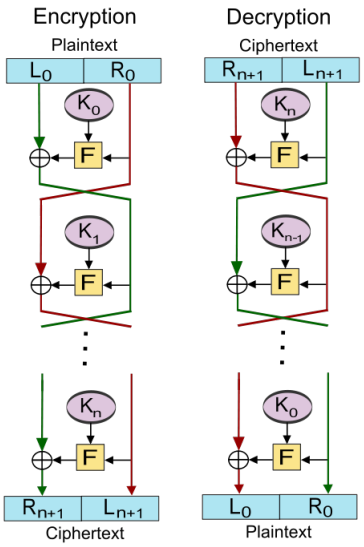

Abb. 4: Feistel-Struktur
Quelle: [Wik12b]

Die meisten Kryptographiealgorithmen benutzen die Feistel-Struktur zur Rundentransformation. In dieser Struktur werden jedoch meistens nur Bits von einer Position zur anderen transformiert ohne wirklich verändert zu werden. Der AES-Algorithmus verwendet nicht die Feistel-Struktur, dafür setzt sich aber die Rundentransformation aus drei verschiedenen invertierbaren Einheitstransformationen zusammen. Die drei Transformationen sind:

- *Lineare Mixschicht: Garantiert eine hohe Diffusion (Durchmischung) der Bits über mehrere Runden*
- *Nichtlineare Schicht: parallele Anwendung von S-Boxen, die ein Optimum an Nichtlinearität besitzen*
- *Schlüsseladditionsschicht: Eine einfache $\oplus$ Verknüpfung vom aktuellen Zustand mit dem Rundenschlüssel.*

6 AES Spezifikation

6.1 Struktur

AES ist ein iterativer symmetrischer Blockchiffre mit einer variablen Block- und Schlüssellänge von 128,192 oder 256 Bits.

Definition 3 (Zustand). *Die Chiffre-Zwischenergebnisse werden Zustand genannt.*

Der Einfachheit halber beschränken wir uns hier nur auf eine Block- und Schlüssellänge von 128 Bit. Der Zustand kann als quadratische Anordnung von Bytes dargestellt werden, welche dann 4 Reihen und Nb Spalten hat, wobei $Nb = Blocklaenge/32$ ist, also bei uns auch vier. Der Chiffre-Schlüssel kann zudem als Quadrat dargestellt werden mit 4 Reihen und $Nk = Schluessellaenge/32$ Spalten, was hier auch wieder vier ist. Die Figuren 5 und 6 stellen diese dar.

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

Abb. 5: Darstellung des Zustandes mit $Nb = 4$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Abb. 6: Darstellung des Schlüssels mit $Nk = 4$

Manchmal stellt man das Quadrat auch als 4-Byte-Wort-Vektor dar, d.h. eine Spalte im Rechteck entspricht einem Wort. Wenn diese Darstellung benutzt wird, dann bezeichnet (a, b, c, d) das Wort mit a, b, c, d an den Positionen $0, 1, 2, 3$.

Die Anzahl der ausgeführten iterativen Runden hängt von der Blockgröße und der Schlüssellänge ab, Tabelle 1 stellt diesen Zusammenhang dar:

Tab. 1: Rundenanzahl in Abhängigkeit von Block- und Schlüssellänge

Anzahl der Runden	*128 Bit Blockgröße*	*196 Bit Blockgröße*	*256 Bit Blockgröße*
128 Bit Schlüssellänge	*10*	*12*	*14*
196 Bit Schlüssellänge	*12*	*12*	*14*
256 Bit Schlüssellänge	*14*	*14*	*14*

6.2 Algorithmus

Listing 1: AES-Algorithmus in Pseudo-Java-Code

```
/** AES-Verschluesselungsalgorithmus
 * @param Zustand der Klartext, der verschluesselt werden soll
 * @param ChiffreSchluessel, der Geheimschluessel, entweder 128,196
 *        oder 256 Bit lang
 * @return der Geheimtext, der aus dem Klartext und dem Geheim-
 *         schluessel erzeugt wurden ist
 */
byte[] AES(byte Zustand[], byte ChiffreSchluessel[]) {
  byte[] erweiterterSchluessel =
    Schluesselerweiterung(ChiffreSchluessel);
  Zustand = RundenSchluesselXOR(Zustand, erweiterterSchluessel);
  for(int i=1; i<Nr; i++) {
```

```
    Zustand = Runde(Zustand, erweiterterSchluessel[Nb*i...(Nb+1)*i-1]);
  }
  Zustand = EndRunde(Zustand, erweiterterSchluessel[Nb*Nr...Ende];
  return Zustand;
}

byte[] Runde(byte Zustand[], byte RundenSchluessel[]) {
  Zustand = ByteSubstitution(Zustand);
  Zustand = Reihenverschiebung(Zustand);
  Zustand = MischeSpalten(Zustand);
  Zustand = RundenSchluesselAddition(Zustand, RundenSchluessel);
  return Zustand;
}

byte[] EndRunde(byte Zustand[], byte RundenSchluessel[]) {
  Zustand = ByteSubstitution(Zustand);
  Zustand = Reihenverschiebung(Zustand);
  Zustand = RundenSchluesselAddition(Zustand, RundenSchluessel);
  return Zustand;
}
```

6.2.1 ByteSubstitutions-Transformation

Die ByteSubstitutions-Transformation ist eine nichtlineare Byte-Operation, welche auf jedes Zustandsbyte unabhängig wirkt. Die Substitutionstabelle oder auch S-Box genannt ist invertierbar und entsteht durch die nacheinander Ausführung der beiden Transformationen:

- *Man nimmt das multiplikative Inverse aus der GF(2^8) Gruppe wie im vorigen Kapitel beschrieben, wobei man $0x00$ auf sich selbst abbildet. Genauer:*
  Sei $a = a_7a_6a_5a_4a_3a_2a_1a_0$ nicht das Nullbyte, also $\forall_{0\leq i\leq 7} : a_i \in (0,1) \wedge \sum_{i=0}^{7} a_i \geq 1$ dann bilde das Polynom $p(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ und bestimme dessen Inverses $p^{-1}(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ so, dass $p(x) \bullet p^{-1}(x) = 0x01$. Das Ergebnis dieser Transformation ist das Byte $b = b_7b_6b_5b_4b_3b_2b_1b_0$.
- *Auf $b = b_7b_6b_5b_4b_3b_2b_1b_0$ wird nun die folgende affine Transformation über GF(2) angewendet:*

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \bullet \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Figur 7 illustriert diese Transformation:

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\xrightarrow{S\text{-}Box}$

$c_{0,0}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$
$c_{1,0}$	$c_{1,1}$	$c_{1,2}$	$c_{1,3}$
$c_{2,0}$	$c_{2,1}$	$c_{2,2}$	$c_{2,3}$
$c_{3,0}$	$c_{3,1}$	$c_{3,2}$	$c_{3,3}$

Abb. 7: S-Box Transformation

Beispiel 8. *Wollen die S-Box Transformation von* $a = (0,0,0,0,0,0,1,1)^T$ *berechnen. Nach Beispiel 4 ist* $a^{-1} = b = (1,1,1,1,0,1,1,0)^T$.

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \bullet \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$c = (0,1,1,0,1,1,1,1)^T$

Definition 4. *Eine Funktion* $f : GF(2^8) \to GF(2^8)$ *heißt linear, wenn für alle* $a, b \in GF(2^8)$ *folgendes gilt:* $f(a \oplus b) = f(a) \oplus f(b)$.

Lemma 10. *Die Funktion* $f(x) = x^{-1}$ *ist nicht linear.*

Beweis. Sei $a = (0,0,0,0,0,0,1,1)^T$ und $b = (0,1,1,1,1,1,1,1)^T$, dann ist $a \oplus b = (0,1,1,1,1,1,0,0)^T$ und somit $f(a \oplus b) = (x^6 + x^5 + x^4 + x^3 + x^2)^{-1} = x^7 + x^5 + 1$ nach Beispiel 5. Nach Beispiel 4 ist $f(a) = (x+1)^{-1} = x^7 + x^6 + x^5 + x^4 + x^2 + x$. Nach Beispiel 6 ist $f(b) = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{-1} = x^7 + x^3 + x^2 + x$.
Und somit ist $f(a) \oplus f(b) = x^6 + x^5 + x^4 + x^3 \neq x^7 + x^5 + 1 = f(a \oplus b)$ □

Definition 5 (perfekt nichtlinear). *Die Funktion* $f(x) : GF(2^8) \to GF(2^8)$ *ist perfekt nichtlinear, wenn für jeden fixierten Punkt* $w \in GF(2^8)$ *die Differenz* $f(x+w) - f(x)$ *jeden Wert* $y \in GF(2^8)$ *für genau ein* $x \in GF(2^8)$ *annimmt.*
Quelle: [KAI, S. 381]

Definition 6 (fast perfekt nichtlinear 1). *Sei* $q = 2^n$ *und* $f : GF(q) \to GF(q)$. *Und sei nun* $0 \neq a \in GF(q)$, *dann ist* $H_a(f) = \{f(x) + f(x+a) | x \in GF(q)\}$. f *ist fast perfekt nichtlinear, wenn* $|H_a(f)| = \frac{1}{2}q$ *für alle* $0 \neq a \in GF(q)$.
Quelle: [Man, S. 8]

Definition 7 (fast perfekt nichtlinear 2). $f : GF(q) \to GF(q)$ *ist fast perfekt nichtlinear, genau dann wenn das System* $x + y = a, f(x) + f(y) = b$ *genau keine oder zwei Lösungen* (x, y) *für alle* $(a, b) \neq (0, 0)$ *besitzt.*
Quelle: [Man, S. 8]

Definition 8 (differential δ-uniform). *Die Funktion* $f(x) : GF(2^8) \to GF(2^8)$ *wird differential* δ*-uniform genannt, wenn für alle* $0 \neq a \in GF(2^8), b \in GF(2^8)$ *gilt:*

$$|\{x \in GF(2^8) | f(x+a) - f(x) = b\}| \leq \delta$$

Quelle: [Nyb, S. 58]

Fast perfekt nichtlinear wird oft mit APN, almost perfect nonlinear, abgekürzt.

Lemma 11. *Die Inversionabbildung* $f(x) = x^{-1}$ *mit* $f : GF(2^8) \to GF(2^8)$ *ist nicht perfekt linear und auch nicht fast perfekt nichtlinear. Aber sie ist vierfach differential-uniform.*

Beweis. Dieser Beweis ist von Kaisa Nyberg [Nyb, S. 62].
Sei $a, b \in GF(2^8)$ und $a \neq 0$, nun betrachte man die Gleichung $(x+a)^{-1} - x^{-1} = b$ (1). Angenommen $x \neq 0$ und $x \neq -a$. Dann ist (1) unter Anwendung von
$x \cdot \underbrace{(x+a) \cdot (x+a)^{-1}}_{=1} - (x+a) \cdot \underbrace{x \cdot x^{-1}}_{=1} = b \cdot x \cdot (x+a)$
äquivalent zu $0 = bx^2 + bax - a$ (2). Und (2) hat höchstens zwei Lösungen in $GF(2^8)$. Wenn nun $x = 0$ oder $x = -a$ eine Lösung zu (1) ist, dann sind auch beide Lsg. zu (2) mit $b = a^{-1}$, denn Null ist zu sich selbst invers und somit $(0+a)^{-1} - 0^{-1} = a^{-1} - 0 = a^{-1}$ und $(-a+a)^{-} - 1 - (-a)^{-1} = 0^{-1} + a^{-1} = a^{-1}$. In diesem Fall ist dann (2) equivalent zu: $x^2 + ax - a^2 = 0$ (3), denn $a^{-1}x^2 + a \cdot a^{-1}x - a = 0 \to_{|\cdot a} a \cdot a^{-1}x^2 + ax - a^2 = a \cdot 0 = 0$. Zeigen nun, dass (3) auch noch zwei Lösungen besitzt und somit (1) vier Lösungen hat. Lass uns nun (3) quadrieren: $0 = 0^2 = (x^2 + ax - a^2)^2 = x^4 + 2ax^3 - 2a^2x^2 + a^2x^2 - 2a^3x + a^4 \underset{+a^4 = -a^4}{=} x^4 + 2ax^3 - a^2x^2 - 2a^3x - a^4$ und nun wählen wir x so, dass $x^2 = ax + a^2$, daraus folgt nun: $(ax+a^2)^2 + 2ax(ax+a^2) - a^2(ax+a^2) - 2a^3x - a^4 = a^2x^2 + 2a^3x + a^4 + 2a^2x^2 + 2a^3x - a^3x - a^4 - 2a^3x - a^4 = 3a^2x^2 + a^3x - a^4 = 3a^2(ax+a^2) + a^3x - a^4 = 3a^3x + 3a^4 + a^3x - a^4 = 4a^3x + 2a^4 = a^3x + a^4 + 3a^3x + a^4 = a^2(ax+a^2) + 3a^3x + a^4 = a^2x^2 + 2a^3x + a^4 + a^3x = (ax+a^2)^2 + a^3x = x^4 + a^3x = x(x^3 + a^3)$ Damit suchen wir nun die Lösungen von $x(x^3+a^3) = 0$ (4). Da nun 3 ein Teiler von $2^8 - 1$ ist und $85 = \frac{255}{3}$, lösen $x = a^{1+85} = a^{86}$ und $x = a^{1+2 \cdot 85} = a^{171}$ die Gleichung (4), da in jedem Körper K, $K \backslash \{0\}$ eine abelsche Gruppe G mit $|K| - 1$ Elementen ist und für jedes Element $g \in G$ gilt: $g^{|G|} = 1$. In unserem speziellen Fall hat die Multiplikative Gruppe G vom Körper $GF(2^8)$ 255 Elemente, denn das Nullpolynom gehört nicht dazu, und somit gilt $a^{255} = 1$. $x^3 + a^3 = (a^{1+\frac{255}{3}})^3 + a^3 = a^{1 \cdot 3} \cdot \underbrace{a^{\frac{255}{3} \cdot 3}}_{=1} + a^3 = a^3 + a^3 = 0$
analog gilt es für $x = a^{1+2 \cdot \frac{255}{3}} \to_{\cdot 3} = a^3 \cdot (a^{255})^2 = a^3 \cdot 1^2 = a^3$. Es gibt nur diese zwei neuen Lösungen, denn die Lösung $x = 0$ haben wir schon und $x = a^{1+3 \cdot 85} = a^{256} = a \cdot a^{255} = a = -a$ und diese Lösung haben wir auch schon gefunden.
Damit lösen $x_1 = 0, x_2 = -a, x_3 = a^{86}, x_4 = a^{171}$ für jedes $a \neq 0$ die Gleichung $(x+a)^{-1} - x^{-1} = a^{-1} = b$ und somit ist $\delta = 4$ von $x \to x^{-1}$. □

Um ein Gefühl für das δ *in differential* δ*-uniform zu bekommen, betrachten wir nun einfach den* δ*-Grad der linearen Funktion* $f(x) = x$*. Sei* $a \neq 0$*, dann ist* $b = f(x+a) - f(x) = x + a - x = a$*. Sei nun* $b = a$*, dann erfüllen alle* 256 *Elemente in GF(*2^8*), diese Gleichung. Dies bedeutet die lineare Funktion* $x \to x$ *ist differential* 256*-uniform, und somit sehr anfällig für differentiale Kryptoanalysis.*

Nyberg zeigt auch, dass differential 2-uniforme Abbildungen in $GF(2^n)$ *fast perfekt lineare Permutationen sind. Also, dass Definition 1 gleich Definition 2 ist, denn ist* $x+y = a \to y = a-x = x+a$ *und somit lautet dann bei uns die zweite Gleichung* $f(x) + f(x+a) = f(x+a) - f(x) = b$*, denn in unserem Körper ist* $-a = +a$*. Da wir aber vier Lösungen für* $b = a^{-1}$ *kennen, ist die Inversionsabbildung nicht fast perfekt nichtlinear. Nun ist die Inversionsabbildung nicht APN, da aber* $\delta = 4$ *auch sehr klein ist, ist die Nichtlinearität groß genug. Da die Inversionsabbildung mehrfach angewendet wird, es gibt ja mindestens zehn Runden, ist die S-Box auch praktisch immun gegen lineare Kryptoanalyse. Da aber die Inversionsabbildung eine sehr einfache algebraische Struktur besitzt, wird danach noch eine affine Abbildung ausgeführt, um nicht anfällig gegen Interpolationsangriffe, so genannte XSL-Attacken, zu sein.*

6.2.2 Reihenverschiebung

Bei der Reihenverschiebung werden die Zeilen eines Blockes zyklisch verschoben. Um wieviele Spalten eine Zeile nach links verschoben wird, hängt nur von der Blockgröße Nb ab:

Nb	*C1*	*C2*	*C3*
4	*1*	*2*	*3*
6	*1*	*2*	*3*
8	*1*	*3*	*4*

In unserem Beispiel ist die Blockgröße 128 Byte, also Nb=4 und dann sieht die Transformation wie in Abbildung 8 aus:

$c_{0,0}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$
$c_{1,0}$	$c_{1,1}$	$c_{1,2}$	$c_{1,3}$
$c_{2,0}$	$c_{2,1}$	$c_{2,2}$	$c_{2,3}$
$c_{3,0}$	$c_{3,1}$	$c_{3,2}$	$c_{3,3}$

$\xrightarrow{\textit{Reihenverschiebung}}$

$c_{0,0}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$
$c_{1,1}$	$c_{1,2}$	$c_{1,3}$	$c_{1,0}$
$c_{2,2}$	$c_{2,3}$	$c_{2,0}$	$c_{2,1}$
$c_{3,3}$	$c_{3,0}$	$c_{3,1}$	$c_{3,2}$

Abb. 8: Reihenverschiebung Transformation

Diese Transformation sorgt bei Anwendung über mehrere Runden für eine hohe Diffusion.

6.2.3 MischeSpalten Transformation

Jede Spalte $s_j = (s_{0,j}, s_{1,j}, s_{2,j}, s_{3,j})^T$ *in der aktuellen Zustandsmatrix wird als Polynom* $s_j(x) = s_{3,j}x^3 + s_{2,j}x^3 + s_{2,j}x^3 + s_{1,j}x + s_{0,j}$ *identifiziert. Das Ergebnis der Transformation ist* $S_j(x) = s_j(x) \otimes c$. *Mit* $c(x) = 0x03x^3 + 0x01x^2 + 0x01x + 0x02$. *Da das Polynom* $c(x)$ *nach Lemma 9 invertierbar ist, ist diese Operation auch wieder umkehrbar anwendbar. Nach Lemma 8 lässt sich diese Operation auch wieder in Matrix-Schreibweise darstellen:*

$$\begin{pmatrix} S_{0,j} \\ S_{1,j} \\ S_{2,j} \\ S_{3,j} \end{pmatrix} = \begin{pmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{pmatrix} \bullet \begin{pmatrix} s_{0,j} \\ s_{1,j} \\ s_{2,j} \\ s_{3,j} \end{pmatrix}$$

Diese Transformation sorgt für eine Diffusion innerhalb der Spalten des aktuellen Zustandes.

6.2.4 RundenSchlüsselAddition

In dieser Operation wird der Rundenschlüssel mit einer einfachen $\oplus$ *Operation zum Zustand hinzuaddiert. Der Rundenschlüssel wird vom Chiffre-Schlüssel abgeleitet. Der Rundenschlüssel ist genauso lang wie Blocklänge Nb. Dies ist die eigentliche 'Verschlüsselung', denn nur in dieser Operation wird der Geheimtext vom Benutzerschlüssel abhängig gemacht. Figur 9 stellt diese Operation nochmal grafisch dar.*

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\oplus$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

$=$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Abb. 9: RundenSchlüsselAddition

6.2.5 Schlüsselerweiterung

Die ersten Nk, bei uns ist Nk=4, Worte des erweiterten Schlüssels sind die des orginalen AES-Schlüssels. Die weiteren Worte ergeben sich nach folgenden Schema:

Listing 2: Schlüsselerweiterungs-Algorithmus in Pseudo-Java-Code

```
/**
```

```
 * @param AES_Schluessel Byte-Array mit 16 Elementen,
 *          also 16*8 Bit = 128 Bit, verwenden hier AES-128
 * @return erweiterterSchluessel Integer-Array oder auch Word-Array
 *          mit 4*(Nr+1) =\ 4*11 = 44 Elementen, also 1408 Bit
*/
int[] Schluesselerweiterung(byte AES_Schluessel[]) {
  // Rundenkonstante ist das Wort (RC[i],0,0,0) mit RC[i] = x^(i-1)
  int[] Rundenkonstante = new int[] {
    0x01 << 24; 0x02 << 24; 0x04 << 24; 0x08 << 24; 0x10 << 24; ...
  };
  int [] erweiterterSchluessel = new int[44];
  for(int i=0;i<4;i++) {
    erweiterterSchluessel[i] =
      AES_Schluessel[4*i]   << 24 +
      AES_Schluessel[4*i+1] << 16 +
      AES_Schluessel[4*i+2] << 8  +
      AES_Schluessel[4*i+3];
  }
  for(int i=4;i<44;i++) {
    int tmp = erweiterterSchluessel[i-1];
    if(i % 4 == 0) {
      // ^ ist bitweise XOR-Operation
      temp = ByteSubstitution(Rotiere(temp)) ^ Rundenkonstante[i / 4];
    }
    erweiterterSchluessel[i] = erweiterterSchluessel[i-4] ^ tmp;
  }
  return erweiterterSchluessel;
}
int Rotiere(int wort) {
  // (a_0,a_1,a_2,a_3) -> (a_1,a_2,_a_3,a_0)
  int a_0 = (wort & 0xFF000000) >> 24;
  return (wort & 0x00FFFFFF) << 8) + a_0;
}
```

Abbildungsverzeichnis

Listings

References

Books

[Buc04] Johannes Buchmann. *Einführung in die Kryptographie*. 3. Aufl. Berlin [u.a.]: Springer, 2004. ISBN: 3540405089.

[Nyb] K. Nyberg. „Differentially uniform mappings for cryptography“ ().

[KAI] KAISA NYBERG. „Perfect nonlinear S-boxes,D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 378-386, 1991“ ().

[Man] Mandi S. Maxwell. „Almost Perfect Nonlinear functions and related combinatorial structures“ ().

[Spe] Spektrum der Wissenschaft. „Dossier: Kryptographie. Nr. 4/2001“ (), S. 90.

Online resources

[Dae09] Joan Daemen. *The Rijndael Block Cipher*. 3.09.1999.
URL: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

[SMS07] Rajan Mishra Shashi Mehrotra Seth. *Comparative Analysis Of Encryption Algorithms For Data Communication*. 15.07.2011.
URL: http://www.ijcst.com/vol22/2/shashi.pdf.

[wik10] wikiversity. *Endliche Körper/Existenz und Eindeutigkeit/Fakt mit Beweisklappe – Wikiversity*. 18.10.2012.
URL: http://de.wikiversity.org/wiki/Endliche_K%C3%B6rper/Existenz_und_Eindeutigkeit/Fakt_mit_Beweisklappe.

[Wik12a] Wikipedia. *Advanced Encryption Standard*. Hrsg. von Wikipedia. 1.12.2012.
URL: http://de.wikipedia.org/w/index.php?oldid=111101878.

[Wik12b] Wikipedia. *Feistel cipher - Wikipedia, the free encyclopedia*. Hrsg. von Wikipedia. 2.12.2012.
URL: http://en.wikipedia.org/w/index.php?oldid=526007726.