IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 5: Symmetrische Kryptosysteme

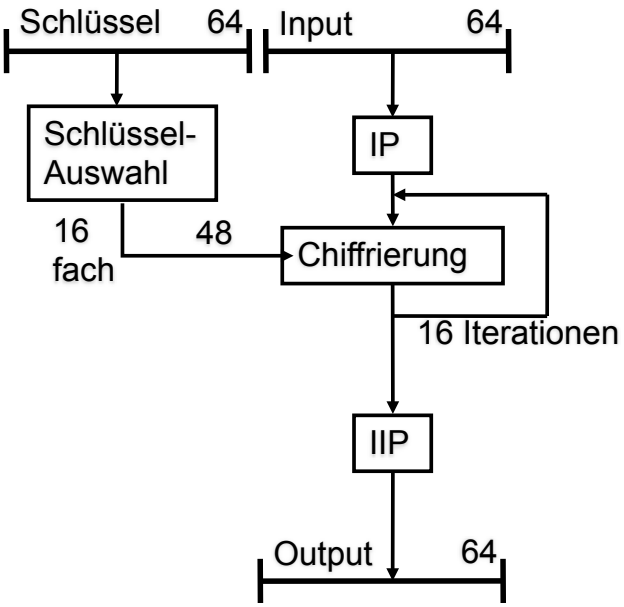
Inhalt

- Symmetrische Kryptosysteme
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

DES (Data Encryption Standard)

- 1977 vom NBS (National Bureau of Standards) heute National Institute of Standards (NIST) in USA zum Standard erklärt
- 2002 durch AES (Advanced Encryption Standard) ersetzt
- DES entwickelt von IBM aus dem 128 Bit Verfahren LUCIFER
- Klassifikation:
  - Symmetrisches Verfahren
  - mit Permutation, Substitution und bitweiser Addition modulo 2
  - Blockchiffre mit 64 Bit großen Ein- und Ausgabeblöcken
  - Schlüssellänge 64 Bit, davon 8 Paritätsbits, d.h. effektive Schlüssellänge 56 Bit

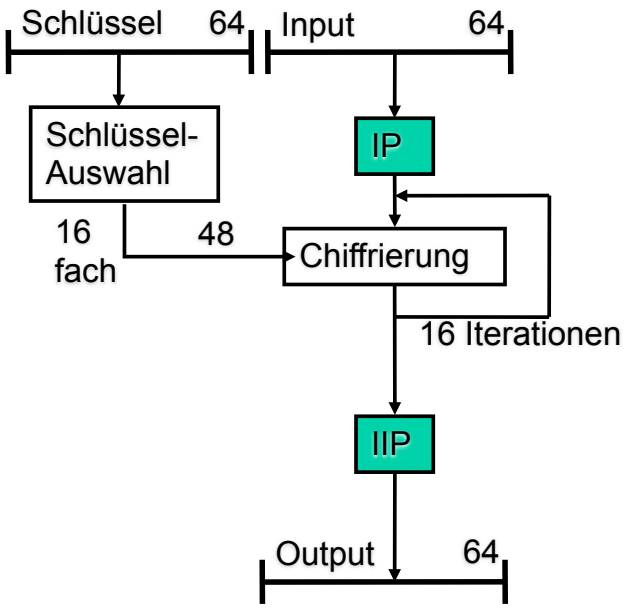
DES Funktion: Grundschema



- Ablauf der Verschlüsselung
1. Initialpermutation (IP) des Input-Blocks
2. 16 schlüsselabhängige Iterationen
   - 48 Bit lange Teilschlüssel
   - werden aus 64 Bit Schlüssel generiert
3. Inverse Initialpermutation (IIP) als Ausgangspermutation

- Entschlüsselung analog zur Verschlüsselung mit Schlüssel in umgekehrter Reihenfolge im Schritt 2.

DES Funktion: Grundschema



- Wie arbeiten Initialpermutation (IP) und Inverse Initialpermutation (IIP)?

DES: IP und IIP

- Initialpermutation IP

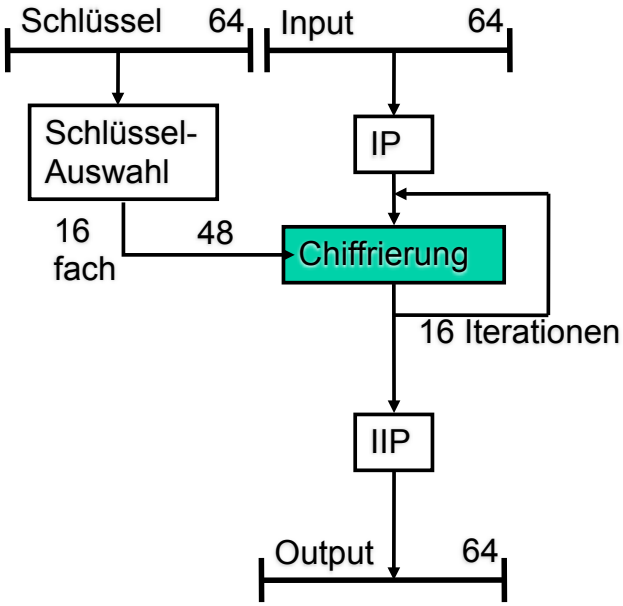
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- Inverse Initialpermutation IIP

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

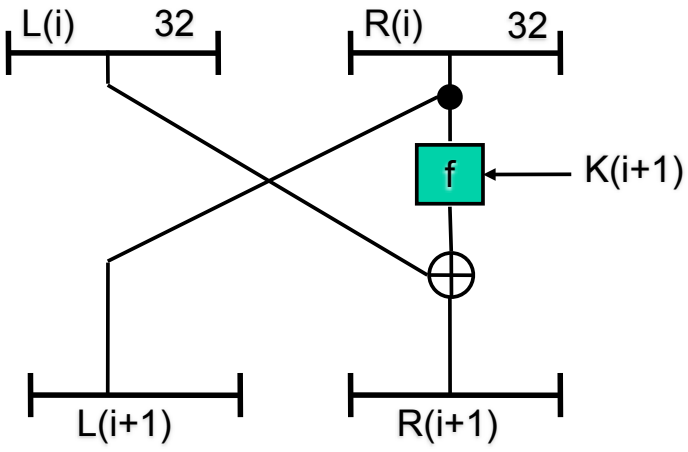
- D.h. aus Bit 58 des Input wird Bit 1, aus Bit 50 wird Bit 2,....., aus Bit 7 wird Bit 64

DES Funktion: Grundschema



DES Funktion: Verschlüsselungsiteration

- Ein Schritt (Runde) der Chiffrierung:

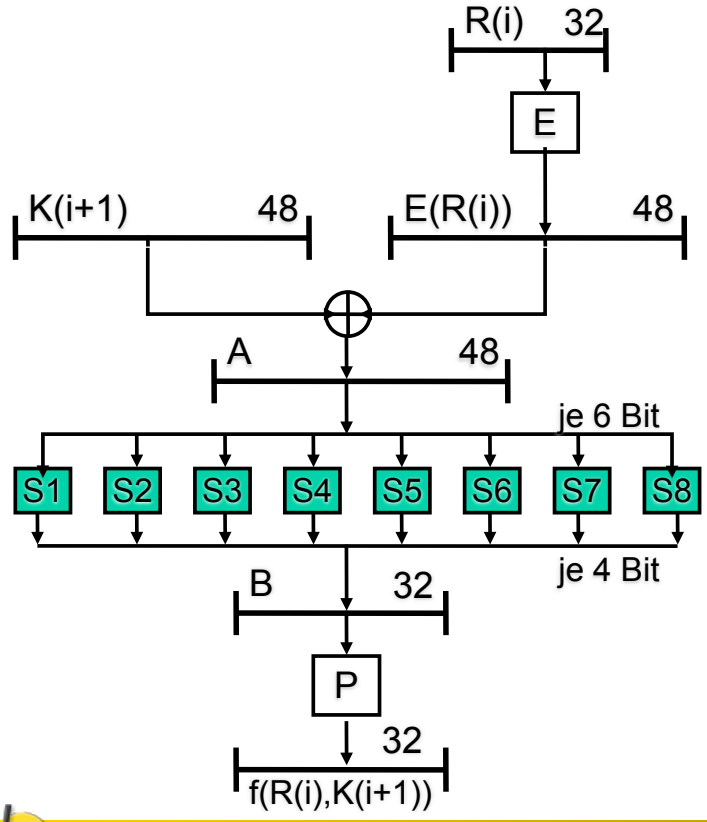


⊕ Addition modulo 2; entspr. XOR

- Verschlüsselungsblock (64 Bit) wird in linken (L) und rechten (R) Block a 32 Bit aufgeteilt
- Anwendung der Verschlüsselungs-iteration:
  L(0) = L und R(0) = R
  L(i+1) = R(i)
  R(i+1) = L(i) XOR f(R(i),K(i+1))

  für i=0,....,15
- Funktion f stellt Kern des Verfahrens dar.

DES Funktion f



- Rechter 32 Bit Input Block wird mittels Expansion E auf 48 Bit expandiert
- XOR Verknüpfung mit dem (Runden-) Schlüssel zum 48 Bit Block A
- A wird in 8 Blöcke zu 6 Bit aufgeteilt
- Jeder dieser Blöcke wird durch S-Box (Substitution) in 4 Bit Ausgabeblöcke (nichtlinear) abgebildet
- Konkatenation der acht 4 Bit Blöcke ergibt Block B der noch der Ausgangspermutation P unterworfen wird

Expansion E und Permutation P

- Expansion E:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

  - Bit 32 aus R(i) wird Bit 1 von E(R(i))

- Ausgangspermutation P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

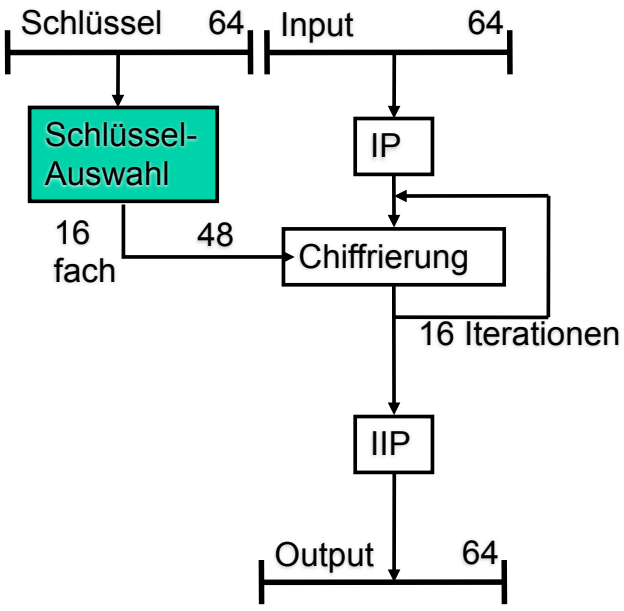
DES S-Boxen

- 6 Bit Input Block (i1,i2,i3,i4,i5,i6) wird auf 4 Bit Outputblock (o1,o2,o3,o4) abgebildet:
  - Redundante Bits (i1,i6) des Inputblocks bestimmten die Zeile der entspr. S-Box
  - Bits (i2,i3,i4,i5) bestimmen Spalte
  - Element in der Matrix bestimmt Outpublock
- Bsp. S-box S1:

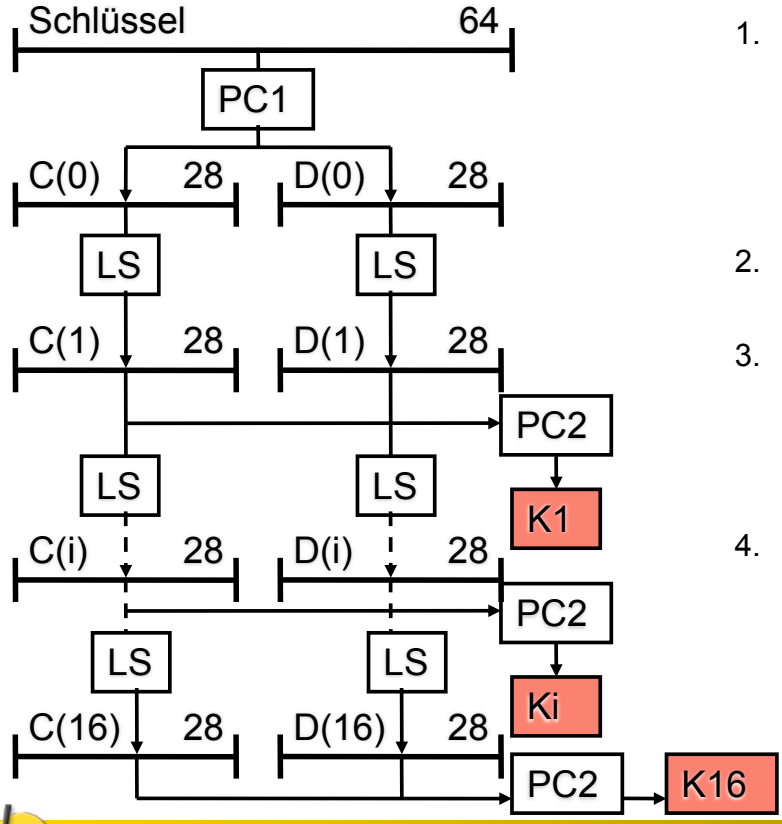
(i1,i6) \ (i2,i3,i4,i5)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- Beispiel
  - S-Box S1
  - Input (0,1,1,0,1,1)
  - Zeile (0,1) = 1
  - Spalte (1,1,0,1) = 13
  - Output (5) = (0,1,0,1)

DES Funktion: Grundschema

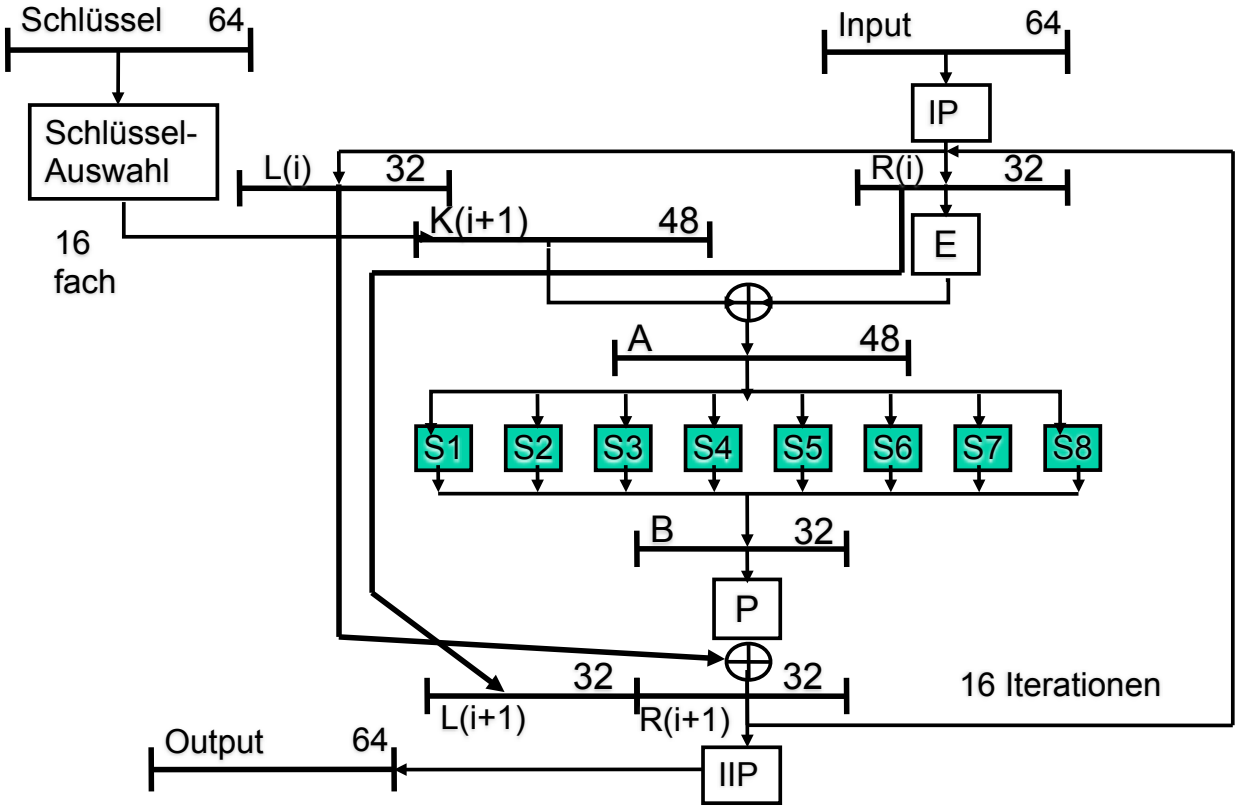


DES Schlüsselauswahl



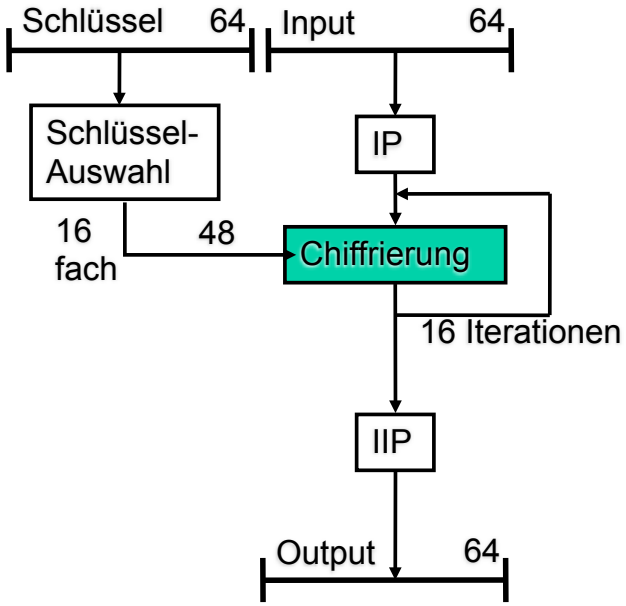
1. 64 Bit Schlüssel wird Permuted Choice 1 (PC1) unterworfen:
   - Key wird auf 56 relevante Bits gekürzt (jedes 8. Bit Parity)
   - Key wird permutiert
2. Schlüssel wird in zwei Teile a 28 Bit aufgeteilt
3. Blöcke werden zyklisch nach links geschiftet
   - In Runde 1,2,9 u. 16 um 1 Bit
   - 2 Bit sonst
4. Teilblöcke werden zusammen-gefasst und PC2 unterworfen:
   - Entfernen der Bits 9,18,22,25,35,38,43 u. 56
   - Permutation der verbleibenden 48 Bit

DES: Zusammenfassung



DES Entschlüsselung

- Es gilt D = E
- DES wird für Ver- und Entschlüsselung prinzipiell gleich verwendet, außer
- Umkehrung der Schlüsselreihenfolge
- In Runde i wird K(16-i) verwendet



DES Stärken und Schwächen

- Starker **Avalanche-Effekt** (Lawineneffekt; große Streuung) durch S-Boxen und Permutation P:
  Kleine Änderungen in der Eingabe, die nur eine S-Box betreffen breiten sich schnell aus.
  Eine Änderung eines Bits in der Eingabe verursacht eine Änderung von durchschnittlich 50% der Ausgabe
- 16 Iterationen:
  Known-plaintext Angriff auf DES mit < 16 Runden immer effizienter als Brute force
- Stark gegen analytische Angriffe
  Differentielle Kryptanalyse braucht 2^{47} gewählte Klartexte (chosen-pl.t.)

- (teilweise) geheimes Design
- Deutlich zu geringe Schlüssellänge
  Schlüsselraum der Größe 2^{56}
- 4 schwache Schlüssel mit:
  DES(DES(x,K),K) = x
- 6 semi-schwache Schlüsselpaare:
  DES(DES(x,K),K‘) = x
- Differentielle Kryptanalyse lässt sich in der Komplexität reduzieren auf 2^{37}

- Optimiert auf Implementierung in Hardware:
  Initialpermutation IP und inverse IP verbessern die Sicherheit nicht, sondern erhöhen nur den Aufwand für Software-Implementierungen

DES Varianten: Double und Tripple DES

- Double-DES:
  - DES(DES(m,K1),K2)
- Erwartete Komplexität:
  - bei Schlüssellänge n

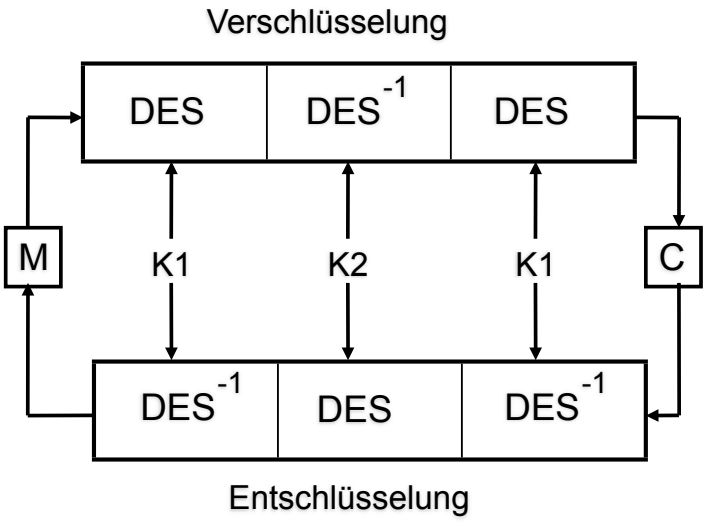
$$2^{2n}$$

- Merkle und Hellman haben gezeigt, dass ein Known-Plaintext Angriff möglich ist mit

$$2^{n+1}$$

  - Allerdings liegt der Speicherverbrauch bei 2^n Blöcken, bei DES 2^56 * 64 Bit, d.h. 10^17 Byte, d.h. im Bereich von Peta Byte
- D.h. doppelte Ausführung von DES bringt **KEINE** merkliche Steigerung der Sicherheit

- Triple-DES



- Komplexität

$$2^{2n}$$

Einschub: SSL/TLS Renegotiation Vulnerability

- Protokollschwäche im SSL/TLS Protokoll erlaubt Man-in-the-Middle Angriff
- Betroffene Software: Alle Systeme die auf SSL/TLS aufsetzen und Client-basierte Authentisierung per Zertifikat machen, z.B.: https, vpn-Software, smtps, ...
- Schwachstelle:
  - SSL/TLS erlaubt während der Sitzung verwendete Verfahren zu wechseln oder eine Re-Authentisierung zu verlangen (Renegotiation)
  - Protokollschwäche führt dazu, dass für Angreifer der Zugriff auf den Verkehr hat Man-in-the-Middle Angriff möglich wird
- Lösung:
  - derzeit keine
  - Workaround: Renegotiation deaktivern; Problem von Seiteneffekten
  - IETF arbeitet an einer Protokollaktualisierung
- weitere Infos: http://isc.sans.org/diary.html?storyid=7534

Vortragsreihe: Professioneller IT-Betrieb

- Vortrag 19.11.09; 14:15 - 16:00 Uhr; LRZ, Boltzmannstr. 1, Garching

- Abtrennung eines Teilkonzerns; Sascha Haupt (Fa. GeNUA)
  - Münchner Konzern verkauft Tochter an arabischen Investor
  - Netze müssen getrennt werden
  - Projekt: Aufbau einer Firewall Infrastruktur bei der Tochter
  - Migration bestehender FW-Regeln
  - Umzug von Diensten (ohne grössere Ausfallzeiten)
- Fa. GeNUA (Gesellschaft für Netzwerk- und Unix-Administration mbH)
  - IT Sicherheitsspezialist
  - Sitz in Kirchheim bei München
  - eigene Firewall-Produkte und zugehörige Dienstleistungen

Vortragsreihe: Professioneller IT-Betrieb

- 26.11.09:
  - Robert Koch (Uni der Bundeswehr):
    IDS Problemfelder und neue Ansätze;
  - Bernhard Schmidt (LRZ):
    IPv6 im Münchner Wissenschaftsnetz
- 03.12.09: Dr. Michael Brenner (LRZ):
  IT-Service-Management am LRZ: People, Process, Technology
- 10.12.09: Georg Mey (NetApp):
  Konzepte moderner Speichersysteme
- 07.01.10:
  - Dr. Ernst Boetsch (LRZ):
    Security-Bausteine für das Münchner Wissenschaftsnetz
  - Florian Gleixner (LRZ):
    Umfassende Serverüberwachung mit Nagios und SEC

Vortragsreihe: Professioneller IT-Betrieb

- 14.01.10: Christian Lotz (plan42 GmbH):
  ITIL V3 zwischen Anspruch und Realität
- 21.01.10: Marc Lindike (Flughafen München GmbH):
  ITIL-Erfahrungen und -Aktivitäten beim Münchner Flughafen
- 28.01.10:
  - Dr. Matthias Brehm (LRZ):
    Höchstleistungsrechner und ihre Anwendungen;
  - Dr. Bernd Reiner (LRZ):
    Das Archiv- und Backup-System des LRZ
- 04.02.10: Dr. Werner Degenhardt (LMU; Dept. Psychologie)
  Der menschliche Faktor der Informationssicherheit
- 11.02.10: Michael Storz (LRZ):
  Das Mailsystem des LRZ

Inhalt

- Symmetrische Kryptosysteme
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES); Historie

- 1997 öffentliche Ausschreibung des Dept. Of Commerce (Request for Candidate Algorithms for AES):
  - Algorithmus öffentlich und nicht klassifiziert,
  - Mindestblocklänge 128 Bit, Schlüssellänge 128, 192 und 256 Bit
  - Weltweit frei von Lizenzgebühren,
  - nutzbar für 30 Jahre, effizient sowohl in SW als auch versch. HW
- Dreistufiges (Vor-)Auswahlverfahren
  1. Pre-Round 1 (1/97 – 7/98)
     - Call for Candidates
  2. Round 1 (8/98 – 4/99)
     - Vorstellung, Analyse und Test
     - Auswahl der Kandidaten für Round 2
  3. Round 2 (8/99 – 5/2000)
     - Analyse und Tests
     - Auswahl der Finalisten
- Endgültige Auswahl durch NIST

AES Kandidaten

- Pre-Round 1: 21 Kandidaten, 6 aus formalen Gründen abgel.

Algo.	Land	Autor(en)	Algo.	Land	Autor(en)
CAST-256	Kanada	Entrust	MAGENTA	Deutschland	Deutsche Telekom
CRYPTON	Korea	Future Systems	MARS	USA	IBM
DEAL	Kanada	R. Outbridge, L. Knudsen	RC6	USA	RSA Laboratories
DFC	Frankreich	CNSR	RIJNDAEL	Belgien	J. Daeman, V. Rijmen
E2	Japan	NTT	SAFER+	USA	Cylink
FROG	Costa Rica	TecApro	SERPENT	UK, Norwegen, Israel	R. Anderson, E. Biham u.a.
HPC	USA	R.Schroeppel	TWOFISCH	USA	B. Schneier, J. Kelsey, u.a.
LOKI97	Australien	L. Brown, J. Pieprzyk u.a.			

AES: Round 2 Finalisten und Ergebnis

- Finalisten der Runde 2:

MARS	USA	IBM
RC6	USA	RSA Laboratories
RIJNDAEL	Belgien	J. Daeman, V. Rijmen
SERPENT	UK, Norwegen, Israel	R. Anderson, E. Biham, L. Knudsen
TWOFISCH	USA	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Feruson

- 2. Oktober 2000: Rijndael wird gewählt
- 26. Nov. 2001: Veröffentlichung des FIPS-197 (Federal Information Processing Std.) durch NIST (National Institute for Standards and Technology)
- 26. Mai 2002: Inkrafttreten des Standards
- Informationen: `www.nist.gov/aes` mit Link auf AES-Homepage

AES

- Variable Blocklänge: 32*Nb Bits
- Variable Schlüssellänge: 32*Nk Bits
- Nb und Nk aus {4-8}; im Standard eingeschränkt auf 4,6 oder 8
- Variable Rundenanzahl Nr mit Nr = max(Nb, Nk) + 6
- Folgende Beispiele für Nb=Nk=4
- Rijndal arbeit auf sog. States:
  Input Bytes in0,in1,...,in15 werden in State kopiert:

input bytes

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

→

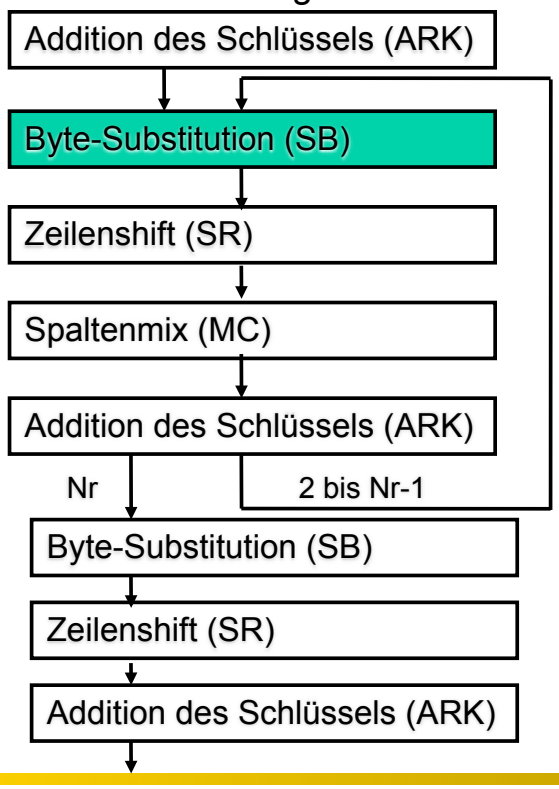
State array

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

- Runden arbeiten auf den States

AES: Ver- und Entschlüsselung

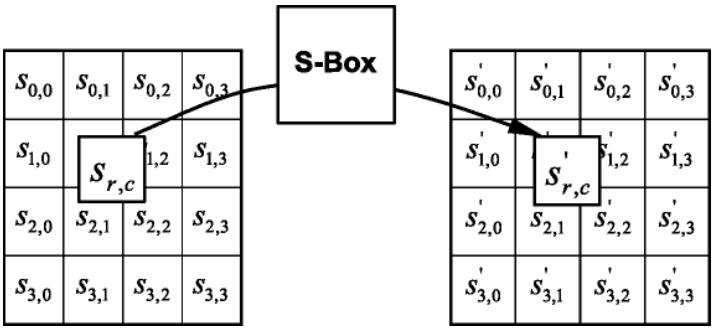
- Verschlüsselung



- Runden arbeiten auf sog. States
- Verschlüsselung
  - Ablauf der Runden 1 bis Nr-1:
    1. Byte-Substitution (`SubBytes`, SB)
    2. Zeilenshift (`ShiftRows`, SR)
    3. Spaltenmix (`MixColumns`, MC)
    4. Addition d. Rundenschlüssels (`AddRoundKey`, ARK)
- Entschlüsselung:
  - Runde 1 bis Nr-1:
    1. Addition d. Rundenschlüssels
    2. Inverser Spaltenmix
    3. Inverser Zeilenshift
    4. Inverse Byte-Substitution
- Letzte Runden Nr analog; aber **ohne** Spaltenmix

AES: Bytesubstitution (`SubBytes()`)

- Angewandt auf jedes Byte des State



- Byte S(r,c) wird als Kodierung eines Polynoms im Körper GF (2^8) aufgefasst
- Substitution:
  1. Bestimme multiplikatives Inverses von S(r,c) in GF(2^8)
  2. Affine Transformation des Inversen:
     - Matrixmultiplikation
     - XOR mit {63}

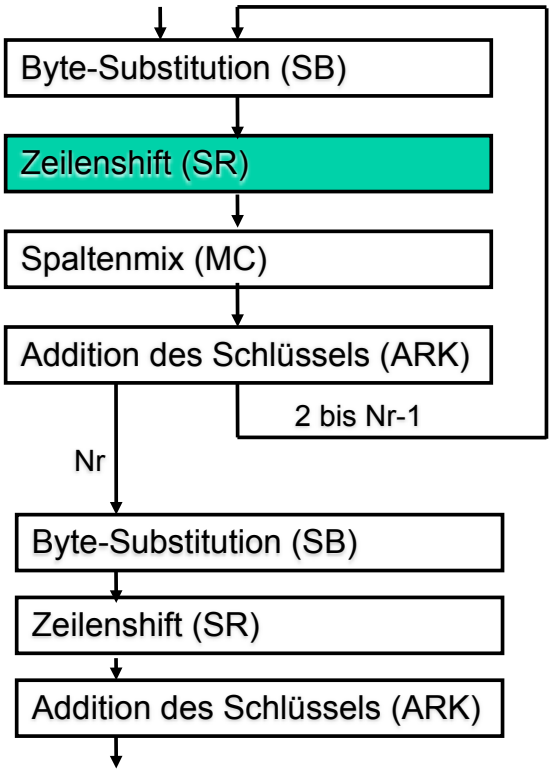
AES: Bytesubstitution Implementierung

- Vorausberechnung für alle 256 möglichen Polynome und Speicherung in S-Box (aus FIPS197)

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

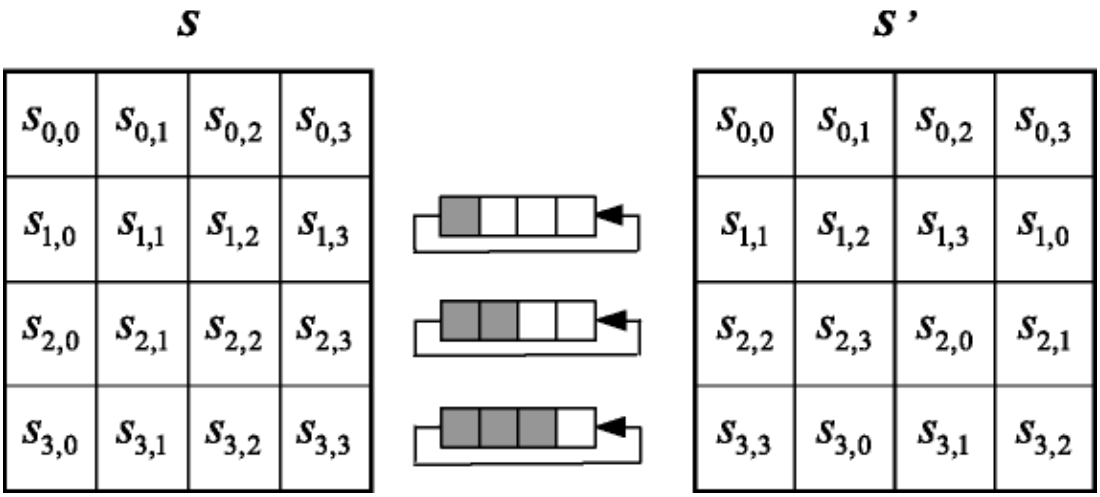
S-box: substitution values for the byte xy (in hexadecimal format).

AES: Verschlüsselung

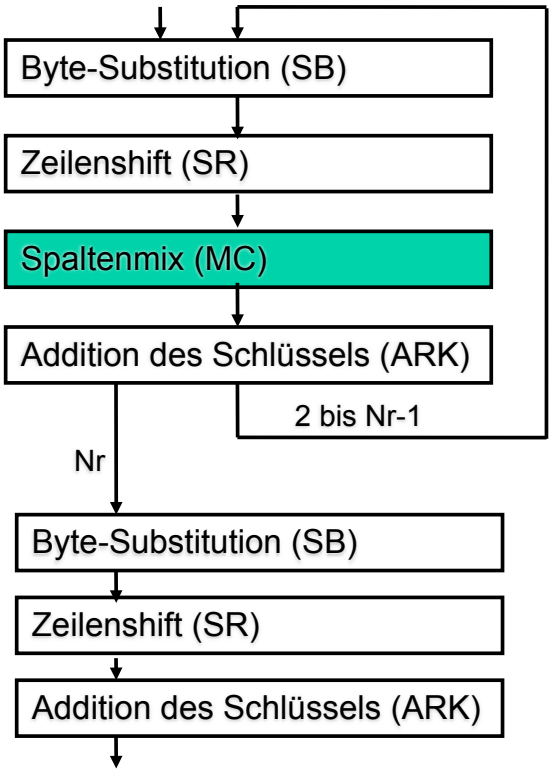


AES Zeilenshift (`ShiftRows()`)

- Zyklischer Shift der letzten drei Zeilen des State:Z
  - Zeile 1 bleibt unverändert
  - Zeile 2 um 1 Byte
  - Zeile 3 um 2 Byte
  - Zeile 4 um 3 Byte

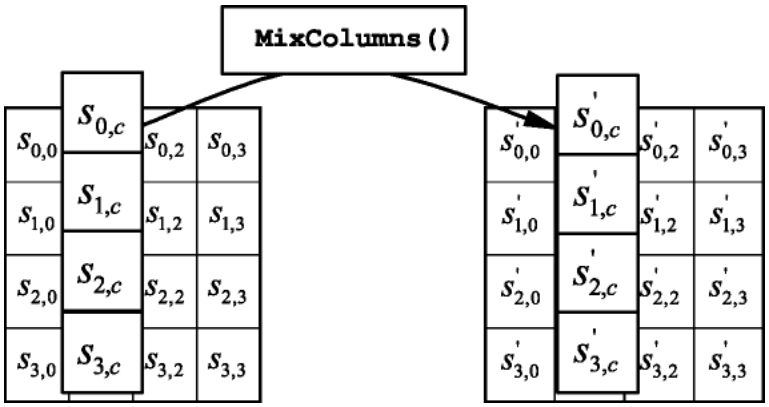


AES: Verschlüsselung



AES Spaltenmix (`MixColumns()`)

- Angewendet auf jede Spalte des State



- Jede Spalte wird als Polynom vom Grad 3 mit Koeffizienten aus GF(2^8) aufgefasst:
  - Multiplikation mit dem festen Polynom a(x) modulo x^4+1

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} .$$

AES Spaltenmix

- Darstellbar als Matrizenmultiplikation:

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{für } 0 \le c < Nb.$$

Ausmultipliziert:

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

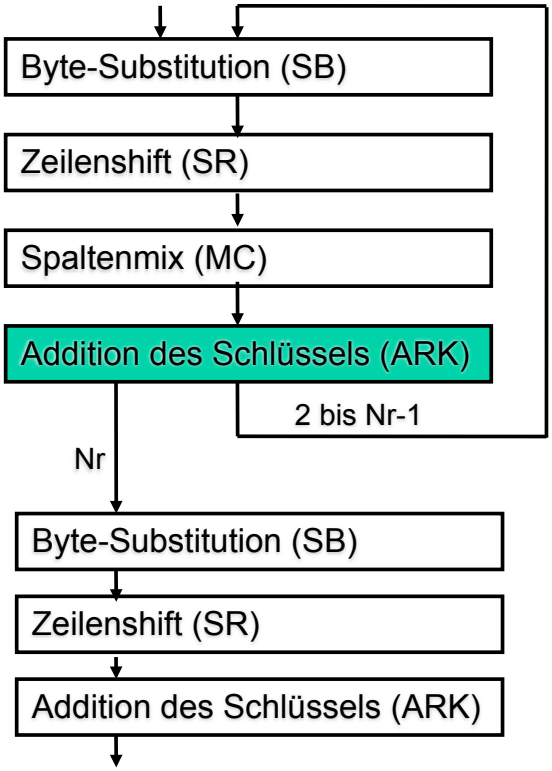
$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}).$$

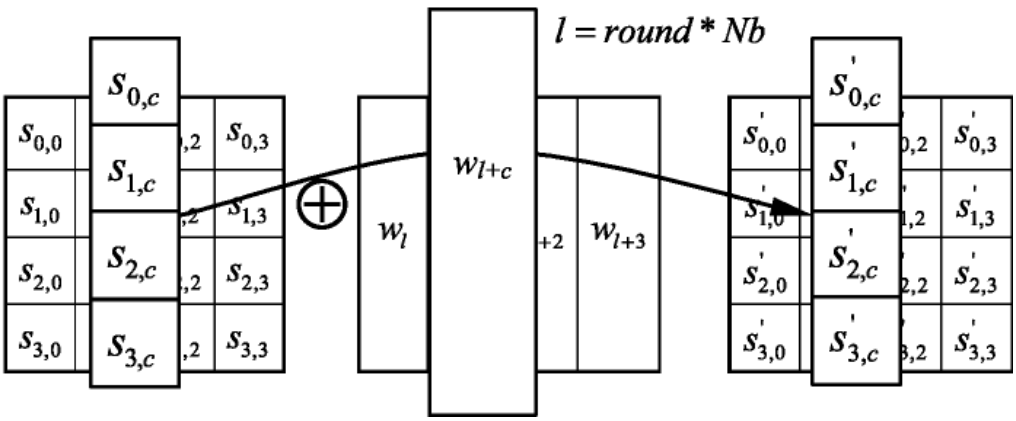
- $\bullet$ ist definiert in $GF(2^8)$ über irreduzibles Polynom $m(x) = x^8 + x^4 + x^3 + x + 1$

AES: Verschlüsselung



AES: Addition des Rundenschlüssels

- Funktion `AddRoundKey()`
- Jede Spalte des State wird mit einem „Wort“ des Rundenschlüssels XOR verknüpft

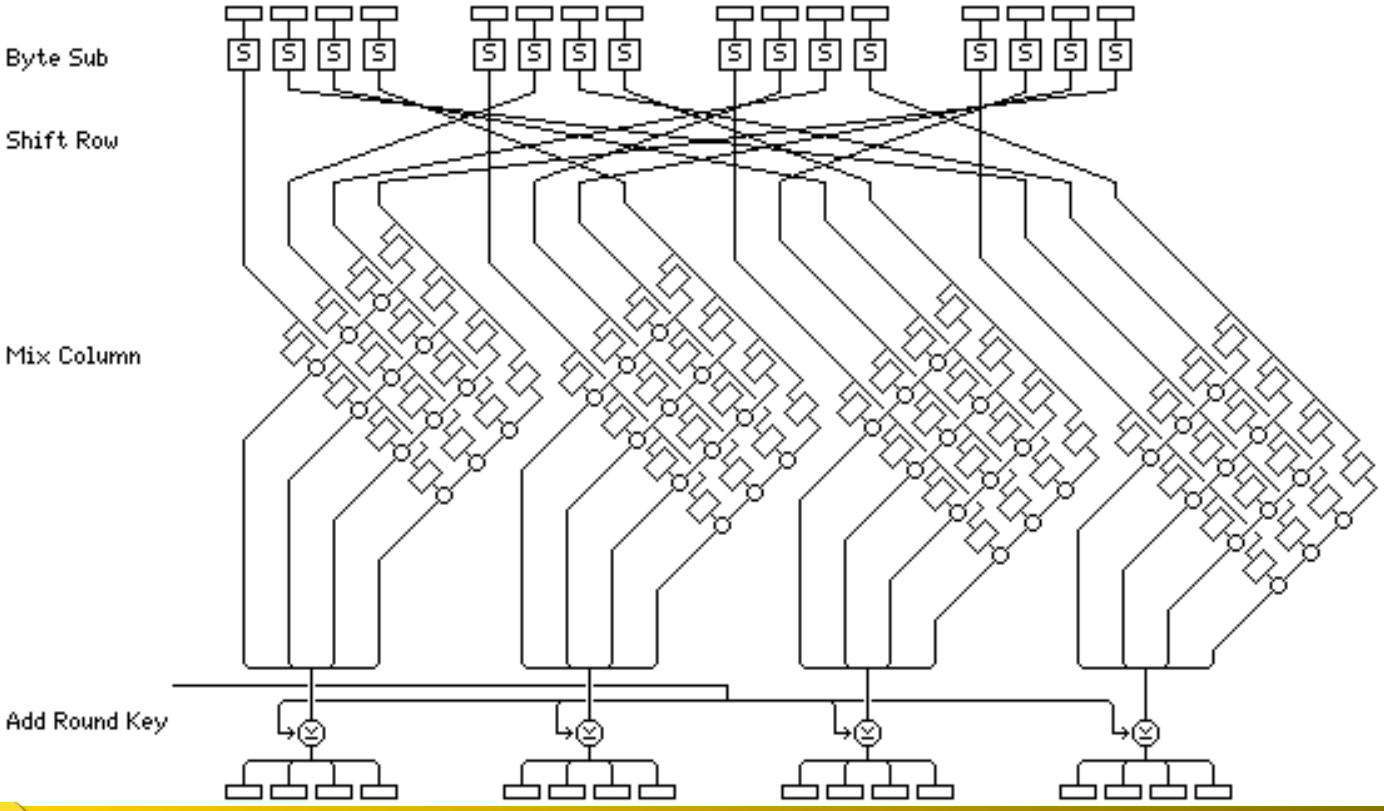


Schlüsselauswahl

- Schlüssel k besteht aus 32 * Nk Bits bzw. 4 * Nk Bytes
- Ein Wort W[i] besteht aus aus 4 Bytes
- W[0] sind die ersten 4 Byte des Schlüssels, W[1] die zweiten 4 Bytes, ..., W[Nk-1] die letzten 4 Bytes
- Insgesamt müssen Nb * (Nr + 1) Wörter berechnet werden
- Im folgenden sei Nk <= 6:
  für i = Nk bis Nb * (Nr +1) gilt:
  - W[i] = W[i-Nk] XOR `SubByte`(W[i-1])

  falls i mod Nk == 0 gilt
  - W[i] = W[i-Nk] XOR `SubByte`(`RotByte`(W[i-1]) XOR `Rcon`[i/Nk]
    mit `SubByte` = AES Byte-Substitution angew. auf Bytes eines Wortes
    mit `RotByte` = zyklischer Shift um 1 Byte (abcd wird bcda)
  - `Rcon[i]=(RC[i], 00, 00, 00)` (Rundenkonstante) mit
    RC[1] = {01}; RC[i] = {02} * RC[i-1]

AES Verschlüsselung

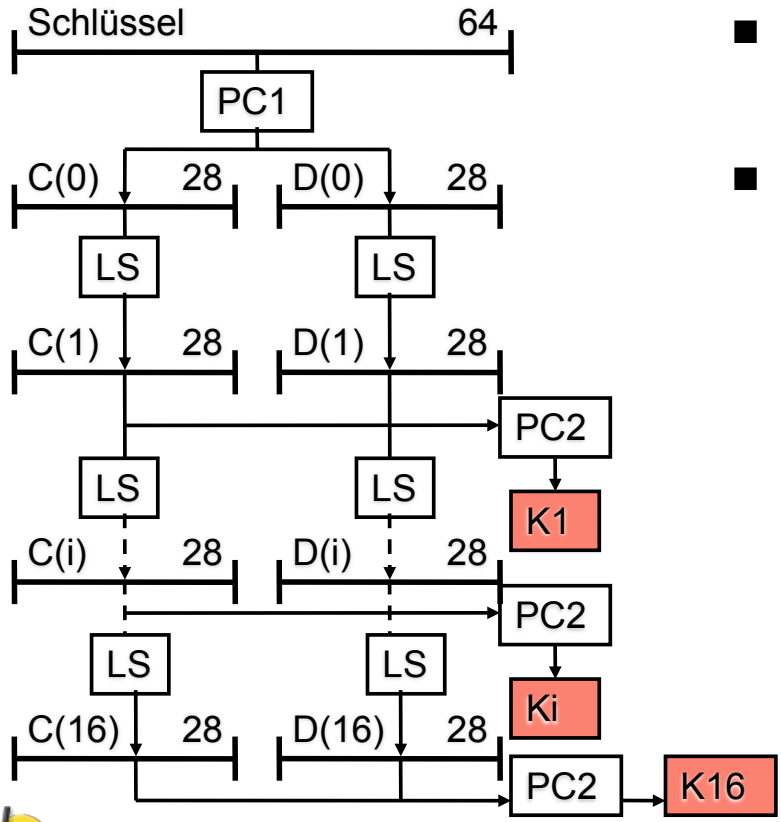


AES Design-Kriterien

- Design-Kriterien mussten offen gelegt werden
- Abschätzung und Stellungnahme zur Widerstandsfähigkeit gegen bekannte Angriffe

- Schlüsselauswahl mit nichtlinearer Durchmischung:
  wegen Verwendung der S-Box;
  damit widerstandsfähig gegen folgende Angriffe:
  - Kryptanalyst kennt Teile des Schlüssels und versucht den Rest zu berechnen
  - Zwei ähnliche Schlüssel haben **keine** große Zahl von gemeinsamen Rundenschlüsseln
  - Rundenkonstante verhindert Symmetrien im Verschlüsselungsprozess; jede Runde ist anders

Wdhlg.: DES Schlüsselauswahl



- Lediglich Permutation und Shift-Operationen

- Keine Substitution bzw. Anwendung von S-Boxen wie bei AES

AES Design-Kriterien (Forts.)

- Keine Feistel Chiffre, d.h. deutlich höhere Diffusion:
  nach 2 Runden hängt jedes Output Bit von jedem Input Bit ab
- Algebraische S-Box Konstruktion; Offengelegt; In hohem Maße nichtlinear
- Damit stabil gegen lineare und differentielle Kryptanalyse
- `ShiftRow` wurde eingefügt um zwei neue Angriffsarten zu verhindern (truncated differentials und Square attack)
- `MixColumn` für hohe Diffusion; Änderung in einem Input Byte verursacht Änderung in allen Output Bytes
- Auswahl von 10 Runden:
  Bei AES mit bis zu 7 Runden sind Angriffe bekannt die besser sind als Brute Force. Bei mehr als 7 Runden sind keine solchen Angriffe bekannt. D.h. 3 Runden „Reserve“ die sehr leicht erweitert werden können