Kryptografie verständlich

Ein Fachbuch für
Studierende und Anwender

von
Christof Paar und Jan Pelzl

www.crypto-textbook.com

Kapitel 3

Der Data Encryption Standard (DES) und Alternativen

(Version: 1. Dezember 2016)

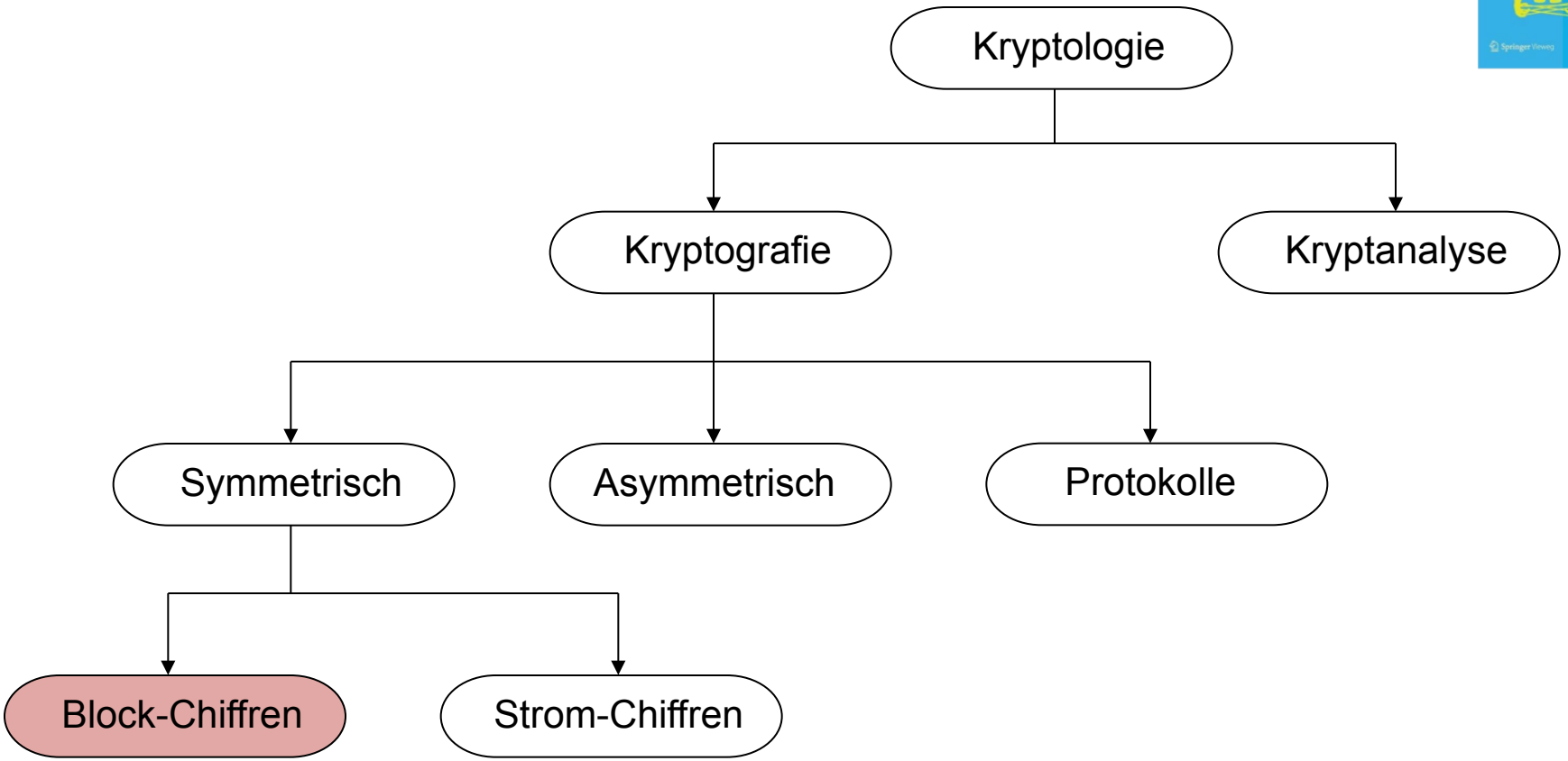
Übersicht

- Einführung
- Übersicht über den Algorithmus
- Interne Struktur
- Entschlüsselung
- Sicherheitsbetrachtung

Übersicht

- **Einführung**
- Übersicht über den Algorithmus
- Interne Struktur
- Entschlüsselung
- Sicherheitsbetrachtung

Blockchiffren in der Kryptologie



DES
Fakten

- Blockgröße **64 Bit**
- Von **IBM** unter Einfluss der NSA entwickelt
- Algorithmus basiert auf der *Lucifer* Chiffre
- **1977 standardisiert** durch das **National Bureau of Standards** (NBS, heute *National Institute of Standards and Technology* (NIST))
- Bis 2000 die bei weitem meist verbreitete **Block Chiffre**
- Sehr gut untersucht
- Aus heutiger Sicht nicht mehr einsetzbar wegen **geringer Schlüssellänge von 56 Bit**
- **Aber: 3DES ist eine sichere Chiffre** und wird heute noch verwendet
- Seit 2000 durch den *Advanced Encryption Standard* (**AES**) abgelöst

Exkurs: Primitive von Blockchiffren

Konfusion und Diffusion

- Claude Shannon: Kann mit zwei primitiven Operationen starke Verschlüsselungsalgorithmen konstruieren
  1. **Konfusion:** Verbirgt Zusammenhang von Schlüssel und Chiffrat.
     (In heutigen Chiffren wie dem AES oder DES verwendet man die **Substitution** als gängiges Element für die Konfusion)

  2. **Diffusion:** Einfluss eines Klartextsymbols erstreckt sich auf viele Symbole des Chiffrates. Ziel: Verbergen statistischer Eigenschaften des Klartextes.
     (Ein einfaches Element der Diffusion ist die **Bit-Permutation**, z.B. beim DES häugif verwendet)

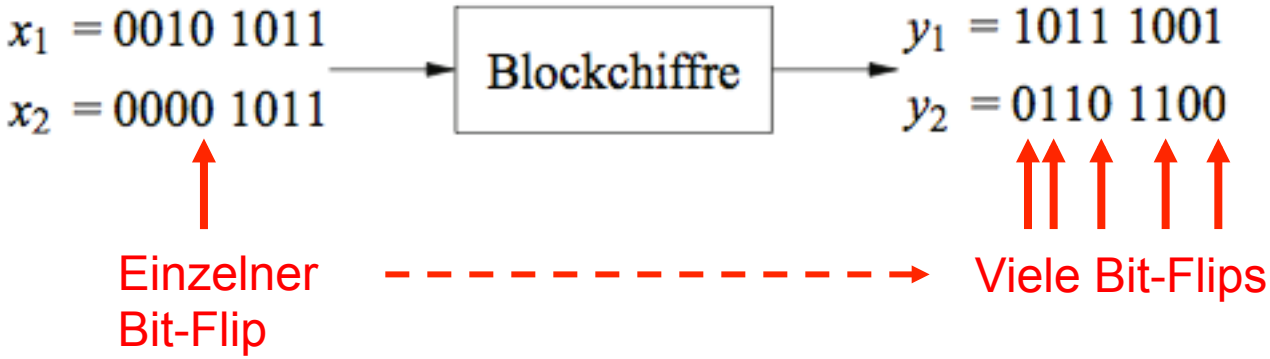
- Beide Operationen können keine Sicherheit gewährleisten, aber deren Kombination (sog. *Produktchiffren).*

Exkurs: Primitive von Blockchiffren
Produktchiffren

- Heutige Chiffren sind meistens Produktchiffren
- Sie verfügen über eine Rundenfunktion, welche wiederholt auf die Daten angewendet wird

- Gut Diffusionseigenschaft: **Änderung eines einzelnen Klartextbits** führt zu Änderung von **durchschnittlich der Hälfte der Ausgangsbits**

Beispiel:

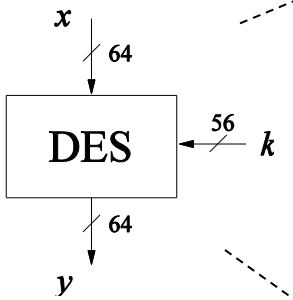


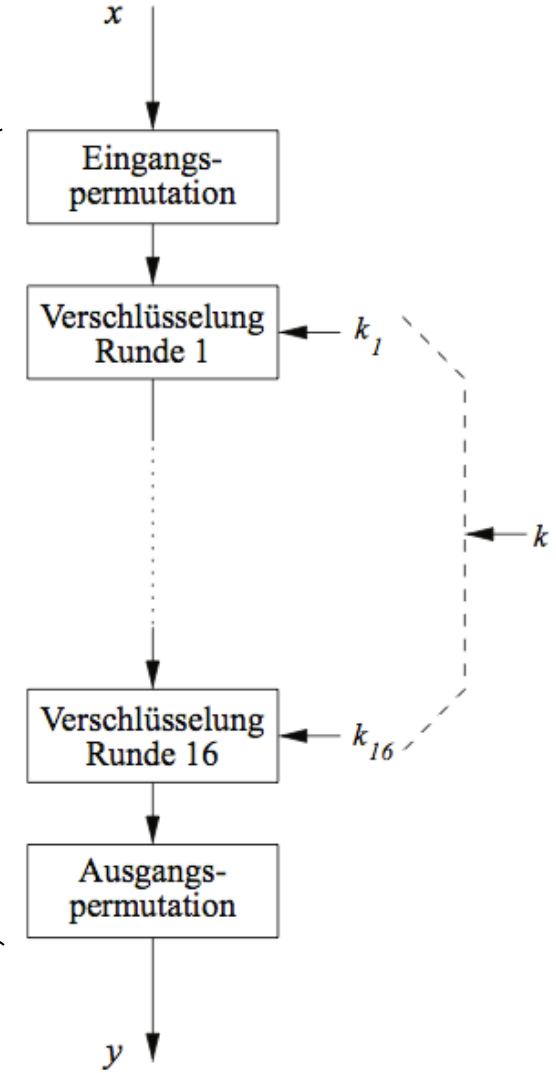
Übersicht

- Einführung
- **Übersicht über den Algorithmus**
- Interne Struktur
- Entschlüsselung
- Sicherheitsbetrachtung

DES

Algorithmus: Übersicht



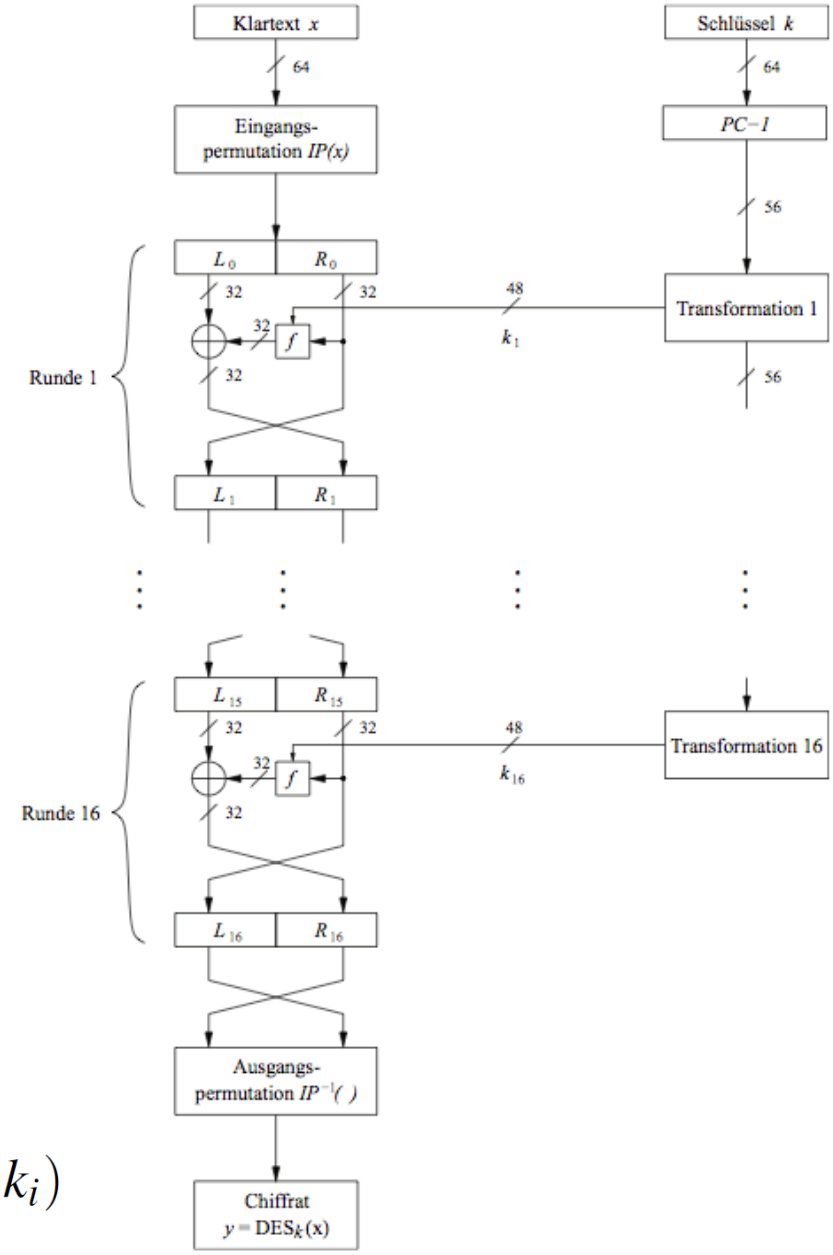


- **Verschlüsselung von 64-Bit Blöcken**
- **Schlüssellänge von 56 Bit**
- Symmetrische Chiffre: Verwendung des gleichen Schlüssels für die Ver- und Entschlüsselung
- Basiert auf 16 Runden mit identischen Operationen
- Verwendung von Rundenschlüsseln (abgeleitet aus dem Schlüssel) für jede Runde

DES
Algorithmus: Feistelnetzwerk (1)

- DES Struktur ist ein *Feistelnetzwerk*
- Vorteil: Ver- und Entschlüsselung bis auf den Schlüsselfahrplan gleich
- Bitweise Anfangspermutation, dann 16 Runden
  - Aufteilung des Klartextes in 32 Bit Hälften L_i und Ri
  - R_i ist Eingabe der f-Funktion, deren Ausgabe mit L_i XORiert wird
  - Vertauschung von rechter und linker Hälfte
- Rundenfunktion: $L_i = R_{i-1},$

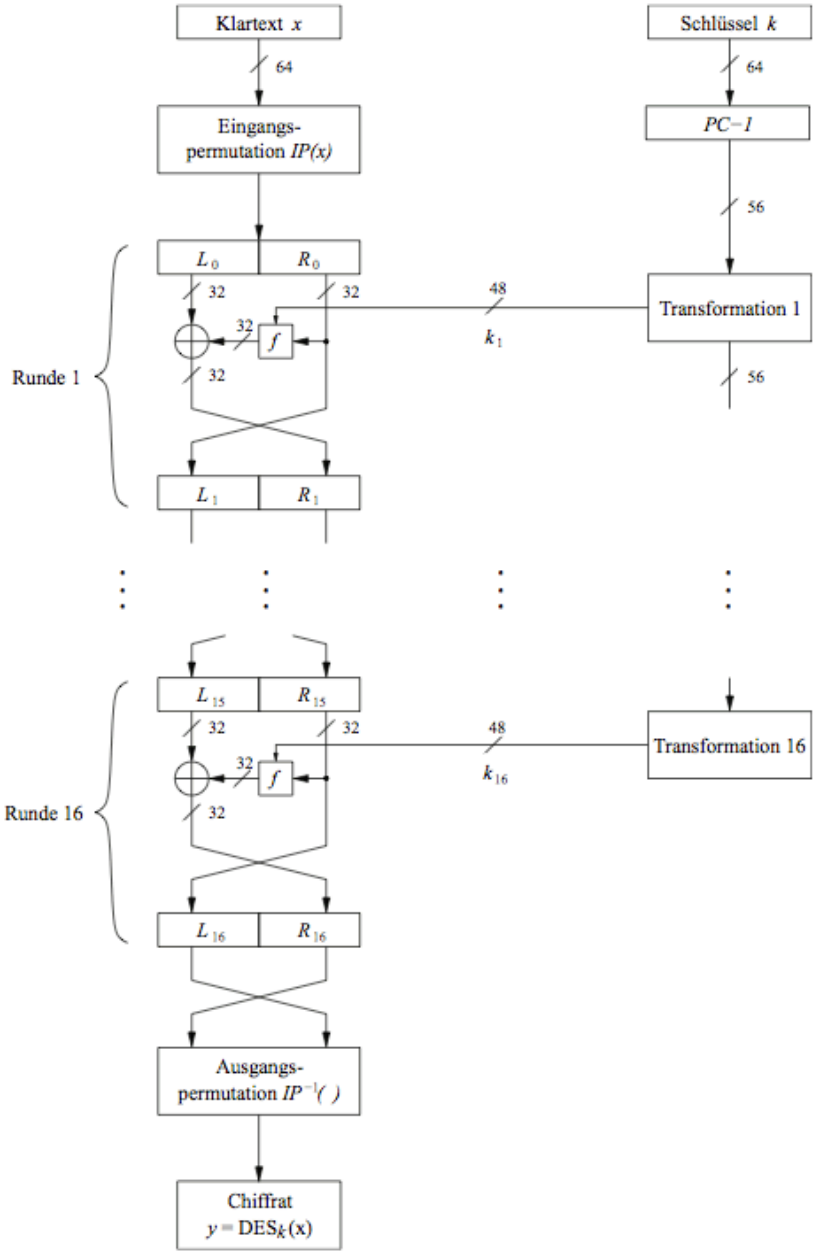
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$



DES

Algorithmus: Feistelnetzwerk (2)

- Vertauschung von L und R am Ende der letzten Runde
- Ausgangspermutation



Übersicht

- Einführung
- Übersicht über den Algorithmus
- **Interne Struktur**
- Entschlüsselung
- Sicherheitsbetrachtung

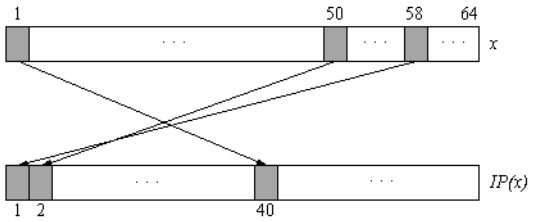
DES

Eingangs- und Ausgangspermutation

- Bitweise Permutationen
- Inverse Operationen
- Beschrieben durch die Tabellen *IP* und IP^{-1}

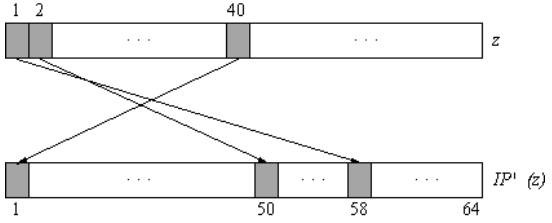
Eingangspermutation

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



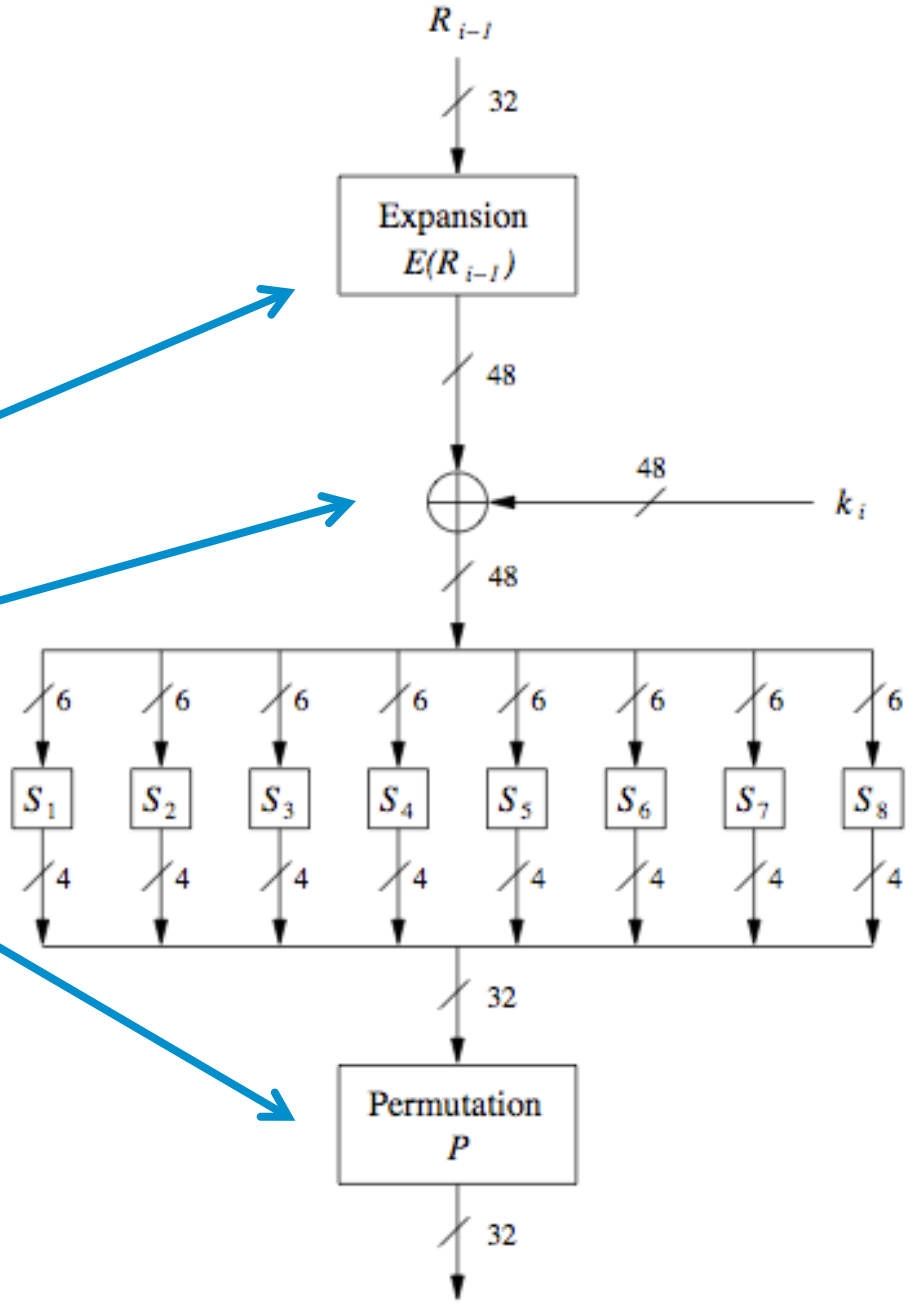
Ausgangspermutation

IP^{-1}							
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



DES
Die f-Funktion (1)

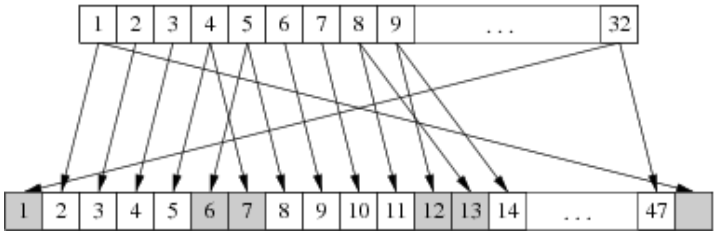
- **Hauptoperation** des DES
- Eingänge in die *f*-Funktion
  R_{i-1} und Rundenschlüssel k_i
- **4 Schritte**:
  1. Expansion *E*
  2. XOR mit Rundenschlüssel
  3. S-Box Substitution
  4. Permutation

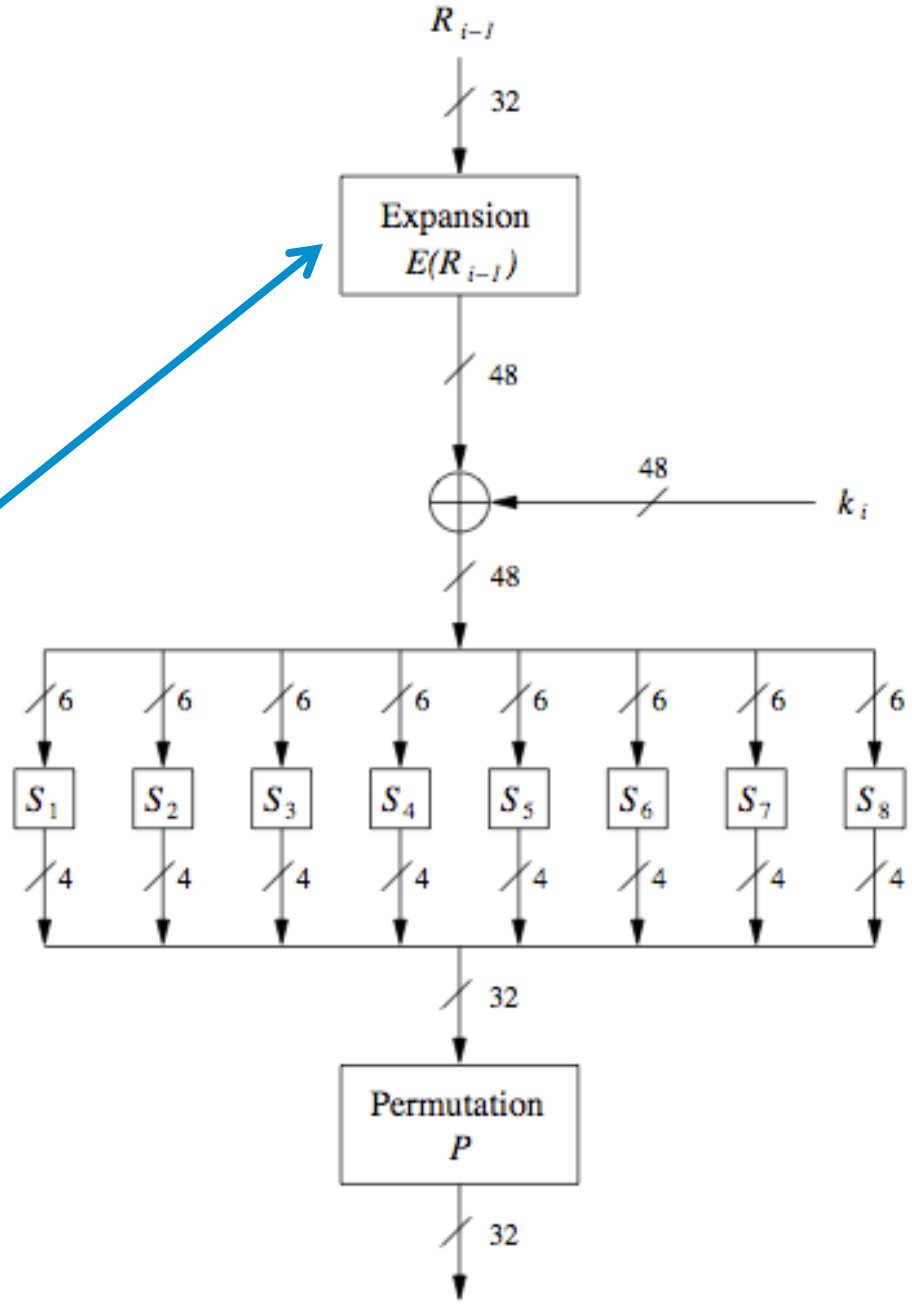


DES
Die f-Funktion (2)

1. Die Expansionsfunktion *E*
– Ziel: Erhöhung der Diffusion

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



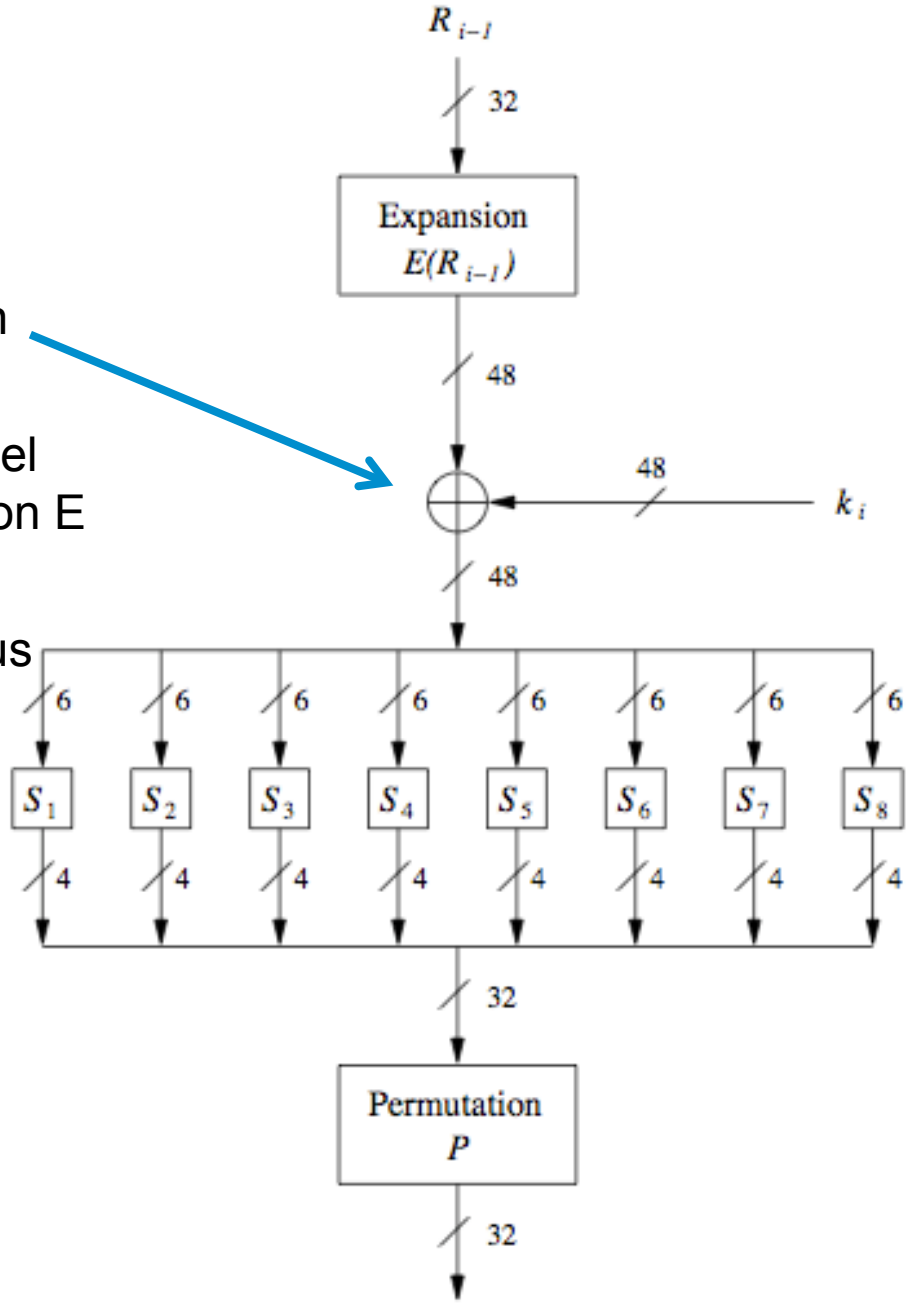


DES
Die f-Funktion (3)

2. Rundenschlüssel mit XOR addieren

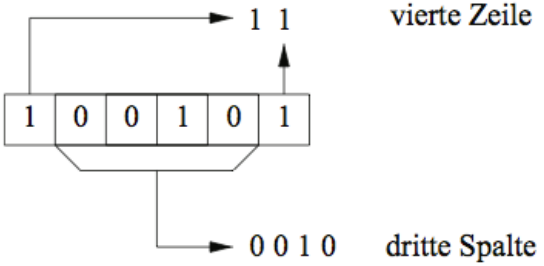
– Bitweises XOR von Rundenschlüssel und Ausgabe der Expansionsfunktion E

– Ableitung des Rundenschlüssels aus dem Hauptschlüssel durch DES Schlüsselfahrplan

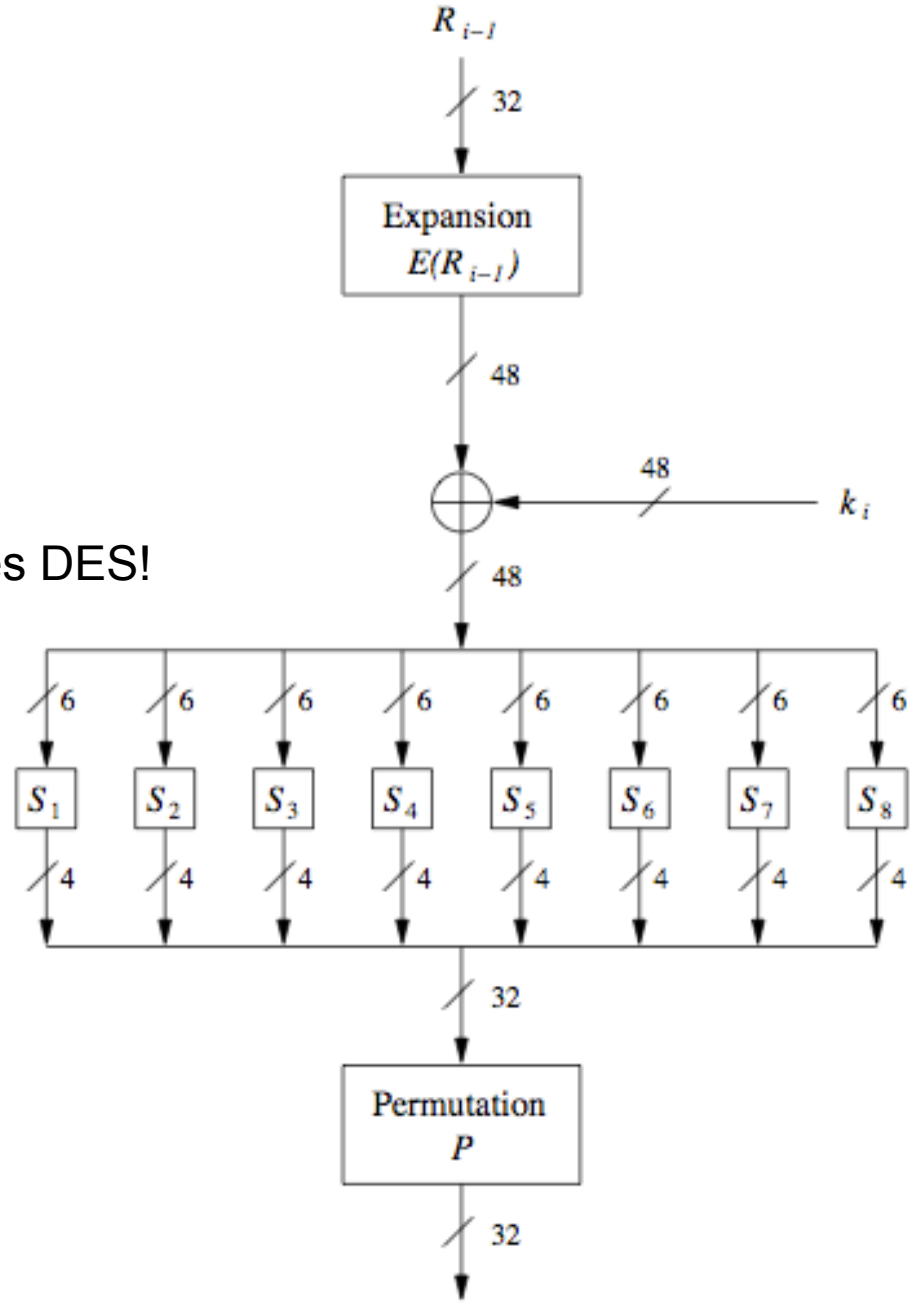


DES
Die f-Funktion (4)

3. Die S-Box Substitution
- 8 Substitutionstabellen
- 6 Bit Eingang, 4 Bit Ausgang
- Nichtlinear
- Ausschlaggebend für die Sicherheit des DES!



S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00

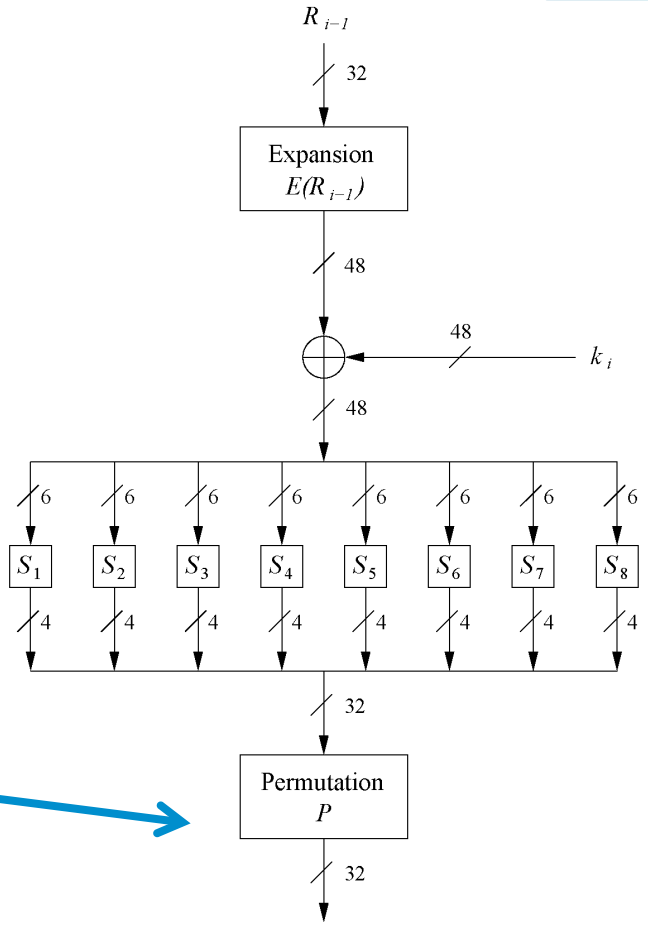


DES

Die f-Funktion (5)

4. Permutation P
   - Bitweise Permutation
   - Ziel: Diffusion
   - Ausgabe Bits einer S-Box wirken auf zahlreiche S-Boxen der nächsten Runde
   - Diffusion durch E, S-Boxen und P garantiert dass nach 5 Runden jedes Bit von jedem Schlüssel- und Klartextbit abhängt

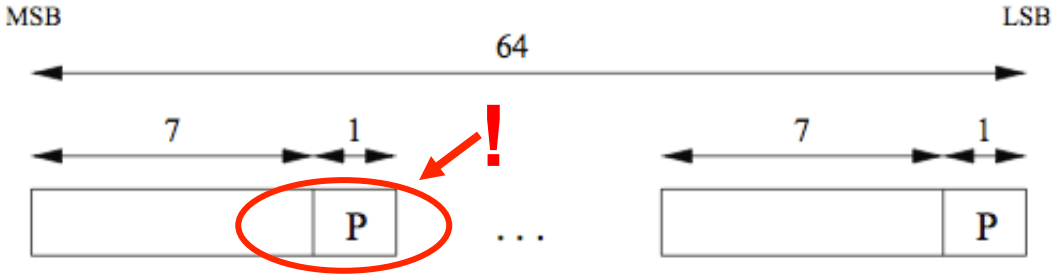
P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25



DES

Der Schlüsselfahrplan (1)

- Ableitung von 16 Rundenschlüsseln (oder *Unterschlüsseln*) k_i mit 48 Bit vom 56 Bit Eingangsschlüssel.
- Die Eingangsgröße des DES-Schlüssels ist 64 Bit: **56 Schlüsselbit** und **8 Paritätsbit**:



P = Paritätsbit

- **Entfernen der Paritätsbits mit der Transformation Permuted Choice** (*PC-1)*:
(Anmerkung: Die Bits 8, 16, 24, 32, 40, 48, 56 und 64 werden überhaupt nicht verwendet)

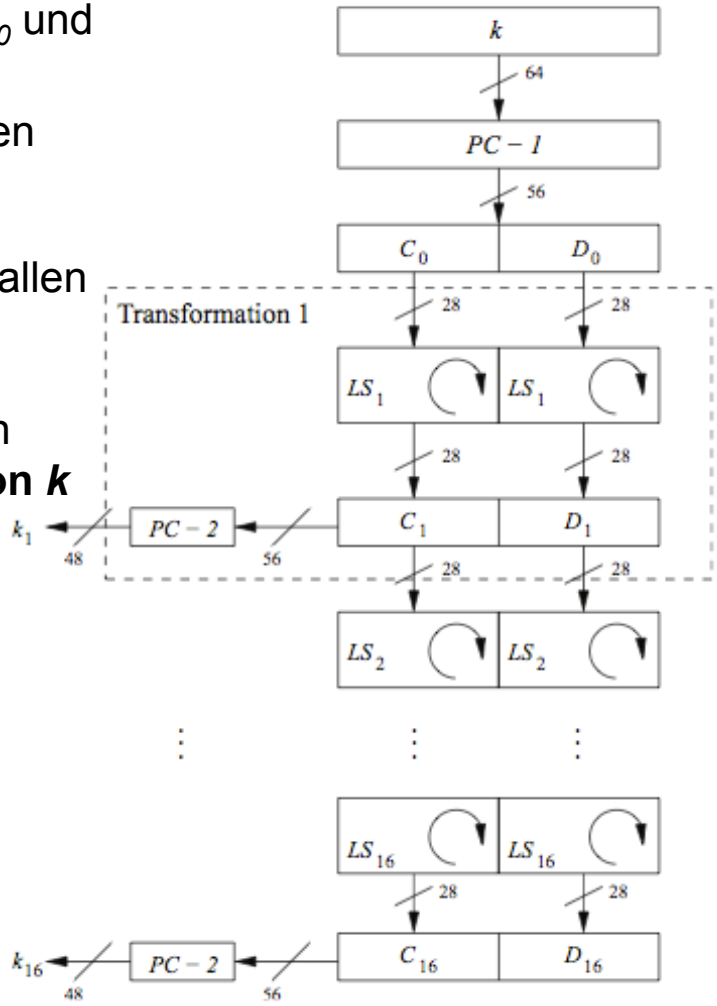
PC − 1							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

DES
Der Schlüsselfahrplan (1)

- **Aufteilen** des Schlüssels in zwei 28 Bit Hälften C_0 und D_0
- **Linksrotation** der beiden Hälften um **ein Bit** in den Runden i = 1, 2, 9 ,16
- **Linksrotation** der beiden Hälften **um zwei Bit** in allen anderen Runden
- 48 Bit Rundenschlüssel k_i wird aus C_i und D_i durch PC-2 ausgewählt, d.h. ***k_i* ist eine Permutation von *k***

$PC-2$							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

- **Anmerkung:** Gesamtzahl an Rotationen ist 4 x 1 + 12 x 2 = 28 $\Rightarrow D_0 = D_{16}$ und $C_0 = C_{16}$!

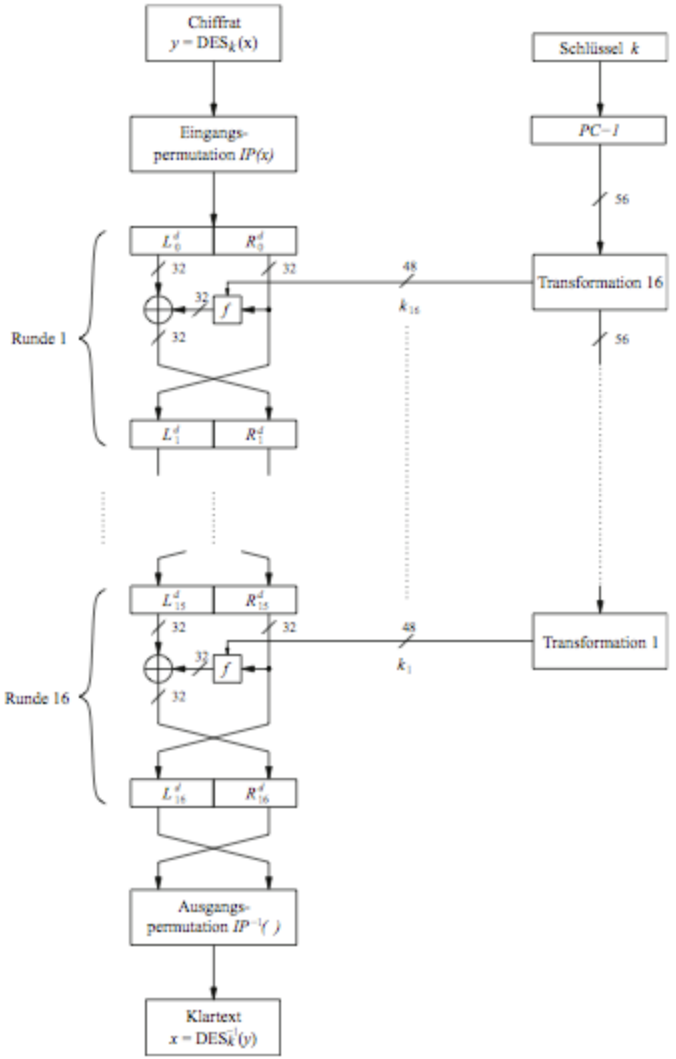


Übersicht

- Einführung
- Übersicht über den Algorithmus
- Interne Struktur
- **Entschlüsselung**
- Sicherheitsbetrachtung

DES
Entschlüsselung

- Bei **Feistel Chiffren** muss nur der Schlüsselfahrplan für die Entschlüsselung verändert werden
- Erzeuge die gleichen 16 Rundenschlüssel in **umgekehrter Reihenfolge:**
  - Da D_0=D_{16} und C_0=C_{16} ist, kann der erste Rundenschlüssel durch *PC-2* unmittelbar nach *PC-1* (ohne Rotation) gewonnen werden
  - Keine Rotation in Runde 1
  - **Rechtsrotation um ein Bit** in Runden 2, 9 und 16
  - **Rechtsrotation um zwei Bit** in allen anderen Runden



Übersicht

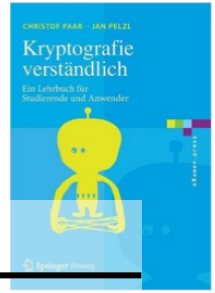
- Einführung
- Übersicht über den Algorithmus
- Interne Struktur
- Entschlüsselung
- **Sicherheitsbetrachtung**

DES
Sicherheitsbetrachtung

- **Zwei Hauptkritikpunkte nach Einführung des DES:**
  1. Schlüsselraum ist zu gering (2^{56} Schlüssel)
  2. Design Kriterien der S-Box wurden geheim gehalten: Gibt es Hintertüren, die nur der NSA bekannt sind?

- **Analytische Angriffe:** DES ist resistent ggü. *Differentieller* und *linearer Kryptanalyse*, welche erst Jahre nach dem DES bekannt veröffentlicht wurden. D.h., IBM und NSA kannten diese Angriffe bereits 15 Jahre vorher!
  Bisher gibt es keine analytischen Angriffe, um den DES in realistischen Szenarios zu brechen
- **Ausführliche Schlüsselsuche:** Für ein gegebenes Chiffrat/ Geheimtext-Paar (x, y) teste alle 2^{56} Schlüssel bis $DES_k^{-1}(x)=y$ gilt

  $\Rightarrow$ Mit heutiger Computertechnologie machbar!



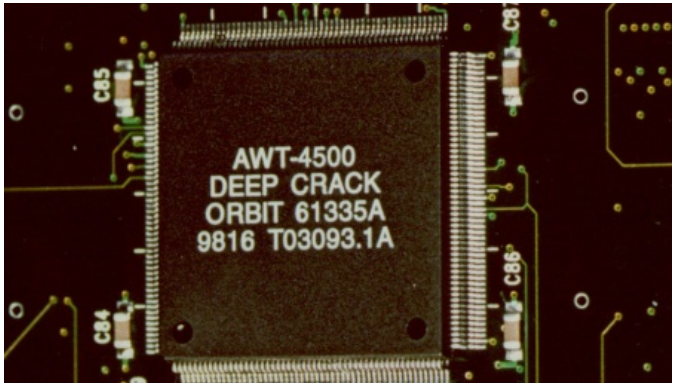
DES

Historie der Angriffe auf DES

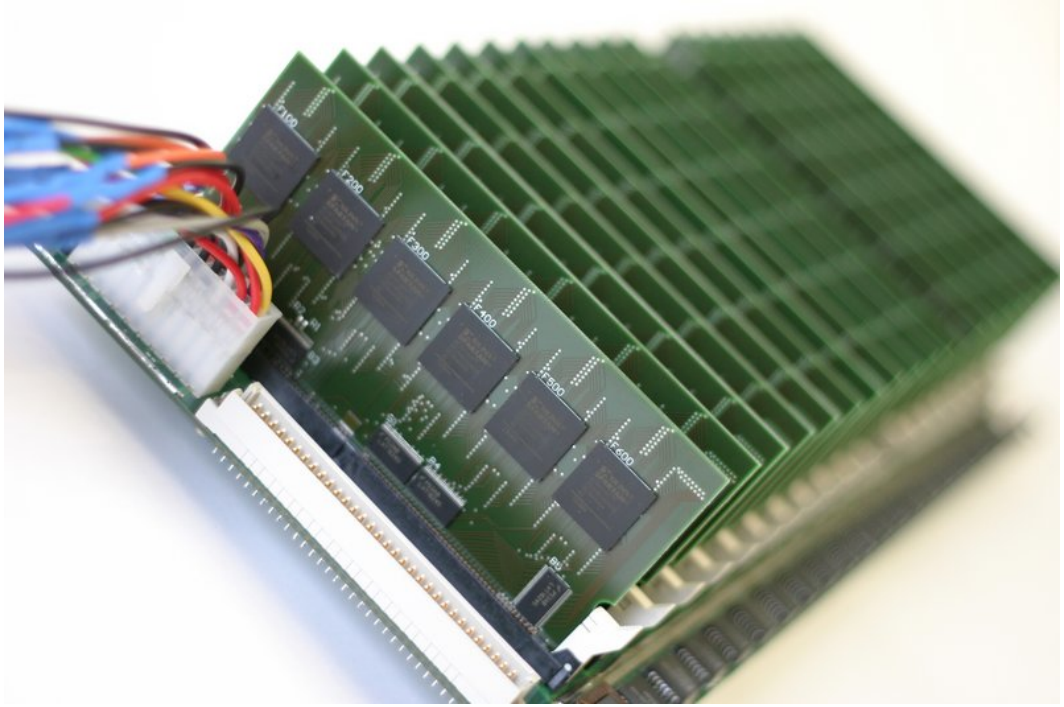
Jahr	Vorgeschlagener/ implementierter DES Angriff
1977	Diffie & Hellman, Kostenabschätzung für eine Schlüsselsuchmaschine
1990	Biham & Shamir stellen differentielle Kryptanalyse vor (2^{47} chosen ciphertexts)
1993	Mike Wiener schlägt sehr effiziente Schlüsselsuchmaschine vor: Durchschnittliche Suche in 36h. Kosten: $1.000.000
1993	Matsui schlägt lineare Kryptanalyse vor (2^{43} chosen ciphertexts)
Jun. 1997	DES Challenge I gebrochen, 4,5 Monate verteiltes Rechnen
Feb. 1998	DES Challenge II--1 gebrochen, 39 Tage verteiltes Rechnen
Jul. 1998	DES Challenge II--2 gebrochen, Schlüsselsuchmaschine gebaut von der Electronic Frontier Foundation (EFF): 1800 ASICs mit je 24 Schlüsselsuch-Einheiten, Kosten: $250 000, 15 Tage durchschnittliche Suche (56h für Challenge)
Jan. 1999	DES Challenge III in 22h 15min gebrochen (Verteilte Suche mit Unterstützung von *Deep Crack*)
2006-2008	Rekonfigurierbare Schlüsselsuchmaschine *COPACOBANA, entwickelt von* den Unis in Bochum und Kiel. Verwendet 120 FPGAs, um DES in 6,4 Tagen im Durchschnitt zu brechen. Kosten ca. $10 000.

DES
Hardware-Angriffe auf DES

Deep Crack und COPACOBANA



Deep Crack [EFF]

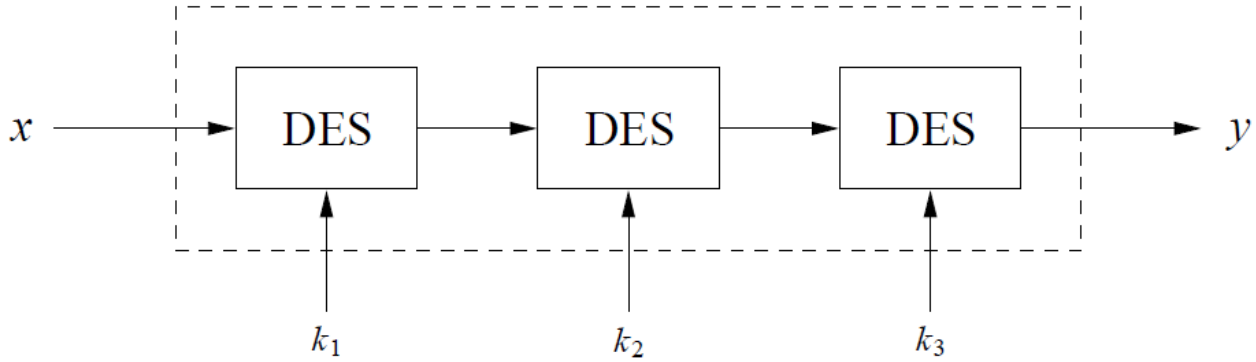


COPACOBANA [RUB]

DES
TripleDES oder 3DES

- Nutzen von Dreifachverschlüsselung mit DES zur Erhöhung der effektiven Schlüssellänge auf 112.

$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$



- Alternative Version von 3DES:

$$y = DES_{k_3}(DES^{-1}_{k_2}(DES_{k_1}(x))).$$

Vorteil: Einfache DES Verschlüsselung durch Wahl von $k_1=k_2=k_3$

- Bis heute keine praktischen Angriffe bekannt
- Wird in vielen Abwärtskompatiblen Systemen verwendet (z.B. Bank-Applikationen)

DES
Alternativen zum DES

a	I/O Bit	Schlüssellänge	Bemerkung
AES / Rijndael	128	128/192/256	DES "Ersatz", weltweiter Standard
Triple DES	64	112 (effektiv)	Konservative Wahl
Mars	128	128/192/256	AES Finalist
RC6	128	128/192/256	AES Finalist
Serpent	128	128/192/256	AES Finalist
Twofish	128	128/192/256	AES Finalist
IDEA	64	128	Bis 2000 patentiert

DES

Lessons Learned

- DES war der dominante symmetrische Algorithmus von Mitte der 1970er bis Mitte der 1990er Jahre
- Da 56 Bit Schlüssel nicht mehr sicher sind, wurde der Advanced Encryption Standard (AES) entwickelt
- Standard DES mit 56 Bit Schlüssellänge kann heute mit ausführlicher Schlüsselsuche gebrochen werden
- DES ist relativ robust ggü. bekannten kryptanalytischen Angriffen wie z.B. differentieller oder linearer Kryptanalyse
- Durch dreimalige Verschlüsselung mit DES hintereinander erhält man Triple DES (3DES), gegen welchen derzeit kein praktikabler Angriff existiert
- Heute ist AES die Standardchiffre für symmetrische Verschlüsselung