Algorithmische Anwendungen

Projekt:

Data Encryption Standard

Team:
Adil Sbiyou
El Moussaid Tawfik

Inhalt Projekt DES

2. Geschichte des DES
3. Eigenschaften
4. Funktionsweise im Detail
5. Sicherheit des Verfahrens
6. Fazit

Inhalt Projekt DES

2. Geschichte des DES
3. Eigenschaften
4. Funktionsweise im Detail
5. Sicherheit des Verfahrens
6. Fazit

Geschichte des DES

- 1972 startete die NBS ein Programm zur sicheren Dateispeicherung und –übertragung.
- Gesucht: ein normungsfähiges Verschlüsselungsverfahren.
- Kriterien (u.A.):
  - Hohe Sicherheit bei leichter Implementation
  - Effizient, flexibel für versch. Anwendungen
  - Sicherheit liegt allein im Schlüssel und nicht in der Geheimhaltung des Algorithmus

Geschichte des DES

- 1974 IBM reicht Algorithmus „Lucifer“ ein.
- NBS bittet die NSA um Hilfe bei der Überprüfung der Sicherheit.
- 1975 wird der von der NSA modifizierte Algorithmus veröffentlicht.
- 1976 wird das Verfahren als U.S Bundesstandard eingeführt.
- KRITIK!
  - Reduzierung der Schlüssellänge auf 64 Bit
  - Geheimhaltung einiger Designkriterien

Inhalt Projekt DES

2. Geschichte des DES
3. Eigenschaften
4. Funktionsweise im Detail
5. Sicherheit des Verfahrens
6. Fazit

Eigenschaften des DES

- Symmetrisches Verfahren.
- Blockchiffre: 64 Bit Klartextblock wird in einen 64 Bit Schlüsseltextblock umgesetzt.
- 64 Bit Schlüssel- davon 8 Paritätsbits deshalb 56 Bit effektive Schlüssellänge.
- Einfache Funktionen! : Permutationen, Substitutionen, XOR-Verknüpfungen
- Schnell, vor allem in Hardware:
  - 15.625 Mio. Blöcke / Sekunde (Hardware)
  - 32.000 Blöcke / Sekunde (Software)

Inhalt Projekt DES

2. Geschichte des DES
3. Eigenschaften
4. Funktionsweise im Detail
5. Sicherheit des Verfahrens
6. Fazit

Funktionsweise im Detail

- Der DES basiert auf einer Feistel-Chiffre (der elementare Algorithmus).

- Formel:

$$(L_i, R_i)=(R_{i-1}, L_{i-1} \text{ XOR } F(R_{i-1},K_i)),1<=i<=r$$

- Mehrmaliges Durchlaufen (Runden).
- Der DES durchläuft r=16 Feistelrunden.

Funktionsweise im Detail

- Der DES basiert auf einer Feistel-Chiffre (der elementare Algorithmus).

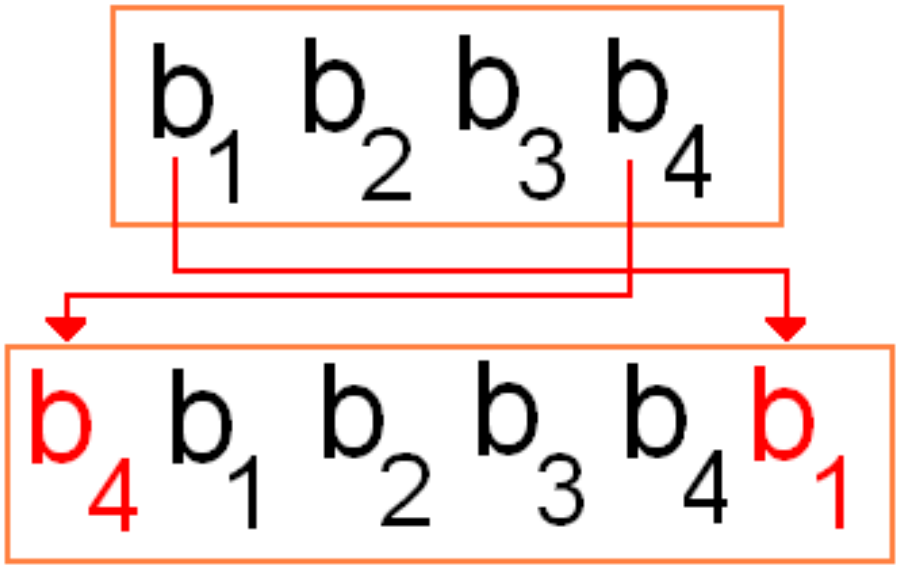
- Erste Runde:

$$(L_1, R_1)=(R_o, L_0 \text{ XOR } F(R_0,K_1)),i=1$$

- Mehrmaliges Durchlaufen (Runden).
- Der DES durchläuft r=16 Feistelrunden.

Funktionsweise im Detail
Innerhalb von Funktion F

- Expansion E (vereinfacht)



(4 Bits werden zu 6 Bits).

Funktionsweise im Detail
Innerhalb von Funktion F

- Substitutions-Box (S-Box)

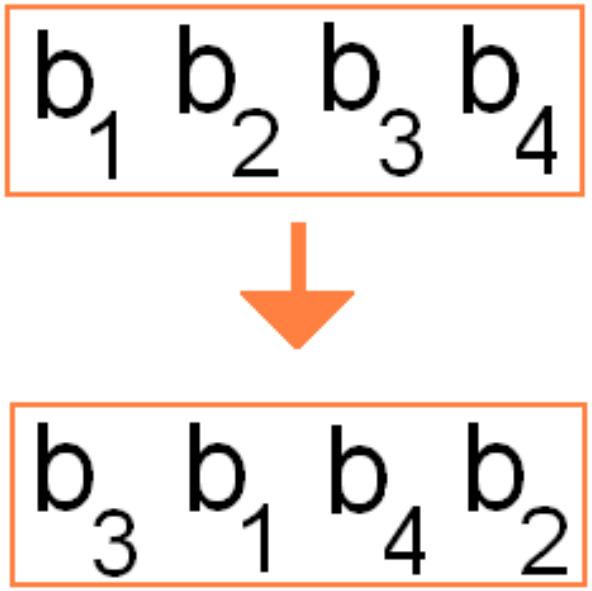
Eingabe: bbbbbb

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
2	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
3	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
4	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

(6 Bit String wird durch 4 Bit String substituiert).

Funktionsweise im Detail
Innerhalb von Funktion F

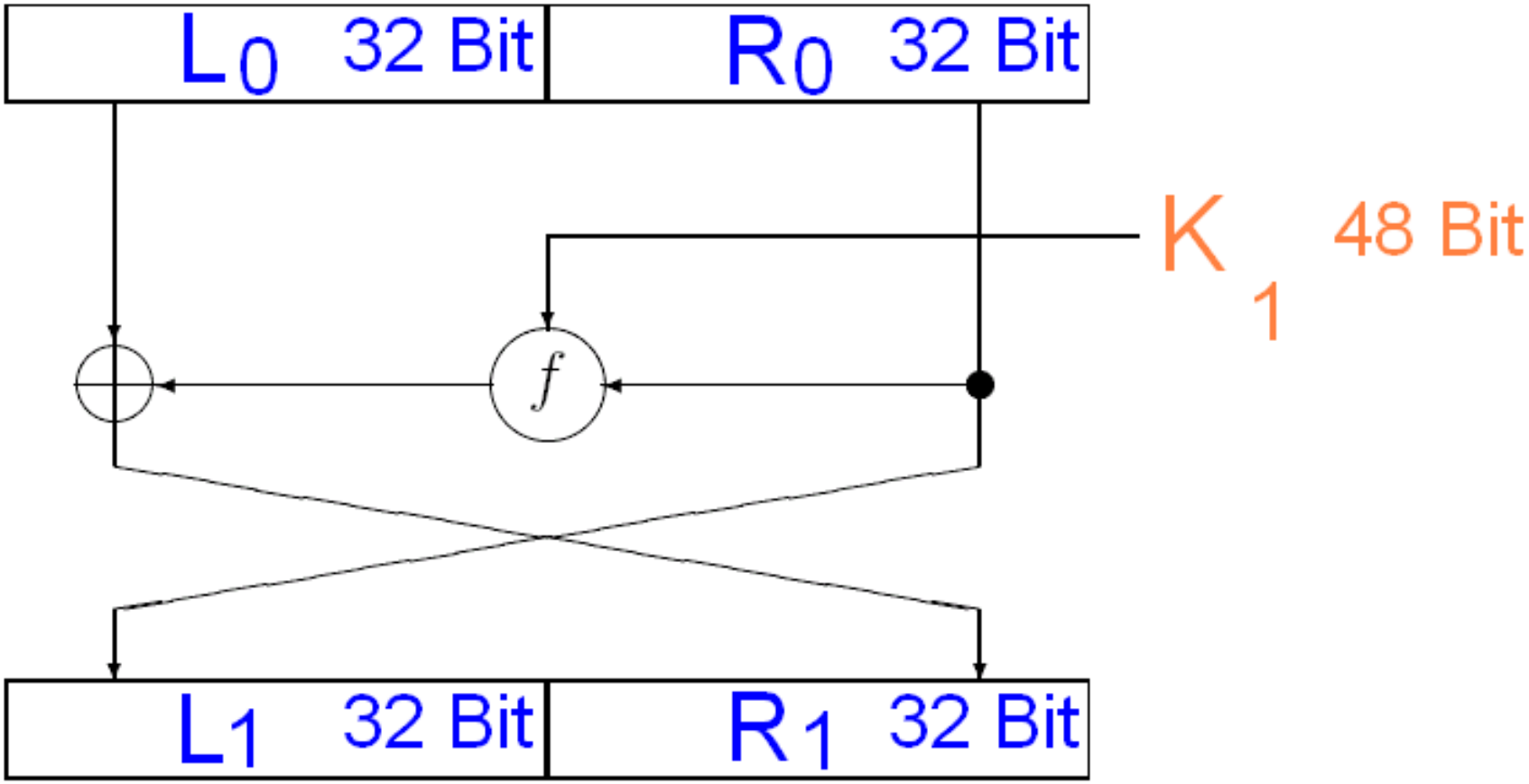
- Permutation P (vereinfacht)

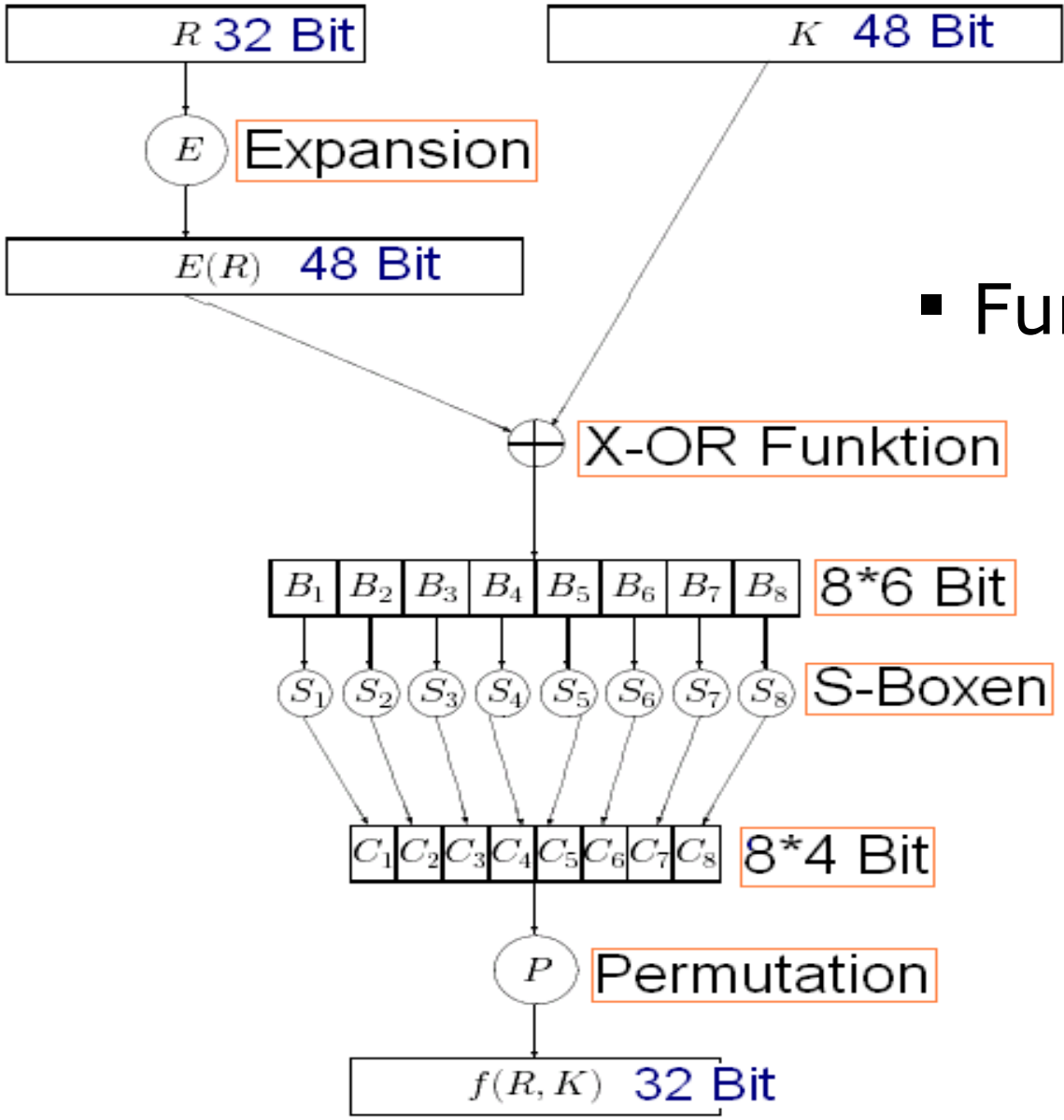


(Bits werden umgestellt).

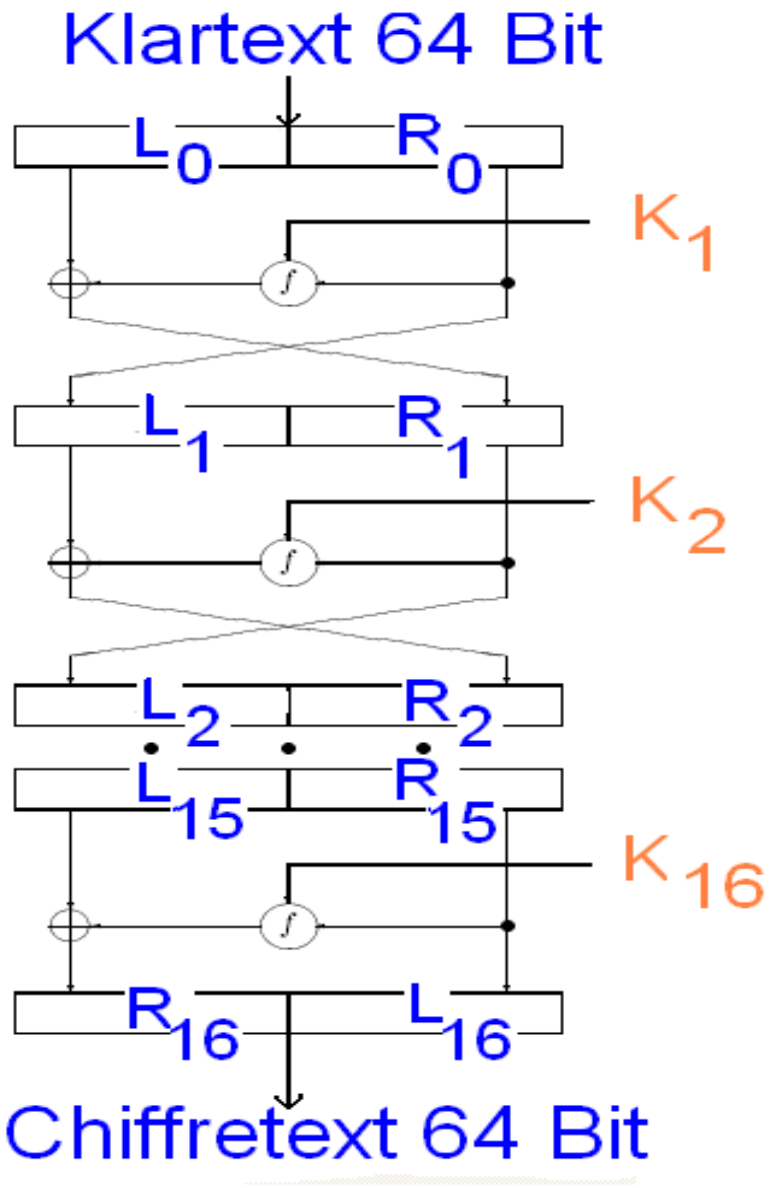
Funktionsweise im Detail

Erste Feistelrunde mit 64 Bit

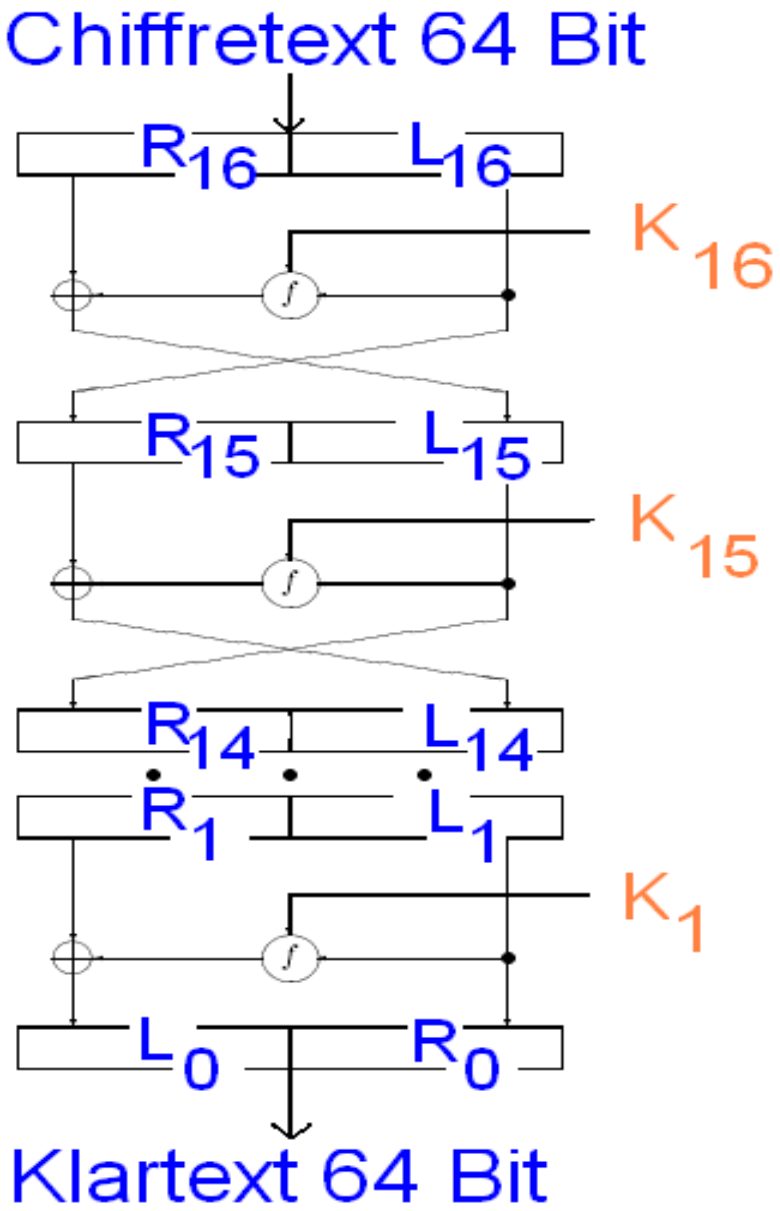



R 32 Bit
K 48 Bit
E
Expansion
E(R) 48 Bit
X-OR Funktion
B1 B2 B3 B4 B5 B6 B7 B8
8*6 Bit
S1 S2 S3 S4 S5 S6 S7 S8
S-Boxen
C1 C2 C3 C4 C5 C6 C7 C8
8*4 Bit
P
Permutation
f(R, K) 32 Bit

- Funktion F

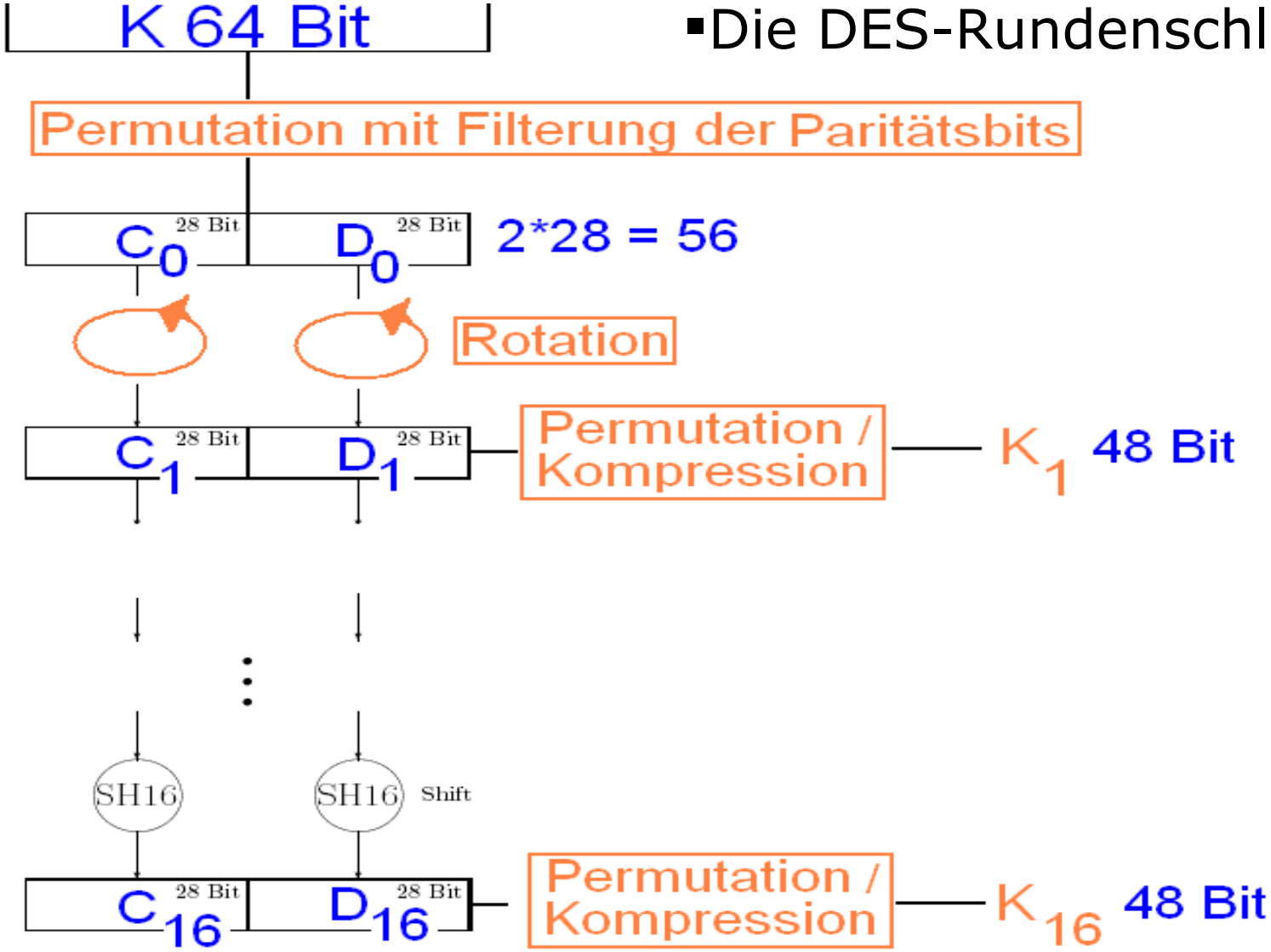


- DES-Verschlüsselung



- DES-Entschlüsselung

- Die DES-Rundenschlüssel



Inhalt Projekt DES

2. Geschichte des DES
3. Eigenschaften
4. Funktionsweise im Detail
5. Sicherheit des Verfahrens
6. Fazit

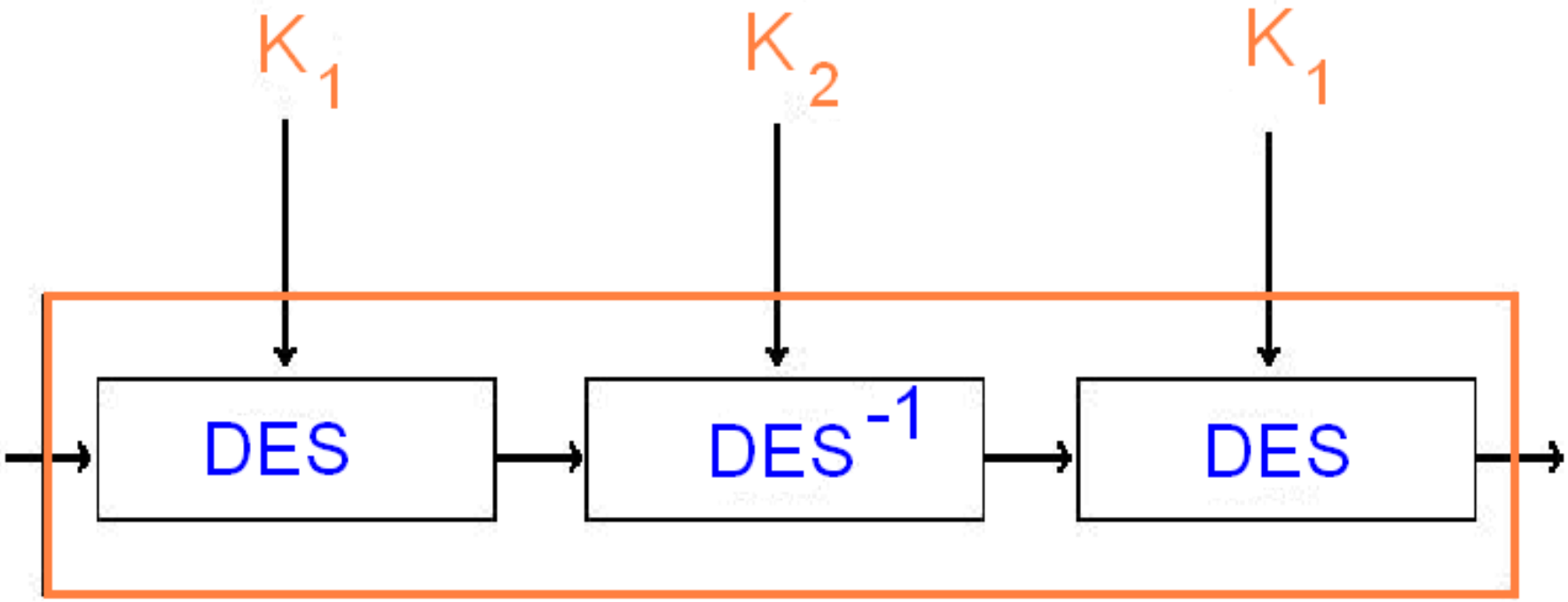
Sicherheit des Verfahrens

- Der DES ist sehr gut untersucht!
- Der Algorithmus offenbart keine entscheidende Schwäche.
- „Verbesserungen“ (z.B bei S-Boxen) schwächten Algorithmus.
- Selbst gegen spezielle Angriffsvarianten robust.
- Differentielle Kryptoanalyse (2^{47} Klartextblöcke benötigt ! Entspricht 18.000 x 60 Gigabyte Festplatten)
- Lineare Kryptoanalyse (2^{43} Klartextblöcke benötigt ! Entspricht 1172 x 60 Gigabyte Festplatten)

Sicherheit des Verfahrens

- Das größte Sicherheitsrisiko: 56 Bit Schlüssel!
- 1997 erster erfolgreicher Brute Force Angriff.
- Mittels spezieller Hardware ist es denkbar den DES in wenigen Sekunden zu knacken.
- Gegenmaßname: Der DES wird mehrfach hintereinander angewandt -> Triple-DES.
- Meistens 2 verschiedene Schlüssel.Das entspricht einer Schlüssellänge von 112 Bit.
- Nachteil: 3 x langsamer !

Sicherheit des Verfahrens
2Key3DES



- Mittlere Entschlüsselung erhält Kompatibilität mit einfachen DES, wenn Schlüssel gleich sind.

Sicherheit des Verfahrens
Wie sicher denn jetzt ?

Schlüssellänge	Aufwand
56 Bit	**1 Sekunde**
64 Bit	4 Minuten
80 Bit	194 Tage
112 Bit	**10^9 Jahre**
128 Bit	10^{14} Jahre
192 Bit	10^{33} Jahre
256 Bit	10^{52} Jahre

Das Alter des Universums wird auf 10^{10} Jahre geschätzt.

Fazit

- Das berühmteste symmetrische Verfahren.
- Hat lange Zeit dominierende Stellung in der symmetrischen Verschlüsselung eingenommen.
- Mit 56 Bit Schlüssel für sensible Daten nicht mehr sicher !
- Triple-DES sicher, doch langsam.
- Bei Neuimplementationen: neue Verfahren bevorzugen.

Literatur

[1] B. Schneier. *Applied Cryptography.* John Wiley, New York, 2nd edition, 1996.

[2] J. Buchmann. *Einführung in die Kryptographie.* Springer, Berlin, 2. Auflage, 2001.

[3] Albrecht Beutelspacher. *Geheimsprachen. Geschichte und Techniken*. C.H.Beck, 2002.

[4] Klaus Schmeh. *Kryptografie und Public- Key Infrastrukturen im Internet*. Dpunkt Verlag, 2001.

[5] Christian Thöing. *Kryptographie – DES*, 03.08.2001. http://home.t-online.de/home/poisoner/krypto/des.htm

Danke für ihre Aufmerksamkeit.