2.3.3 Produkt–Chiffren

Mehrmalige Anwendung von Substitutions– und Transpositions–Chiffren
→ Data Encryption System (DES)–Algorithmus
→ International Data Encryption Algorithmus (IDEA)

2.3.4 Beispiel DES

Chiffriert Blöcke aus 64bit Klartext mit Schlüssel der Länge $56 + 8$bit Parity.

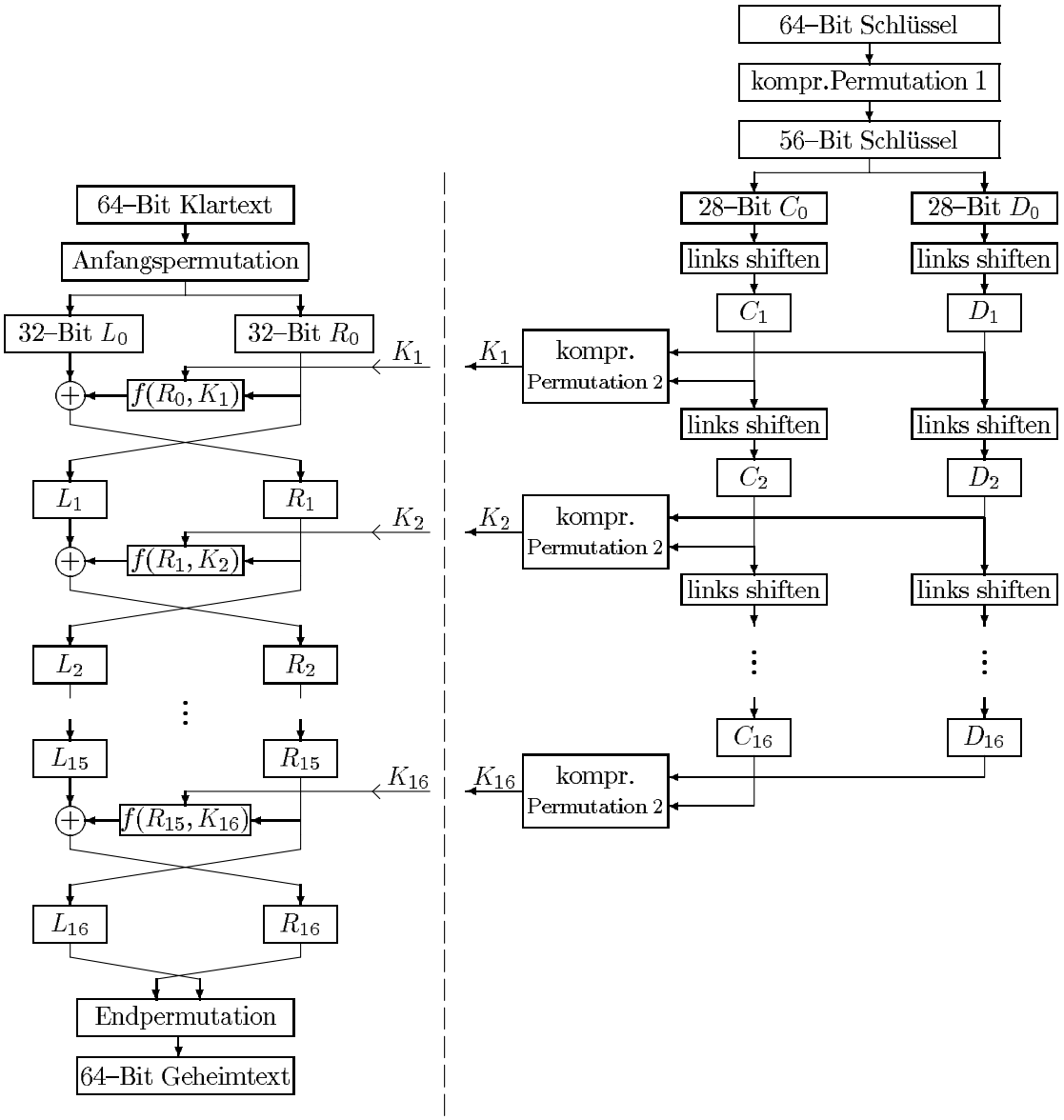

Bild 2.1: Chiffreprinzip des DES