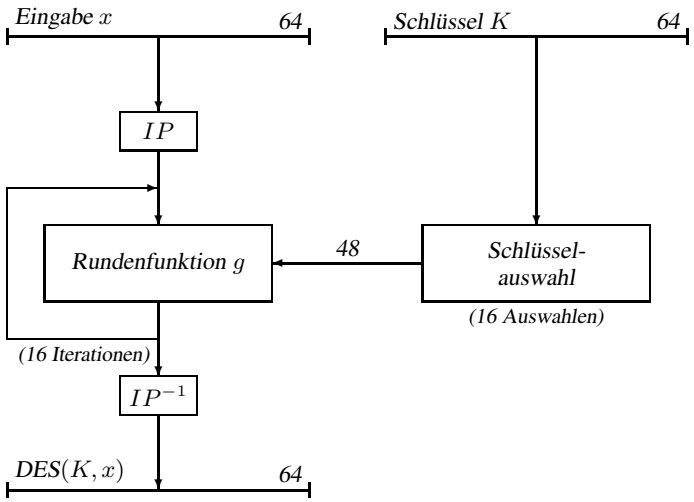
Data Encryption Standard (DES)



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

Initialpermutation IP

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

Ausgabepermutation IP^{-1}

Abbildung 1 Prinzipieller Aufbau des DES

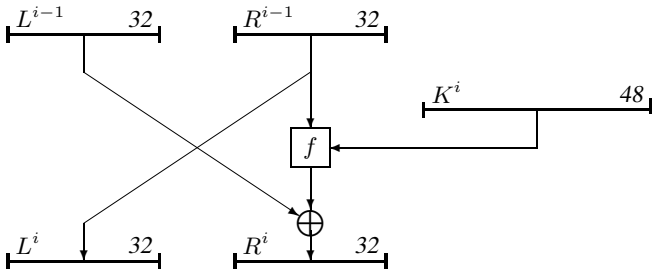
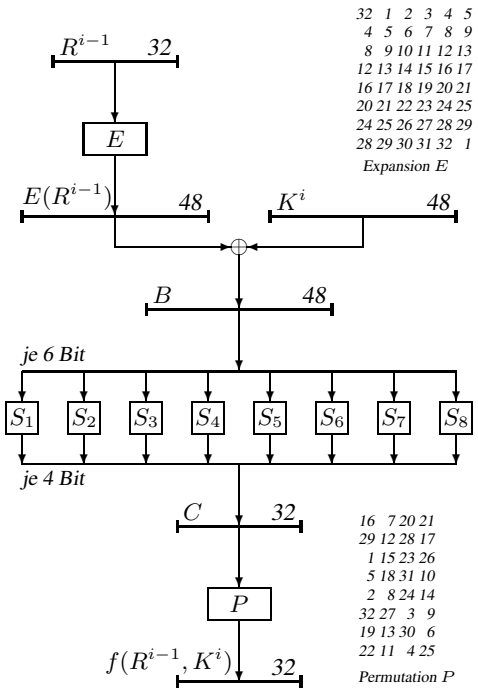


Abbildung 2 Die Rundenfunktion g



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	

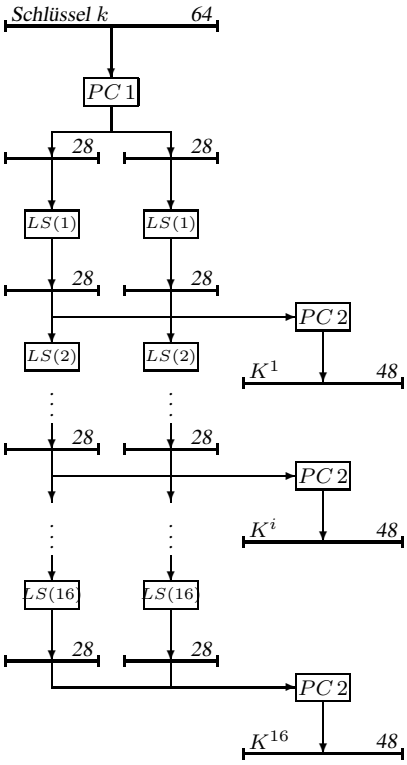
Permutation P

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				

Substitutionsboxen

S_1 :	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2 :	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3 :	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4 :	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5 :	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6 :	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7 :	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8 :	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Abbildung 3 Die Funktion $f(R^{i-1}, K^i)$



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

permuted choice 1

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	

permuted choice 2

Iteration i	Anzahl der Links-Shifts $LS(i)$
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Abbildung 4 Die Schlüsselauswahlfunktion

DES-Betriebsarten

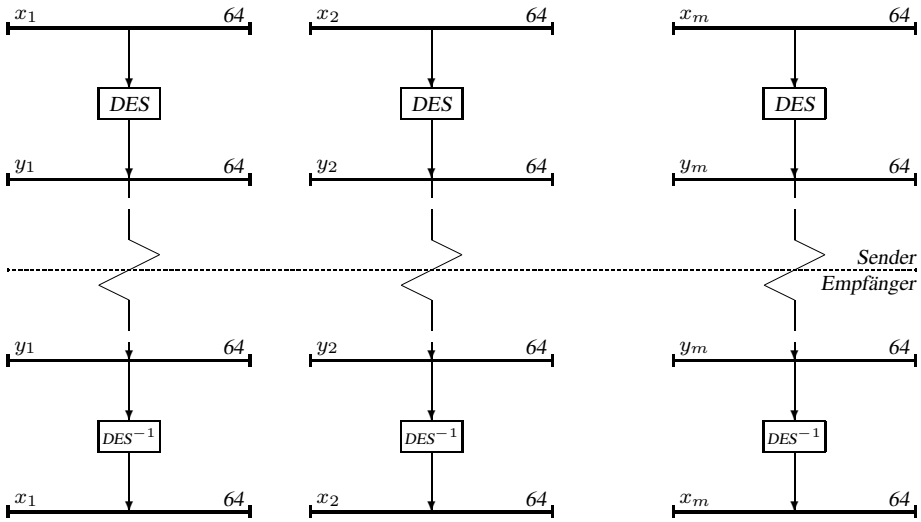


Abbildung 5 Electronic Code Book Mode (ECB)

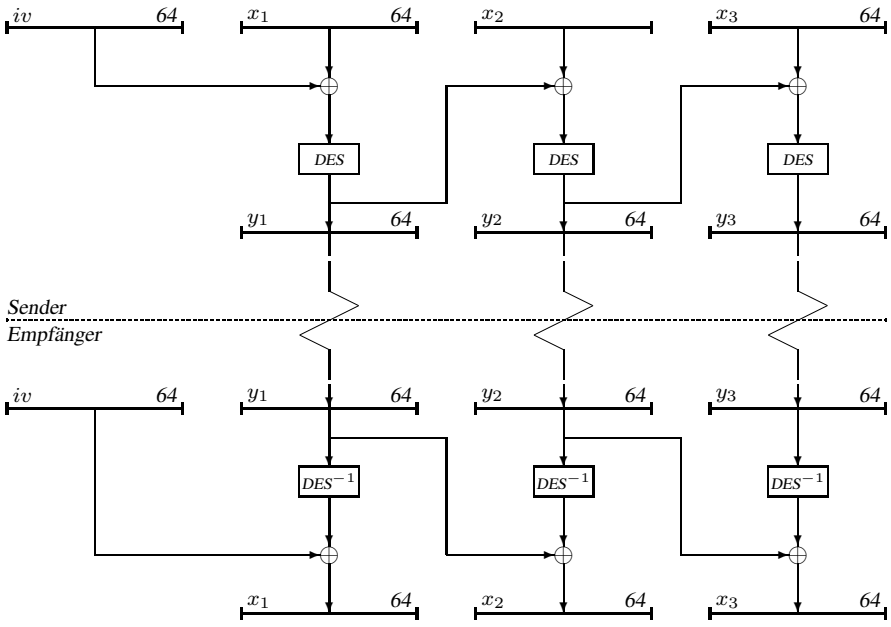


Abbildung 6 Cipher Block Chaining Mode (CBC).

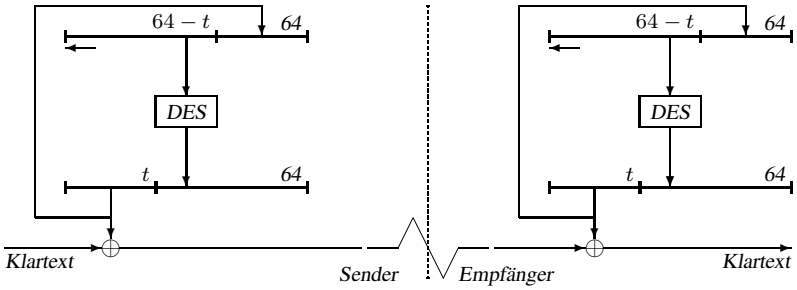


Abbildung 7 Output Feedback Mode (OFB)

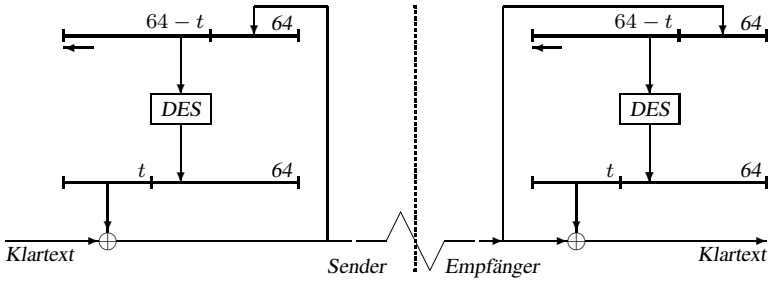


Abbildung 8 Cipher Feedback Mode (CFB)

ECB-Mode (electronic code book; elektronisches Codebuch): Der Klartext x wird in 64-Bit Blöcke x_i (für $1 \leq i \leq m$) zerlegt. Der letzte Block wird, falls nötig, mit einer vorher vereinbarten Bitfolge aufgefüllt. Die Blöcke werden nacheinander mit demselben Schlüssel einzeln verschlüsselt und übertragen (Abbildung 5).

CBC-Mode (cipher block chaining; Blockverkettung des Schlüsseltextes): Um zu verhindern, dass ein Eindringling den Kryptotext verändert, ohne dass der Empfänger dies bemerkt, wird jeder Kryptotextblock nicht nur in Abhängigkeit von dem zugehörigen, sondern auch von den vorausgehenden Klartextblöcken bestimmt (Abbildung 6).

OFB-Mode (output feedback; Rückführung der DES-Ausgabe): Der Klartext x wird in t-Bit Blöcke (für festes t: $1 \leq t \leq 64$) zerlegt. Der DES-Algorithmus dient zur Erzeugung einer pseudozufälligen Folge von t-Bit Blöcken, die bitweise (modulo 2) zu den entsprechenden Klartextblöcken addiert werden. Als Eingabe für den DES-Algorithmus dient ein Schieberegister, das anfangs mit einem Initialisierungsvektor iv geladen ist. Bei jeder Übertragung eines t-Bit Klartextblockes x_i erzeugt der DES-Algorithmus zunächst einen Ausgabevektor, von dem nur die ersten t Bits verwendet werden. Diese dienen sowohl zur Verschlüsselung von x_i, als auch zur Modifikation des Eingaberegisters, in das sie von rechts geschoben werden (Abbildung 7).

CFB-Mode (cipher feedback; Kryptotextrückführung): Ähnlich dem OFB-Mode: zur Erneuerung des Eingaberegisters wird nicht die DES-Ausgabe, sondern der t-Bit Kryptotextblock verwendet (Abbildung 8).