Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
7. Juni 2000

Übungen zur Kryptologie

8. Übung

Abgabe am 21. Juni 2000

Aufgabe 29 (*schriftlich zu bearbeiten,* 9 Punkte)
Berechnen Sie die Wahrscheinlichkeiten p_i für die folgende 3-RC

i	l'_i	r'_i	p_i
0	40080000	04000000	–
1	04000000	00000000	p_1
2	00000000	04000000	p_2
3	04000000	40080000	p_3

Geben Sie auch jeweils die entsprechenden IN-Mengen an.

Aufgabe 30 (*schriftlich zu bearbeiten,* 9 Punkte)
Schildern Sie einen Angriff auf ein 4-Runden DES auf der Basis der 1-RC

i	l'_i	r'_i	p_i
0	20000000	00000000	–
1	00000000	20000000	$p_1 = 1,0$

Aufgabe 31 (*schriftlich zu bearbeiten,* 10 Punkte)
Wir betrachten DES_1 an der ersten S-Box. Gegeben seien die folgenden Ein-/Ausgaben E_1, B_1 (wir betrachten die Eingabe nach der Expansion).

E_1	B_1
000001	1100
110101	0001
011000	1001
101100	1000
100100	1011
010000	1100

Bestimmen Sie *mit der Differenzenmethode* welche Werte für die Bits 1-8 von k_1 noch möglich sind.