Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

3. Exercise sheet
Hand in solutions until Saturday, 30 April 2011, 23:59h.

Exercise 3.1. (7 points)

Suppose that the S-box of the example in the lecture is replaced by the S-box defined by the following substitution: [7]

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

(i) Compute the table of values N_L for this S-box.

(ii) Find a linear approximation using three active S-boxes, and using the piling-up lemma to estimate the bias of the random variable $X_{16} \oplus U_1^4 \oplus U_9^4$.

(iii) How many encrypted messages will you have to request for an attack with this linear approximation in order to achieve similar confidence as with the linear attack described in the lecture? (Remember: In that attack 5 000 encrypted messages were requested.)

Exercise 3.2. (4 points)

For each of the eight DES S-boxes, compute the bias of the random variable $X_2 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4$. (Note that the DES S-boxes map 6-bit input to 4-bit output and are therefore not invertible. But this should not concern you here.) [4]

Exercise 3.3. (4 points)

Imagine an SPN with n-bit input and output, using S-boxes with m-bit input and output. How many rounds are at least necessary to achieve the avalanche criterion. Provide a proper argument for your solution. [4]