Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Monday, 21 November 2011, 23:59:59h.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 3.1 (Using an SPN for decryption). (5 points)

Consider a substitution permutation network (SPN) as in the examples from the lecture, see Heys 2001. Let y be the encryption of a message x with key K by an SPN with S-box S, bit-permutation π and round keys $(K^1, \ldots, K^{N+1})$. Find an S-box S^*, a bit-permutation $\pi*$ and round keys $(L^1, \ldots, L^{N+1})$ that define an SPN for decryption. [5]

Exercise 3.2. (8 points)

Suppose that the S-box of the example in the lecture (see Heys, 2001) is replaced by the S-box defined by the following substitution:

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

(i) Compute the differential table for this S-box. [3]

(ii) Find a differential trail using four active S-boxes, namely $S_{1,1}$, $S_{1,4}$, $S_{2,4}$, and $S_{3,4}$, that has propagation ratio $27/2048$. [3]

(iii) How many encrypted messages will you have to request for a differential attack with this trail in order to achieve similar confidence as with the differential trail described in the lecture? [2]

Exercise 3.3 (Properties of inversion). (5 points)

Consider inversion in $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/(x^5 + x^2 + 1)$, i.e. the function mapping 0 to 0 and any other element z to $1/z$. Produce a differential table that highlights the large values in the table. You might replace small values by some wildcard character. [5]

Exercise 3.4 (Construct!). (15 points)

15

Construct an S-box satisfying Coppersmith's properties S-1 and S-3 to S-7. Your S-box should be chosen randomly as far as possible and must not equal one of the standardized DES S-boxes. Hand in the output of your program and your source code.