Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

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

Exercise 2.1 (Using an SPN for decryption). (7 points)

Let y be the encryption of a message x with key K by an SPN with S-box π_S and bit-permutation π_P. In other words, 7

$$y = \text{SPN}(x, \pi_S, \pi_P, (K^1, \ldots, K^{N+1})),$$

where $(K^1, \ldots, K^{N+1})$ is the key schedule. Find an S-box π_S^*, a bit-permutation π_P^* and a key schedule $(L^1, \ldots, L^{N+1})$, such that

$$x = \text{SPN}(y, \pi_S^*, \pi_P^*, (L^{N+1}, \ldots, L^1)).$$

Exercise 2.2. (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
$\pi_S(z)$	E	2	1	3	D	9	0	6	F	4	5	A	8	C	7	B

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

(ii) Find a differential trail using four active S-boxes, namely S_1^1, S_4^1, S_4^2, and S_4^3, that has propagation ratio $27/2048$.

(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?

Exercise 2.3. (3 points)

Suppose that X_1, X_2, and X_3 are independent discrete random variables defined on the set $\{0, 1\}$. Let ϵ_1 denote the bias of X_i, for $i = 1, 2, 3$. Under which conditions on ϵ_i are $X_1 \oplus X_2$ and $X_2 \oplus X_3$ independent? (Recall, that in the lecture, we saw that this is in general *not* the case.) 3

Exercise 2.4. (3 points)

Daniel shows you his self-made random-number-generator which produces 16-bit numbers. But the distribution is not uniform! Daniel's favorite number is chosen with probability $27/1024$ – and you know that probability, but not the value of the number.

$\boxed{2}$ (i) How many calls to the random-number-generator do you expect to make, such that the favorite number occurs at least 9 times?

$\boxed{1}$ (ii) Assume that the probability distribution of the non-favorite numbers is uniform. What is the probability that any other number occurs at least 5 times, given the numbers of calls you derived in (i)?