Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 5

Friday, May 18, 2018

Problem 1. We consider the Data Encryption Standard (DES) algorithm.

a) How can the same encryption algorithm of DES be used for decryption?

DES encrypts blocks of 64 bits using a key of 56 bits. For each 7 key bits, one (odd) parity bit for error detection is added. The key of a DES cipher is of the form:

$$K_0 = (k_1, \dots, k_7, b_1, k_9, \dots, k_{15}, b_2, k_{17}, \dots, k_{57}, \dots, k_{63}, b_8).$$

From this key K_0, 16 round keys $K_1, K_2, ..., K_{16}$ are generated. The 56 key bits of K_0 are divided into two blocks C_0 and D_0 of 28 bits each as described in the left table below.

1	2	3	4	5	6	7	b_1
9	10	11	12	13	14	15	b_2
17	18	19	20	21	22	23	b_3
25	26	27	28	29	30	31	b_4
33	34	35	36	37	38	39	b_5
41	42	43	44	45	46	47	b_6
49	50	51	52	53	54	55	b_7
57	58	59	60	61	62	63	b_8

C_0 ↑ (green block: columns 1–3 of all rows and 36, 44, 52, 60), D_0 ↑ (red block: 4–7, 12–15, 20–23, 28–31, and columns 5–7 of rows 5–8)

PC2					
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

C_0 is read column-wise from 57 to 36 and D_0 column-wise from 63 to 4.

In a second step, C_n and D_n for $n = 1, ..., 16$, are each generated from C_{n-1} and D_{n-1} by a cyclic left-shift of s_n positions, where s_n is defined by:

$$s_n = \begin{cases} 1, & \text{if } n \in \{1, 2, 9, 16\} \\ 2, & \text{otherwise} \end{cases}$$

From each of these (C_n, D_n), with $n = 1, ..., 16$, one now selects 48 key bits as in the above table PC2 on the right to obtain K_n.

In the following, a particular pair of keys for DES is considered[1]:

$$K_0 = (\texttt{01FE 01FE 01FE 01FE}), \quad \hat{K}_0 = (\texttt{FE01 FE01 FE01 FE01})$$

[1]The keys are shown in hexadecimal representation.

b) Determine (C_0, D_0) and (C_1, D_1) from K_0, and $(\hat{C}_0, \hat{D}_0)$ and $(\hat{C}_1, \hat{D}_1)$ from $\hat{K}_0$.

c) Which of the generated subkeys $K_1, K_2, ..., K_{16}$ are identical when K_0 is used?

d) Show that $\text{DES}_{\hat{K}_0}(\text{DES}_{K_0}(M)) = M$ holds for all $M \in \mathcal{M}$.

Problem 2. (*DES Complementation property*) Let M be a block of bits of length 64 and let K be a block of bits of length 56. Let $\text{DES}(M, K)$ denote the encryption of M with key K using the DES cryptosystem. $\overline{x}$ denotes the bitwise complement of a block x.

a) Show that the *complementation property* holds:

$$\text{DES}(M, K) = \overline{\text{DES}(\overline{M}, \overline{K})}$$

b) How does the complementation property help to attack DES?

Problem 3. (*weak DES keys*) There are four so called *weak* DES keys. One of those keys is

$$K = 00011111\ 00011111\ 00011111\ 00011111\ 00001110\ 00001110\ 00001110\ 00001110.$$

a) What happens if you use this key?

b) Can you find the other three weak keys?