Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 9
Version 25.06.2020

Exercise 1.

Check the correctness of the following DES master key: `1A DE C0 28 FF 34 2A 8B`. If necessary, adjust the row parity bits in order to create a valid DES master key.

Exercise 2.

Let $X =$ `AF 32 16 A3` be a text block and let $\tilde{K} =$ `B2 2B EE 5B 5E CC` be a fixed round key of the inner block cipher of the DES. Compute the four associated output bits of the first S-box.

Exercise 3.

a) Show that the DES master key `1F FE 01 E0 0E FE 01 F1` generates precisely 4 different round keys.

b) Show that the DES master key `40 DF 80 BF A1 AE A1 AE` generates precisely 14 different round keys.

Exercise 4.

Let $E_K(P)$ represent the ciphertext associated with a plain text $P \in \mathbb{Z}_2^{64}$ and a master key $K \in \mathbb{Z}_2^{64}$ using the DES. Set $C := E_K(P)$ and $C' := E_{\sim K}(\sim P)$ where $\sim\colon \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ denotes the **bitwise complement operator** of its argument,i.e. $\sim$ converts every 1 to a 0 and vice versa. Prove that $C' = \sim C$ holds.

Note: the actual structure of **S-boxes** and other components of the system are irrelevant for the above property.