LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / I & C
CH-1015 Lausanne
Phone: ++41 (0) 21 693 76 03
Fax: ++41 (0) 21 693 68 79
URL: http://lasecwww.epfl.ch

Exercise S#2

cDES is a block cipher based on a 16 rounds Feistel scheme where the round function $f_i : \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ is defined by $f_i(m) = m \oplus k_i$, where k_i is the i-th round key. All the round keys are assumed to be independent from each other. As a consequence, the secret key of cDES can be expressed as $k = (k_1, k_2, \ldots, k_{16}) \in \{0,1\}^{512}$. An adversary knows one plaintext/ciphertext pair $M, C \in \{0,1\}^{64}$ such that

$$C = \mathsf{cDES}_k(M).$$

Show that the adversary can easily deduce the ciphertext C' associated to a plaintext M' of his choice.