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#1

Consider the following construction based on DES:

$$\mathsf{DESV}_{k,k_1}(M) = \mathsf{DES}_k(M) \oplus k_1.$$

Assume an adversary knows d distinct pairs of plaintext/ciphertext $M_i, C_i \in \{0,1\}^{64}$ such that

$$C_i = \mathsf{DESV}_{k,k_1}(M_i)$$

for all $i = 1, \ldots, d$. We assume that $d \geq 2$. Find an attack that recovers both k and k_1 using on the order of 2^{56} DES encryption.