Cryptographie – Feuille d'exercices 3

Cryptanalyse du chiffrement DES

M1 Informatique – 2014-2015

1 Exercice 1

1. Montrer que
$$\mathrm{DES}_{\overline{K}}(\overline{x}) = \overline{\mathrm{DES}_K(x)}$$
où on désigne par $\overline{z}$ le *complément* bit à bit de z, pour toute chaîne de bits z.
2. En déduire une attaque par recherche exhaustive sur la clé du DES, dont la complexité soit en moyenne de 2^{54} chiffrements DES.

2 Exercice 2

1. On dit qu'une clé K du DES est *faible* si DES_K est une involution. Trouver quatre clés faibles pour le DES.
2. On dit qu'une clé K du DES est *semi-faible* si elle n'est pas faible et s'il existe K' tel que
$$\mathrm{DES}_K^{-1} = \mathrm{DES}_{K'}.$$
Trouver six paires (K, K') de clés semi-faibles pour le DES.