密 碼 學 與 應 用 補 救 作 業

94/12/08 (四)

(Trappe 2nd Ed. 4.9.6)

Suppose Triple DES is performed by choosing two keys K_1, K_2 and computing $E_{K_1}(E_{K_2}(E_{K_2}(m)))$ (note that the order of the keys has been modified from the usual two-key version of Triple DES). Show how to attack this modified version with a meet-in-the-middle attack.