Original paper of Vaudenay on Padding oracle attack

Vaudenay, S.: Security flaws induced by CBC padding – applications to SSL, IPSEC, WTLS. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 534–546. Springer, Heidelberg (2002).