DES 解密与加密证明

Cuiting Shi

2016 年 11 月 29 日

1 DES 解密与加密关系

证明 DES 解密只需要将原本用于加密的 subkeys 的次序颠倒即可
首先，对于加密，已知 LE_i, RE_i, 求 LE_{i+1}, RE_{i+1}, 则有

$$\begin{aligned} LE_{i+1} &= RE_i; \\ RE_{i+1} &= LE_i \oplus Fiestel(RE_i, subkeys_i) \\ &= LE_i \oplus Permutation(\\ &\quad SubstituteSBOX(ExpandBlock(RE_i) \oplus Subkey_i)) \end{aligned} \tag{1}$$

则对于解密，相当于已知 LE_{i+1}, RE_{i+1}, 求 LE_i, RE_i, 则有

$$\begin{aligned} RE_i &= LE_{i+1}; \\ LE_i &= RE_{i+1} \oplus Fiestel(RE_i, subkeys_i) \\ &= LE_i \end{aligned} \tag{2}$$