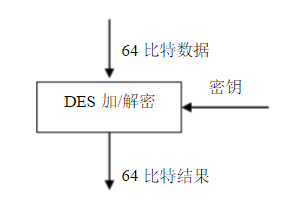
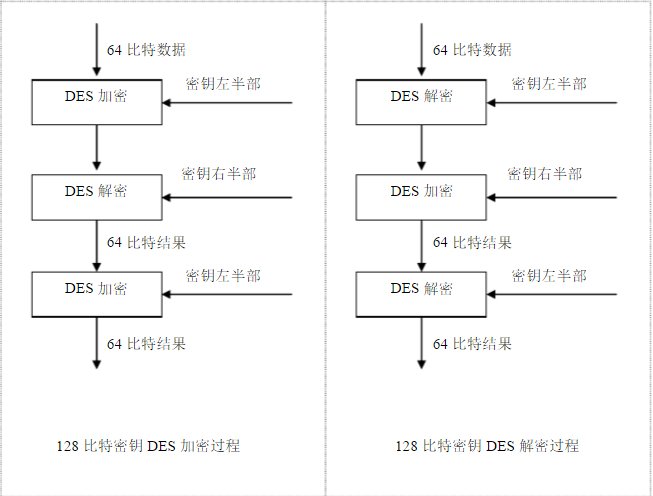
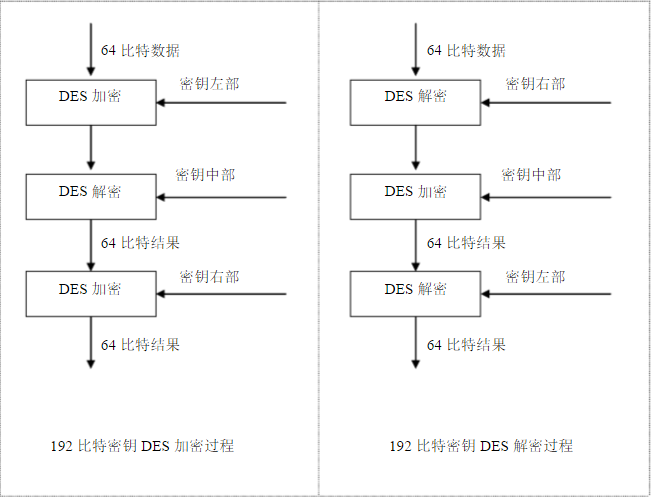
## 1.1 64比特（8字节）密钥DES加/解密



## 1.2 128比特（16字节）密钥DES加/解密



## 1.3 192比特（24字节）密钥DES加/解密



## 1.4 XOR MAC算法

(1)XOR MAC算法可以使用单倍长、双倍长、三倍长密钥。

(2)MAC数据先按8字节分组，表示为D0～Dn，如果Dn不足8字节时，尾部以字节00补齐。

(3)D0～Dn所有分组异或，然后用MAC密钥加密。

(4)取加密结果的左半部作为MAC。

## 1.5 ANSI X9.9MAC算法

(1)ANSI X9.9MAC算法只使用单倍长密钥。

(2)MAC数据先按8字节分组，表示为D0～Dn，如果Dn不足8字节时，尾部以字节00补齐。

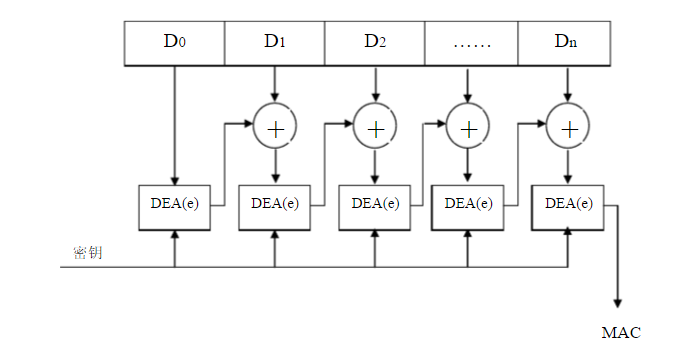
(3)用MAC密钥加密D0，加密结果与D1异或作为下一次的输入。

(4)将上一步的加密结果与下一分组异或，然后再用MAC密钥加密。

(5)直至所有分组结束，取最后结果的左半部作为MAC。

图示如下，其中：DEA(e) 表示加密操作

‘⊕’表示异或操作



## 1.6 ANSI X9.19 MAC算法描述

(1)ANSI X9.19MAC算法只使用双倍长密钥。

(2)MAC数据先按8字节分组，表示为D0～Dn，如果Dn不足8字节时，尾部以字节00补齐。

(3)用MAC密钥左半部加密D0，加密结果与D1异或作为下一次的输入。

(4)将上一步的加密结果与下一分组异或，然后用MAC密钥左半部加密。

(5)直至所有分组结束。

(6)用MAC密钥右半部解密(5)的结果。

(7)用MAC密钥左半部加密(6)的结果。

(8)取(7)的结果的左半部作为MAC。

图示如下，其中：DEA(e)表示加密操作，DEA(d)表示解密操作，‘⊕’表示异或操作。

