## **第4章 SM4分组密码算法**

**1. SM4是一种分组密码算法，其分组长度和密钥长度分别为（  ）。**

A．64位和128位　　B．128位和128位　　C．128位和256位　　D．256位和256位

答案：B

**2. SM4分组密码算法中某S盒定义如下，设S盒的输入为DE，则经S盒运算的输出结果是多少？**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | D6 | 90 | E9 | FE | CC | E1 | 3D | B7 | 16 | B6 | 14 | C2 | 28 | FB | 2C | 05 |
| 1 | 2B | 67 | 9A | 76 | 2A | BE | 04 | C3 | AA | 44 | 13 | 26 | 49 | 86 | 06 | 99 |
| 2 | 9C | 42 | 50 | F4 | 91 | EF | 98 | 7A | 33 | 54 | 0B | 43 | ED | CF | AC | 62 |
| 3 | E4 | B3 | 1C | A9 | C9 | 08 | E8 | 95 | 80 | DF | 94 | FA | 75 | 8F | 3F | A6 |
| 4 | 47 | 07 | A7 | FC | F3 | 73 | 17 | BA | 83 | 59 | 3C | 19 | E6 | 85 | 4F | A8 |
| 5 | 68 | 6B | 81 | B2 | 71 | 64 | DA | 8B | F8 | EB | 0F | 4B | 70 | 56 | 9D | 35 |
| 6 | 1E | 24 | 0E | 5E | 63 | 58 | D1 | A2 | 25 | 22 | 7C | 3B | 01 | 21 | 78 | 87 |
| 7 | D4 | 00 | 46 | 57 | 9F | D3 | 27 | 52 | 4C | 36 | 02 | E7 | A0 | C4 | C8 | 9E |
| 8 | EA | BF | 8A | D2 | 40 | C7 | 38 | B5 | A3 | F7 | F2 | CE | F9 | 61 | 15 | A1 |
| 9 | E0 | AE | 5D | A4 | 9B | 34 | 1A | 55 | AD | 93 | 32 | 30 | F5 | 8C | B1 | E3 |
| A | 1D | F6 | E2 | 2E | 82 | 66 | CA | 60 | C0 | 29 | 23 | AB | 0D | 53 | 4E | 6F |
| B | D5 | DB | 37 | 45 | DE | FD | 8E | 2F | 03 | FF | 6A | 72 | 6D | 6C | 5B | 51 |
| C | 8D | 1B | AF | 92 | BB | DD | BC | 7F | 11 | D9 | 5C | 41 | 1F | 10 | 5A | D8 |
| D | 0A | C1 | 31 | 88 | A5 | CD | 7B | BD | 2D | 74 | D0 | 12 | B8 | E5 | B4 | B0 |
| E | 89 | 69 | 97 | 4A | 0C | 96 | 77 | 7E | 65 | B9 | F1 | 09 | C5 | 6E | C6 | 84 |
| F | 18 | F0 | 7D | EC | 3A | DC | 4D | 20 | 79 | EE | 5F | 3E | D7 | CB | 39 | 48 |

答案：经S盒运算的输出结果为表中第D行、第E列的值，即Sbox(DE)=0xB4。

**3.证明：SM4分组密码算法的对合性**

答案：SM4的加密轮函数，加密变换:







将SM4的加密轮函数，分成加密函数G和数据交换E；

轮函数。

 

这说明加密函数G是对合的。

因为，E变换为



显然，E是对合运算。综上，轮函数是对合的。

SM4的加密过程为：

SM4的解密过程为：

比较SM4和SM4-1可知，运算相同，只有密钥的使用顺序不同。所以SM4是对合的。

**4.证明：SM4分组密码算法的可逆性。**

答案：SM4的加密过程的数据变化：



(其中最后一步变换为反序)

密文(Y0,Y1,Y2,Y3)解密过程数据的变化：

(其中最后一步变换为反序)



所以SM4是可逆的。

**5. 若选取“Love you perfect”作为SM4分组密码算法的初始密钥，经过密钥扩展算法生成的前三个子密钥分别是多少？**

答案:Love you perfect

初始密钥MK：4C 6F 76 65 20 79 6F 25 20 70 65 72 66 65 63 74

系统参数FK：A3 B1 BA C6 56 AA 33 50 67 7D 91 97 B2 70 22 DC

K0=EF DE CC A3

K1=76 D3 5C 75

K2=47 0D F4 E5

K3=D4 15 41 A8

K4=3A 41 93 87

K5=DD CC D4 46

K6=89 D3 2A 6C

CK0=00 31 62 93

CK1=C4 F5 26 57

CK2=88 B9 EA 1B

前三个子密钥：

rk0=K4=9A 41 93 87

rk1=K5=DD CC D4 46

rk2=K6=89 D3 2A 6C

**6.若给出“AE260F63”作为线性变换*L*的输入，输出结果是多少？**

答案:设输入为B，输出为C，则



输入B=AE260F63，则输出C=D0A322C2