密 码 学

（第四讲）

中国商用密码SMS4

张焕国

武汉大学计算机学院

目　录

目　录

一、我国的密码政策

一、我国的密码分级：

①核心密码：

用于保护党、政、军的核心机密。

②普通密码：

用于保护国家和事企业单位的低于核心机密而高于商业机密的密码信息。

③商用密码：

用于保护国家和事企业单位的非机密的敏感信息。

④个人密码：

用于保护个人的隐私信息。

前三种密码均由国家密码管理局统一管理。

一、我国的密码政策

二、我国商的业密码政策

①统一领导：

国家密码管理局统一领导。

②集中管理：

国家密码管理局办公室集中管理。

③定点研制：

研制只允许定点单位进行。

④专控经营：

经许可的单位才能经营。

⑤满足使用：

国内各单位都可申请使用。

二、我国商用密码SMS4

一、我国商用密码概况

(1) 密码的公开设计原则

密码的安全应仅依赖于对密钥的保密，不依赖于对算法的保密。

(2) 公开设计原则并不要求使用时公开所有的密码算法

核心密码不能公布算法；

核心密码的设计也要遵循公开设计原则。

(3) 商用密码应当公开算法

①美国DES开创了公开商用密码算法的先例；

②美国经历DES（公开）→EES（保密）→AES（公开）。

③欧洲也公布商用密码算法

二、我国商用密码SMS4

(4)我国的商用 密码概况

- 我国在密码技术方面具有优势：

  密码理论、密码分析

- 长期以来不公开密码算法，只提供密码芯片

  少数专家设计，难免有疏漏；

  难于标准化，不利于推广应用。

- 2006年2月我国公布了部分商用密码算法；

  ☆*商用密码管理更科学化、与国际接轨；*

  ☆*将促进我国商用密码的发展。*

二、我国商用密码SMS4

二、SMS4 密码概况

①分组密码：

数据分组长度=128位、密钥长度=128位

数据处理单位：字节（8位），字（32位）

②密码算法结构：

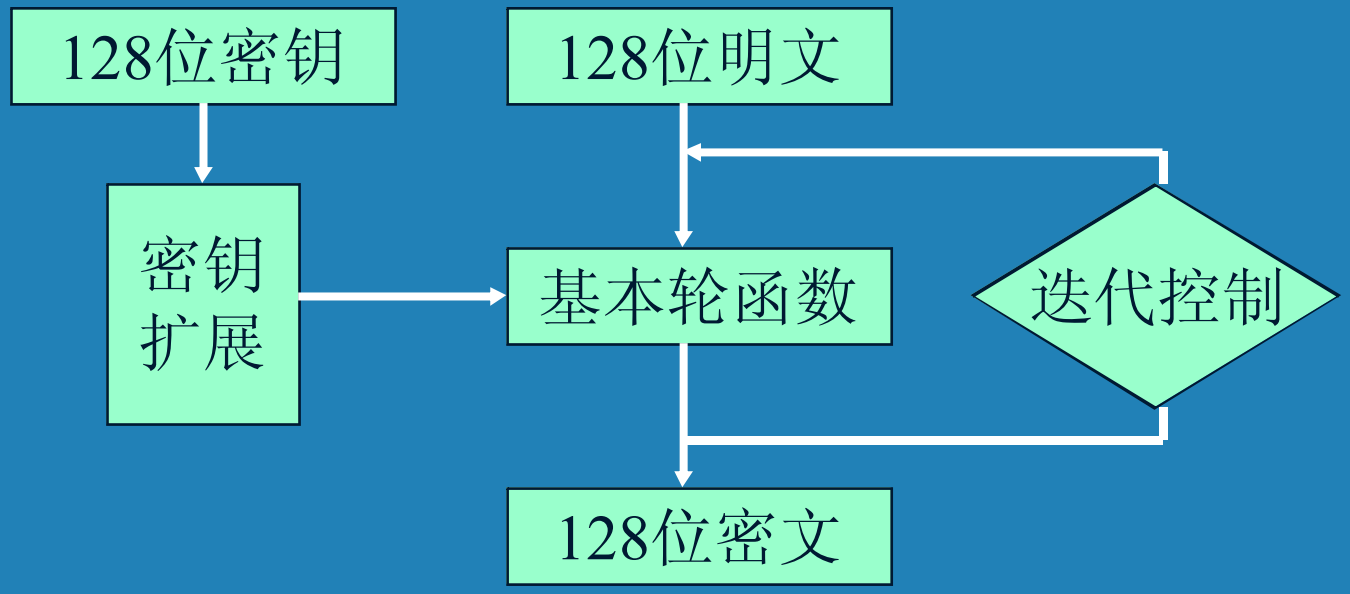
基本轮函数加迭代

对合运算：解密算法与加密算法相同

二、我国商用密码SMS4

二、SMS4 密码概况

②密码算法结构：



二、我国商用密码SMS4

三、SMS4 密码算法

1、基本运算：

① 模2加：⊕，32 比特异或运算

② 循环移位：<<< *i* ，把32位字循环左移*i* 位

2、基本密码部件：

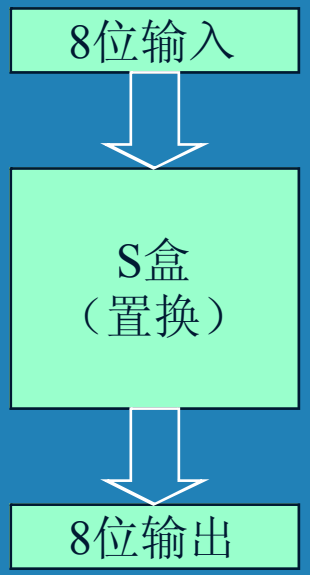
① 非线性字节变换部件S盒：

☆*8位输入、8位输出。*

☆*本质上，8位的非线性置换。*

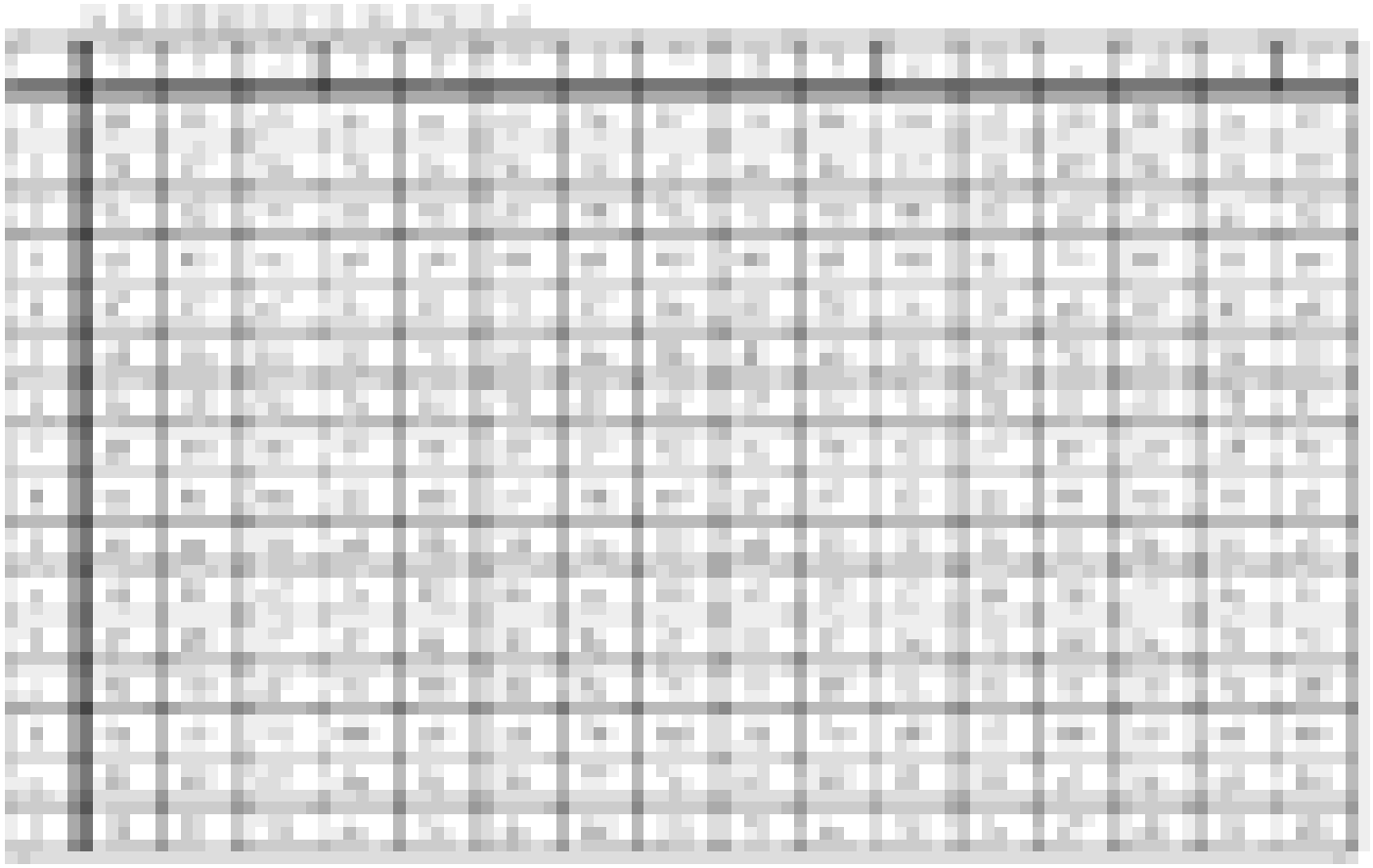
☆*设输入位a，输出位b，表示为：*

$b=S\_Box(a)$



二、我国商用密码SMS4

S盒中数据为16进制数



二、我国商用密码SMS4

☆S盒的置换规则：

以输入的前半字节为行号，后半字节为列号，行列交叉点处的数据即为输出。

举例：*设输入为“ef”，则行号为e，列号为f，于是S盒的输出值为表中第e行和第f列交叉点的值，*

Sbox(‘ef’)= ‘84’。

②非线性字变换τ：*32位字的非线性变换*

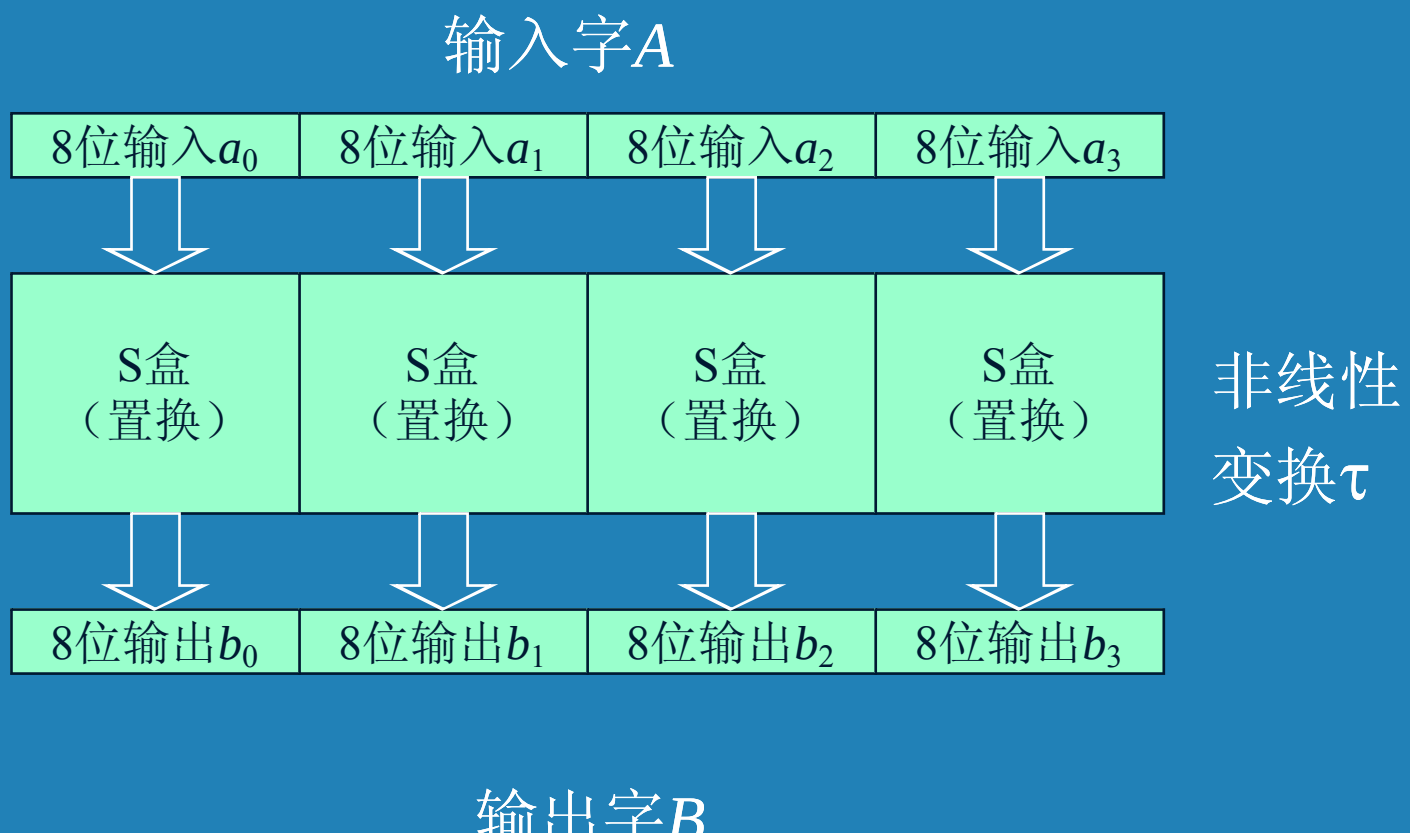
▼4个S盒并行置换；

▼设输入字$A=(a_0,a_1,a_2,a_3)$,输出字$B=(b_0,b_1,b_2,b_3)$,

$B=\tau(A)=(S\_box(a_0), S\_box(a_1), S\_box(a_2), S\_box(a_3))$

二、我国商用密码SMS4

②非线性变换τ：*32位字的非线性变换*



二、我国商用密码SMS4

③字线性部件*L*变换：

☆*32*位输入、*32*位输出。

☆设输入位*B*，输出位*C*，表为：

$$C=L(B)$$

☆运算规则：

$$C=L(B)$$

$$=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24)$$

④字合成变换*T*：

☆由非线性变换τ 和线性变换L 复合而成；

☆ $T(X)=L(\tau(X))$。先*S*盒变换，再*L*变换。

二、我国商用密码SMS4

3、轮函数F：

☆输入数据：（X_0，X_1，X_2，X_3），128位，四个32位字。

☆输入轮密钥：rk，32位字。

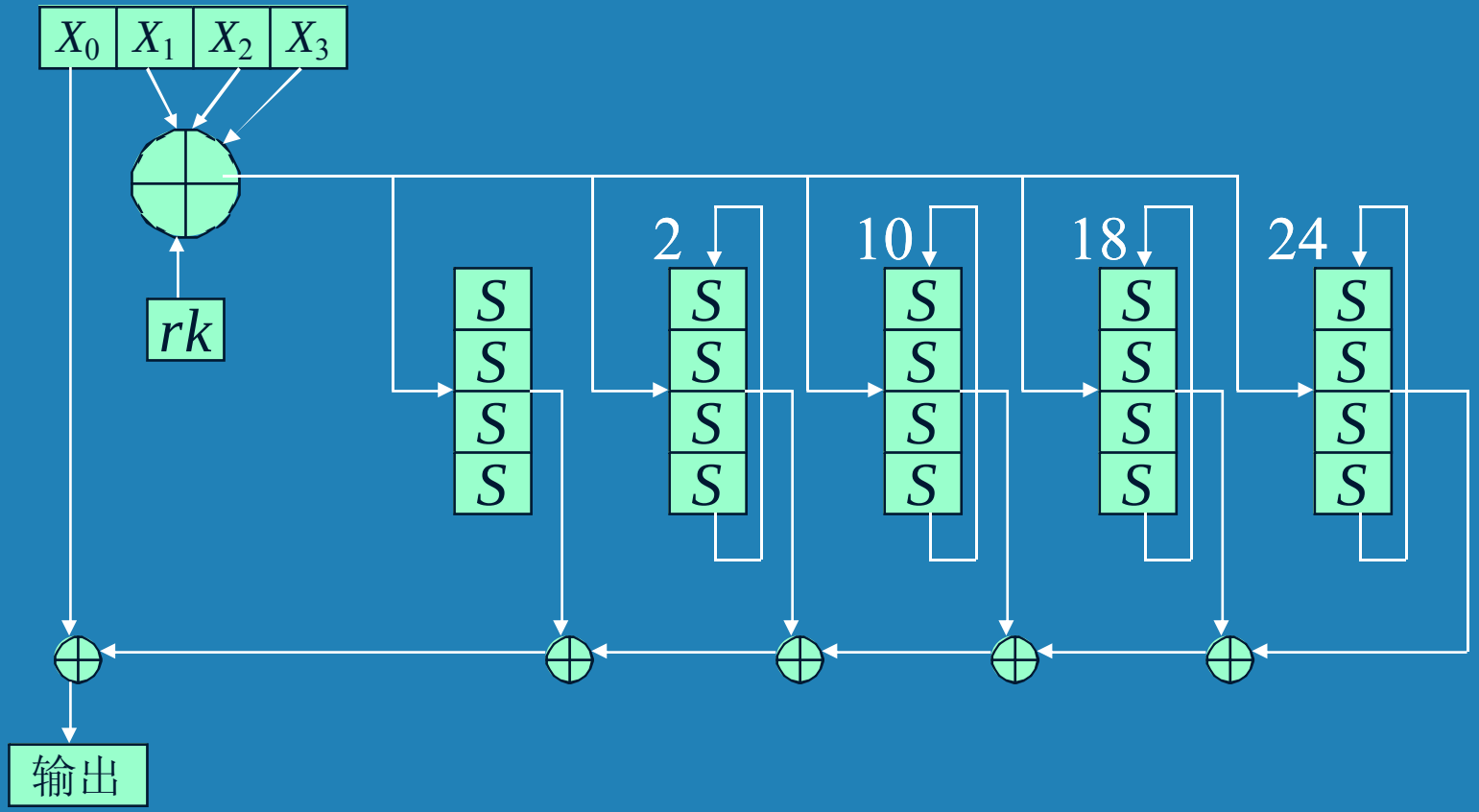
☆输出数据：32位字。

☆轮函数F：

$$F(X_0, X_1, X_2, X_3, rk)$$
$$= X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$$

二、我国商用密码SMS4

3、轮函数F：



二、我国商用密码SMS4

4、加密算法：

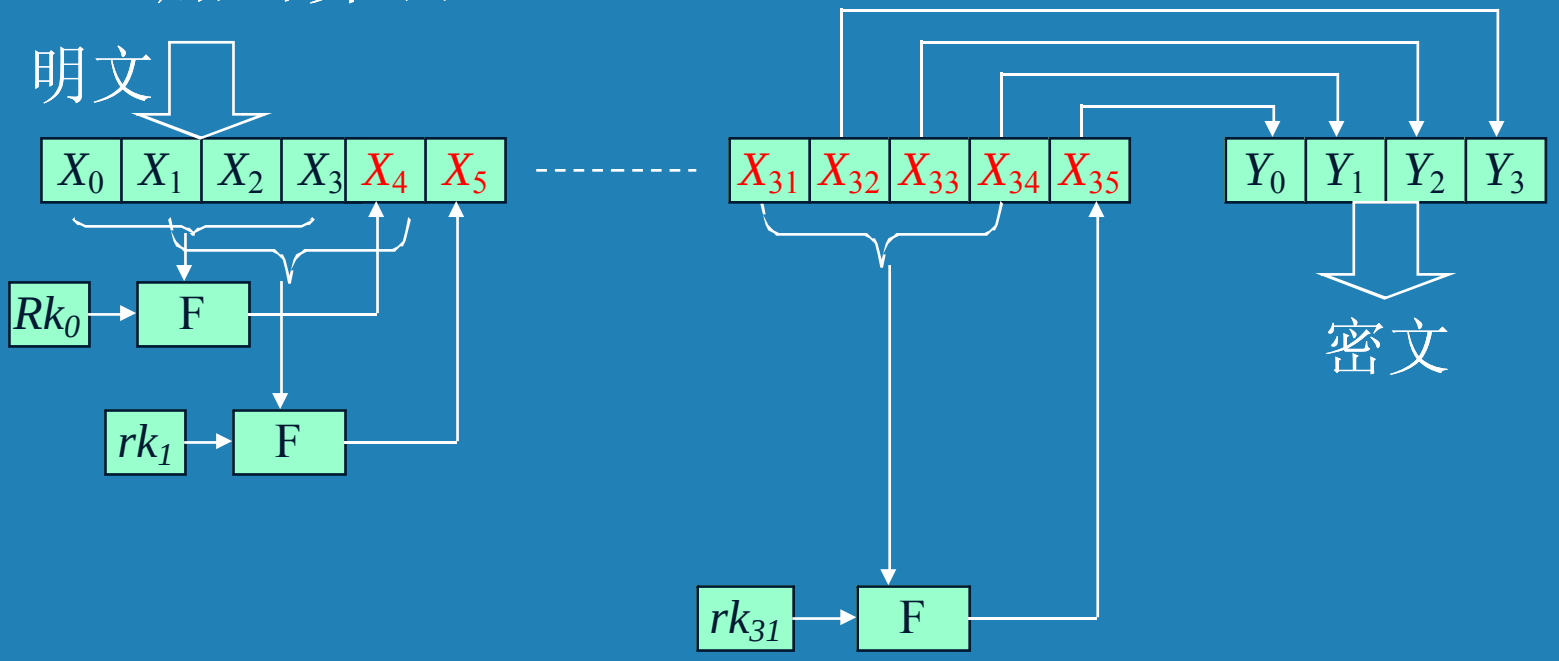
- *输入明文：（X_0，X_1，X_2，X_3），128位，四个字。*
- *输入轮密钥：rk_i，$i=0,1,\ldots,31$，32个字。*
- *输出密文：（Y_0，Y_1，Y_2，Y_3），128位，四个字。*
- *算法结构：轮函数的32轮迭代，每轮使用一个轮密钥。*
- *加密算法：*

$$X_{i+4}=F\ (X_i,\ X_{i+1},\ X_{i+2},\ X_{i+3},\ rk_i)$$

$$\begin{cases} = X_i \oplus T\ (X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i),\quad i=0,1\ldots31 \\ (Y_0,\ Y_1,\ Y_2,\ Y_3) = (X_{35},\ X_{34},\ X_{33},\ X_{32}) \end{cases}$$

二、我国商用密码SMS4

4、加密算法：



二、我国商用密码SMS4

5、解密算法：

- 输入密文：（X_0，X_1，X_2，X_3）
- 输入轮密钥：rk_i，$i=31,30,\ldots,1,0$
- 输出明文：（Y_0，Y_1，Y_2，Y_3）
- 算法：轮函数的32轮迭代，每轮使用一个轮密钥。
- 解密算法：

$$\begin{cases} X_{i+4}=F\ (X_i,\ X_{i+1},\ X_{i+2},\ X_{i+3},\ rk_i) \\ \quad\quad = X_i \oplus T\ (X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i),\ i=31,\ldots 1,0 \\ (Y_0,\ Y_1,\ Y_2,\ Y_3) = (X_{35},\ X_{34},\ X_{33},\ X_{32}) \end{cases}$$

二、我国商用密码SMS4

6、密钥扩展算法：

①常数FK

- *在密钥扩展中使用一些常数*

  FK_0=(A3B1BAC6)，FK_1=(56AA3350)，
  FK_2=(677D9197)， FK_3=(B27022DC)。

二、我国商用密码SMS4

6、密钥扩展算法：

②固定参数CK

- *32 个固定参数Ck_i，i=0,1,2…31*

  00070e15, 1c232a31, 383f464d, 545b6269,
  70777e85, 8c939aa1, a8afb6bd, c4cbd2d9,
  e0e7eef5, fc030a11, 181f262d, 343b4249,
  50575e65, 6c737a81, 888f969d, a4abb2b9,
  c0c7ced5, dce3eaf1, f8ff060d, 141b2229,
  30373e45, 4c535a61, 686f767d, 848b9299,
  a0a7aeb5, bcc3cad1, d8dfe6ed, f4fb0209,
  10171e25, 2c333a41, 484f565d, 646b7279

产生规则：Ck_{ij}= (4i+j) ×7（mod 256） ，i=0,1,2…31,j=0,1,…3 。

二、我国商用密码SMS4

6、密钥扩展算法：

- 输入加密密钥：$MK=(MK_0, MK_1, MK_2, MK_3)$
- 输出轮密钥：rk_i，$i=0, 1\ldots,30, 31$
- 中间数据：K_i，$i=0, 1\ldots,34, 35$
- 密钥扩展算法：

① $(K_0,K_1,K_2,K_3)=(MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$

② For $i=0, 1\ldots,30, 31$ Do

$$ik_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$$

- 说明：T’变换与加密算法轮函数中的T基本相同，只将其中的线性变换L修改为以下：L’

$$L'(B)=B \oplus (B \lll 13) \oplus (B \lll 23)$$

二、我国商用密码SMS4

7、实例：

- 明文: 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
- 密钥: 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
- 密文: 68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46

8、安全性

①国家专业机构设计。算法简洁，以字和字节为处理单位，对合运算，符合当今分组密码主流。

②专业机构进行了密码分析，因此是安全的。

③民间学者对21轮SMS4进行了差分密码分析。

④尚需经过实践检验。

二、我国商用密码SMS4

练习题

1、分析SMS4在密码结构上与DES和AES有何异同？

2、编程研究SMS4的S盒的以下特性：

①输入改变1位，输出平均改变多少位？

②对于一个输入，连续施加S盒变换，变换多少次时出现输出等于输入？

3、我国公布商用密码算法有何意义？

大作业

以SMS4作为加密算法开发出文件加密软件系统：

- *具有文件加密和解密功能；*
- *具有加解密速度统计功能；*
- *采用密文反馈链接和密文挪用短块处理技术；*
- *具有较好的人机界面。*