作业二

题目：2012 年 3 月，国家密码管理局发布了一个分组密码标准，即 SM4 算法作为我国商用密码标准算法。

请回答以下问题：

1. SM4 算法的分组长度和密钥长度分别是多少？迭代轮次是多少？是以多少位为单位进行加解密运算的。

答：分组长度为 128bit，密钥长度也为 128bit，迭代轮次为 32 轮，以字（32 位）为单位进行加解密运算。

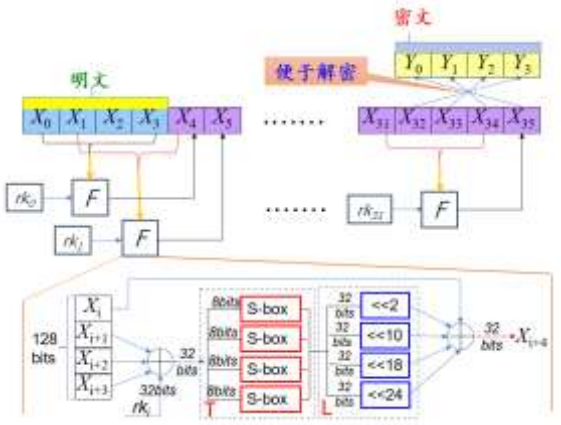
2. 描述 SM4 算法的加密过程。

答：假设明文输入为(X_0, X_1, X_2, X_3)，则$X_4 = F(X_0, X_1, X_2, X_3), X_5 = F(X_1, X_2, X_3, X_4), \ldots$，以此类推，共迭代 32 轮，最后输出密文：$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32})$。其中轮函数$F$的步骤如下：

1) 计算$X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i$，其中$rk_i$为轮密钥，输出 32bit 结果；

2) 将步骤 1）输出的 32bit 结果分为 4 组 8bit 数据带入 s 盒进行非线性变换（T 变换），再将变换结果重新组合为 32bit 数据作为输出B；

3) 将B分别左移 2、10、18、24 位进行线性变换（L 变换），计算$X_{i+4} = X_i \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24)$。



3. 描述 SM4 算法的子密钥生成过程。

答:

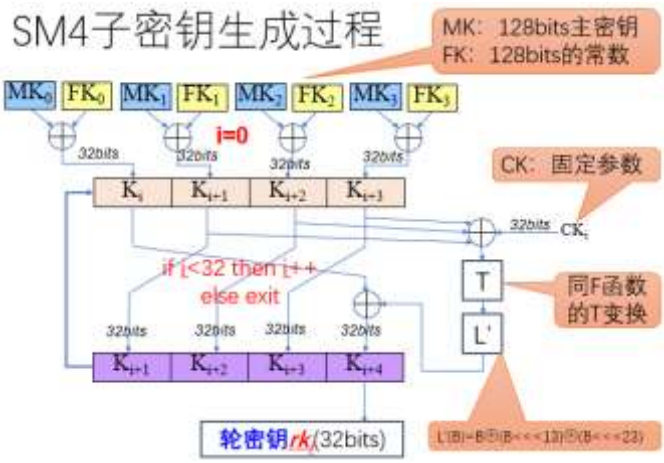
先将 128bit 主密钥MK分为四组(MK_0, MK_1, MK_2, MK_3)，每组长度 32bit，分别计算$MK_i \oplus FK_i, i = 1,2,3,4$,其中$FK_i, i = 0,1,2,3$为系统固定参数，得到$(K_0, K_1, K_2, K_3)$。则轮密钥$rk_0 = K_4 = F'(K_1, K_2, K_3, CK_1)$，$rk_1 = K_5, rk_2 = K_6$ …，以此类推，共迭代 32 轮。其中F'的步骤如下:

1) 计算$K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i$，其中$CK_i$为系统固定参数，输出 32bit 结果;

2) 将步骤 1）输出的 32bit 结果分为 4 组 8bit 数据带入 s 盒进行非线性变换（T 变换），再将变换结果重新组合为 32bit 数据作为输出B，该过程和F函数的T变换过程相同;

3) 将B分别左移 13、23 位进行线性变换，计算$L'(B) = B \oplus (B \ll 13) \oplus (B \ll 23)$;

4) 计算$rk_i = K_{i+4} = K_i \oplus L'(B)$。



4.描述 SM4 算法的解密过程。

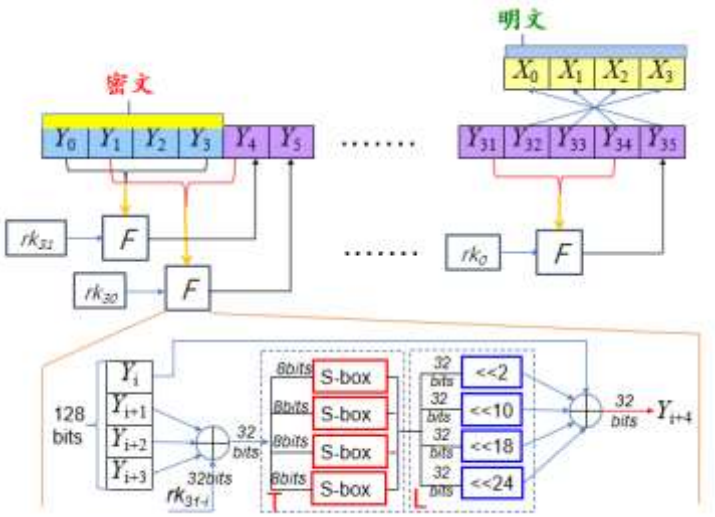
答：SM4 密码算法是对合运算，因此解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

设输入密文为$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32})$，输入轮

密钥为rk_{31-i}，$i = 0,1,\ldots,30,31$，输出明文为(X_0, X_1, X_2, X_3)。则解密算法可描述如下：

$$Y_{i+4} = F(Y_i, Y_{i+1}, Y_{i+2}, Y_{i+3}, rk_{31-i})$$
$$= Y_i \oplus L(T(Y_{i+1} \oplus Y_{i+2} \oplus X_{i+3} \oplus rk_{31-i}))，\text{其中} i = 0,1,\ldots,30,31$$

明文$(X_0, X_1, X_2, X_3) = R(Y_{32}, Y_{33}, Y_{34}, Y_{35}) = (Y_{35}, Y_{34}, Y_{33}, Y_{32})$



5.请描述 SM4 算法与 DES 算法、AES 算法的相似之处。

答：

1) SM4 算法与 DES 算法、AES 算法所采用的设计原理相同，即扩散和混淆；

2) SM4 使用类似 DES 的 Feistel 的结构，每轮 DES 处理 1/2 分组，SM4 处理 1/4 分组；

3) SM4 加解密算法同 DES 是可复用的，即加密算法也可用于解密算法；

4) SM4 的非线性代换部分类似 AES 的字节代换；

5) SM4 的线性变换 L 中的移位类似 AES 的行移位；

6) SM4 的子密钥生成部分类似 AES 的子密钥生成部分，递归迭代并含有非线性部分；

7) DES 密钥位数 56bit，AES 为 128、192 或 256bit，SM4 为 128bit。密钥较长

意味着安全性较高，但会降低加、解密速度。这种安全性的增加来自更好的抗穷尽攻击能力和更好的混淆性；

8) AES 和 SM4 的分组长度都为 128bit，分组长度越长意味着安全性越高，但是会降低加、解密的速度。这种安全性的增加来自更好的扩散性。