应用密码学第二次作业

姓名：何小溪 学号：1901210398

sm4可逆性的证明

1、sm4的加密过程

加密算法由32次迭代运算和1次反序变换R组成，设明文输入为$(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$,密文的输出为$(Y_0,Y_1,Y_2,Y_3)\in(Z_2^{32})^4$,轮密钥为$rk_i\in Z_2^{32},i=0,1,\cdots,31$。

（1）32次迭代运算：

$$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i),i=0,1,\cdots,31$$

（2）反序变换：

$$(Y_0,Y_1,Y_2,Y_3)=R(X_{32},X_{33},X_{34},X_{35})=(X_{35},X_{34},X_{33},X_{32})$$

2、轮函数结构

设输入为$(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$，轮密钥为$rk_i\in Z_2^{32},i=0,1,\cdots,31$，则轮函数$F$为：

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

3、证明

第一步：轮密钥的顺序为$(rk_0,\cdots,rk_{31})$,第i轮加密为：

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

产生密文的顺序为：$(X_0,X_1,\cdots,X_{34},X_{35})$，然后经过一次反转后。最后所得密文为：$(X_{35},X_{34},X_{33},X_{32})$。解密密文的顺序与产生密文的顺序相反，为$(X_{35},X_{34},\cdots,X_1,X_0)$。

第二步：解密的过程与加密流程一致，但轮密钥的顺序与加密相反，为$(rk_{31},\cdots,rk_0)$。则第

$31-i$轮解密为：

$$
\begin{aligned}
X_i &= X_{i+4} \bigoplus T(X_{i+3} \bigoplus X_{i+2} \bigoplus X_{i+1} \bigoplus rk_{31-(31-i)}) \\
&= X_i \bigoplus T(X_{i+1} \bigoplus X_{i+2} \bigoplus X_{i+3} \bigoplus rk_i) \bigoplus T(X_{i+3} \bigoplus X_{i+2} \bigoplus X_{i+1} \bigoplus rk_i) \\
&= X_i \bigoplus 0 \\
&= X_i
\end{aligned}
$$

综上，可得sm4的加密过程是可逆的。