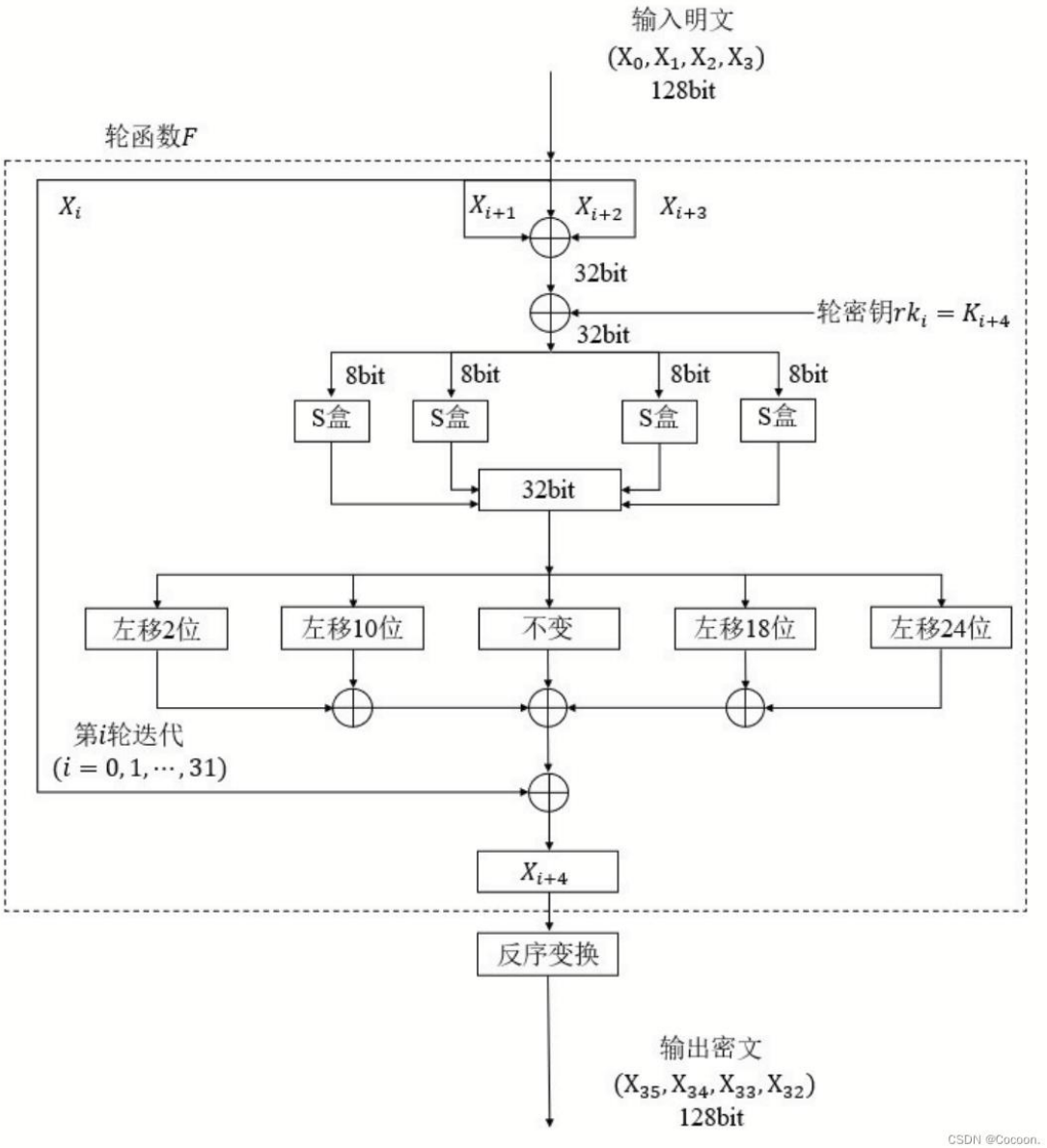
*Project9: AES / SM4 software implementation

SM4 的代码说明:

流程图:



线性变化：主要是移位运算和异或运算，输入输出都为 32 位。例如 B 为 32 位，则运算为 B⊕(B<<<2) ⊕(B<<<10) ⊕(B<<<18) ⊕(B<<<24)

密钥扩展算法：输入 128 位的密钥，进行 32 轮迭代，每一轮产生一个 32 位的轮密钥，共产生 32 个轮密钥。先进行(k0,k1,k2,k3)=(mk0⊕fk0,mk1⊕fk1,mk2⊕fk2, mk3⊕fk3),然后进行 32 轮迭代，每一轮为 rki=ki+4=ki⊕t'(ki+1⊕ki+2⊕ki+3⊕cki)，其中 rki 为 i 轮的密钥，cki 与 fki 都为常数，t'运算为先进行 s 盒代换，然后进行线性变化，只不过这里的线性变化为 B⊕(B<<<13) ⊕(B<<<23)。

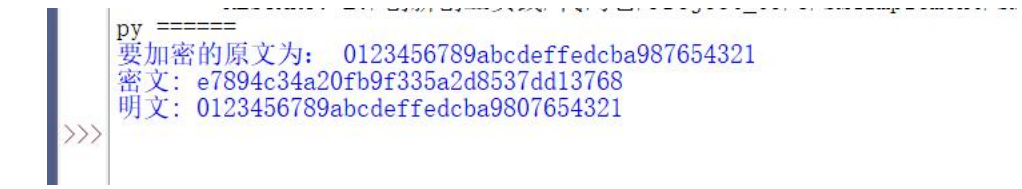
加密算法：输入为 128 位，即 4 个 32 位的字，输出也为 128 位。共有 32 轮迭代，每一轮使用一个 32 位的轮密钥。每一轮的运算为 x0⊕t(x1⊕x2⊕x3⊕rk)。之后将得到的 x35,x34,x33,x32 再进行一个反序处理，作为密文。

其中 rk 为该轮轮密钥，x0,x1,x2,x3 为 4 个 32 位的字，t 运算包含 s 盒代换和线性变换，即每一轮的运算为 x0⊕[s(B)] ⊕[s(B)<<<2] ⊕[s(B)<<<10] ⊕[s(B)<<<18] ⊕ [s(B)<<<24] ,B 为 x1⊕x2⊕x3⊕rk

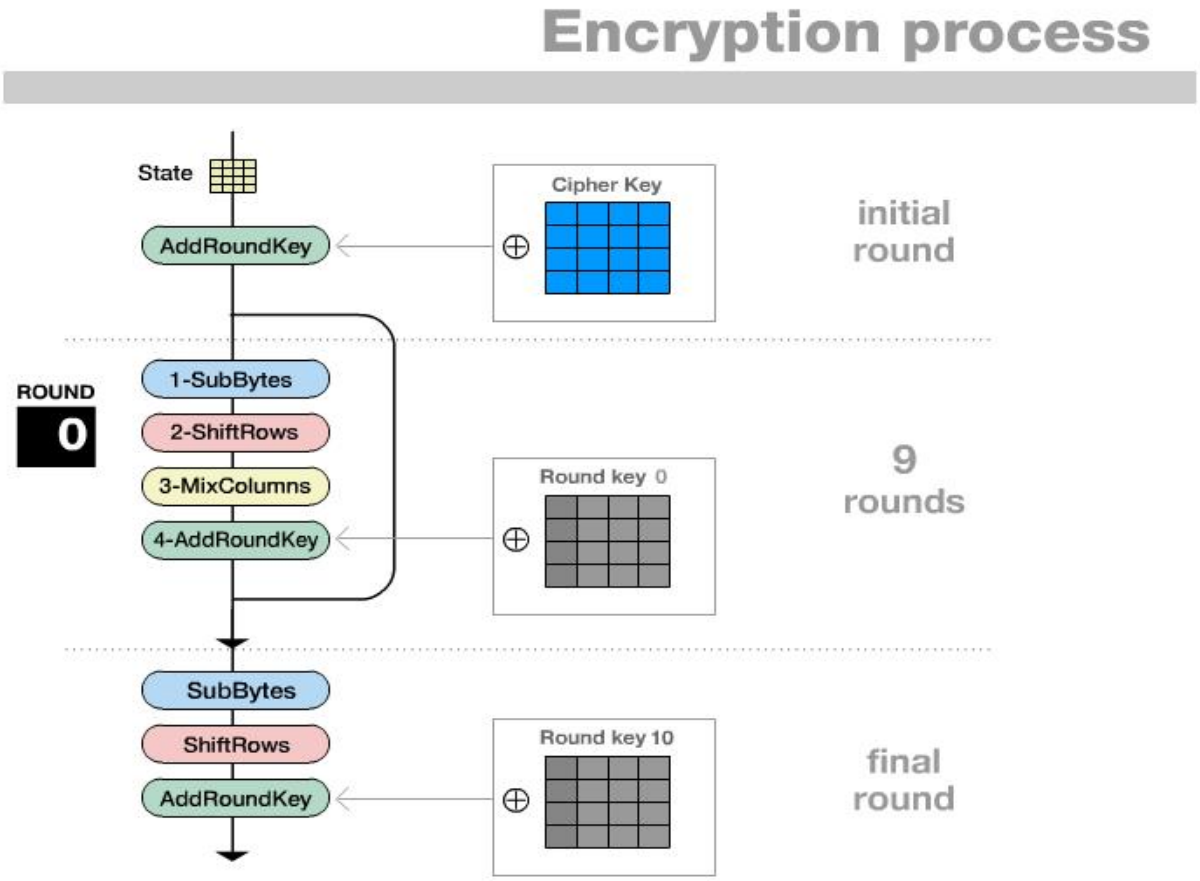
解密算法：与加密算法相同,只是轮密钥的使用顺序相反。

实现方式：python

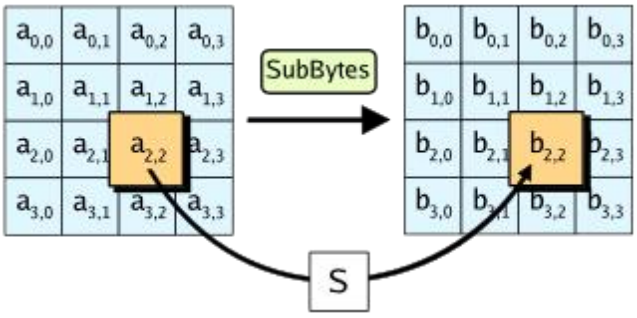
运行结果：



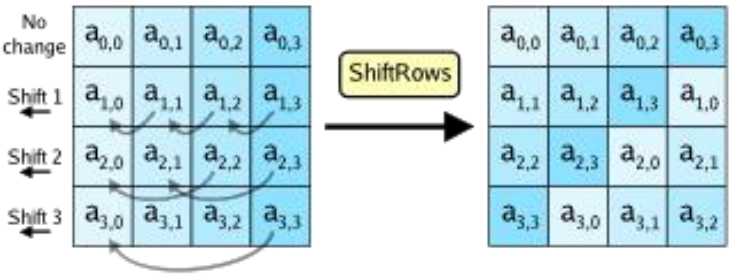
AES:


Encryption process
State
AddRoundKey
Cipher Key
initial round
ROUND
0
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey
Round key 0
9 rounds
SubBytes
ShiftRows
AddRoundKey
Round key 10
final round

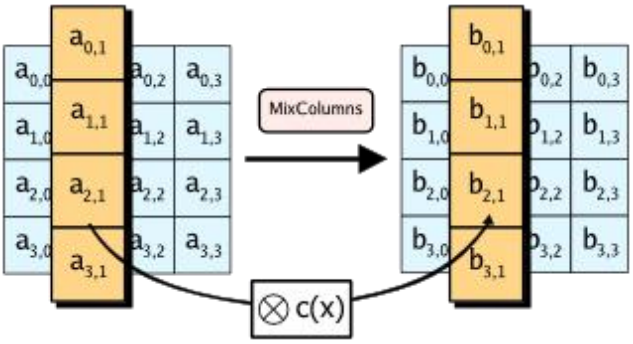
S 盒:


SubBytes
S

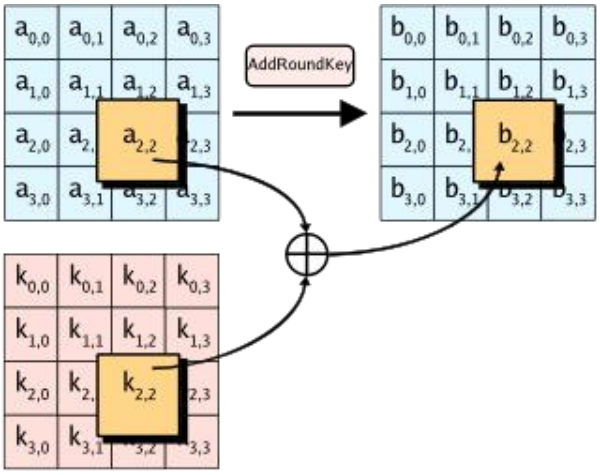
行移位:


No change
Shift 1
Shift 2
Shift 3
ShiftRows

列混合:



轮密钥异或:



结果:

```
所要加密的明文(编码后)为:
32 30 32 31
30 30 31 35
30 30 38 34
0 0 0 0
所要加密的密钥(编码后)为:
32 30 32 31
30 30 31 35
30 30 38 34
0 0 0 0

加密结果为:
61 dd f7 20
32 18 9f bf
b5 a7 ac 50
7e 99 56 ea
```

分工: 自己独立完成