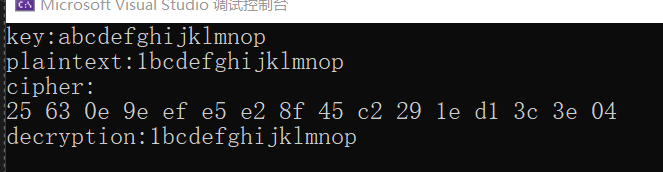
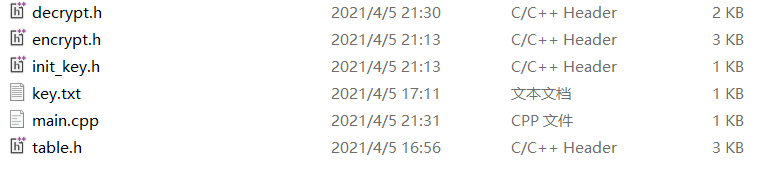
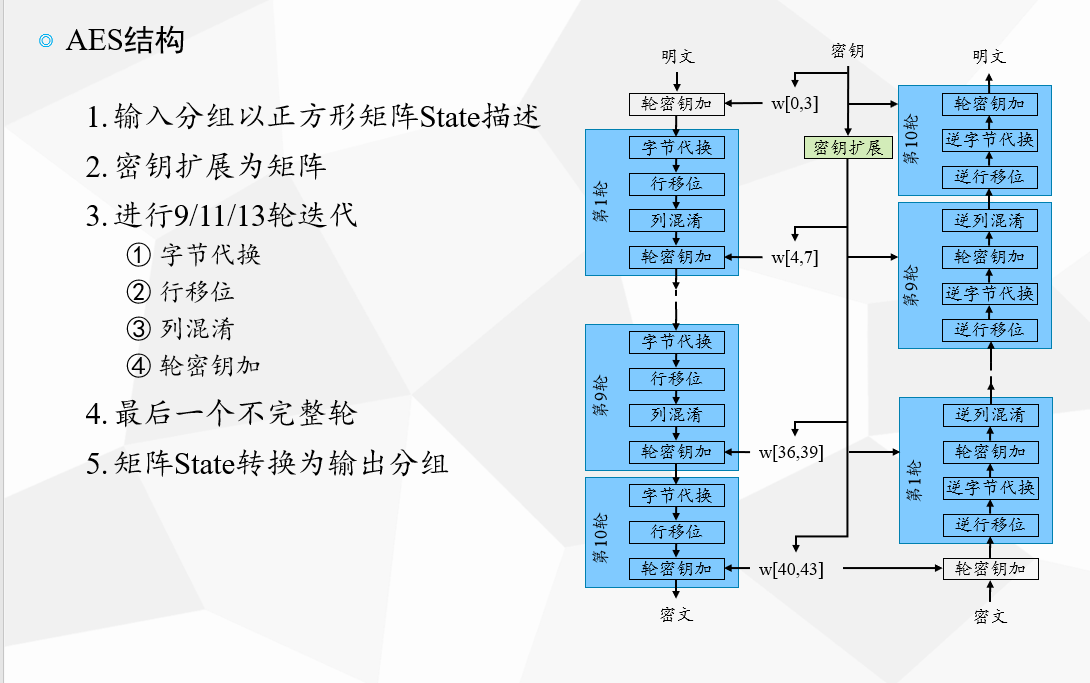
本代码实现了AES算法经行加密、解密，先上效果图：

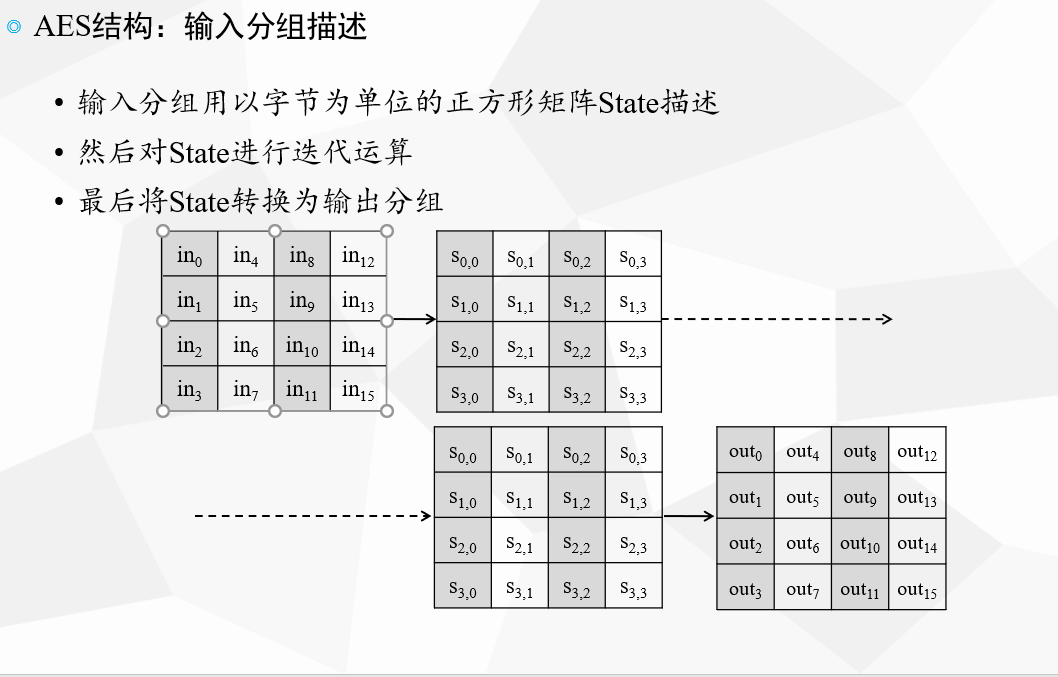


本程序源代码由以下几个文件组成，decrypt.h实现了AES算法的加密功能，encrypt.h实现了AES中的解密部分，init\_key.h实现了密钥矩阵的初始化，key.txt保存了密钥，main.cpp为程序的主部分，table.h存放了AES算法所使用到的一些常数矩阵。

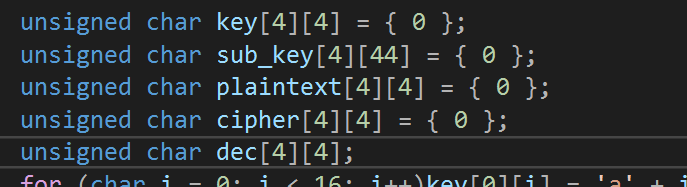


AES算法数据结构：

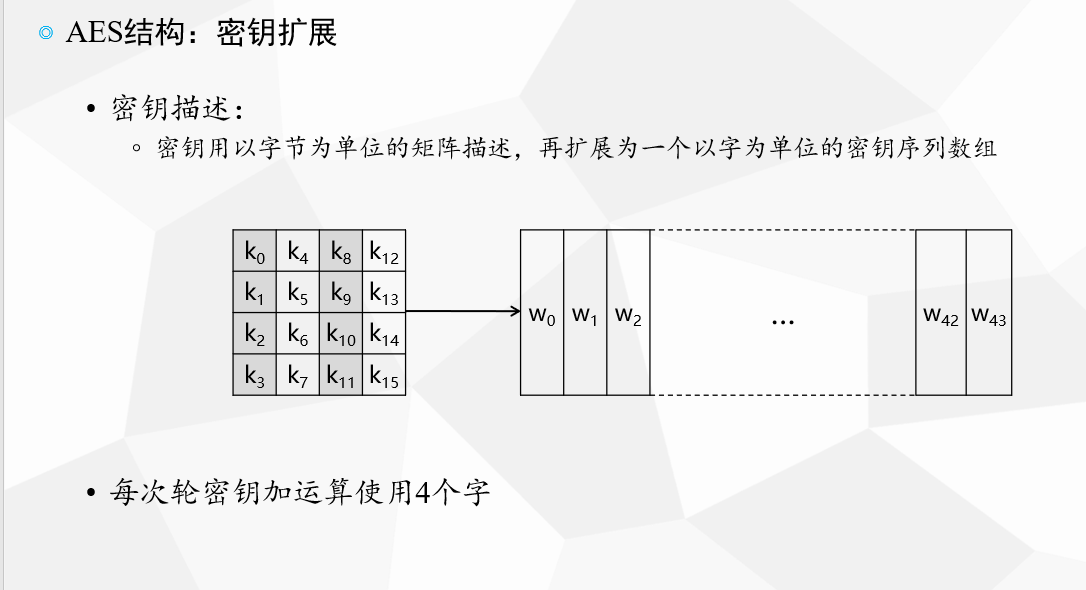


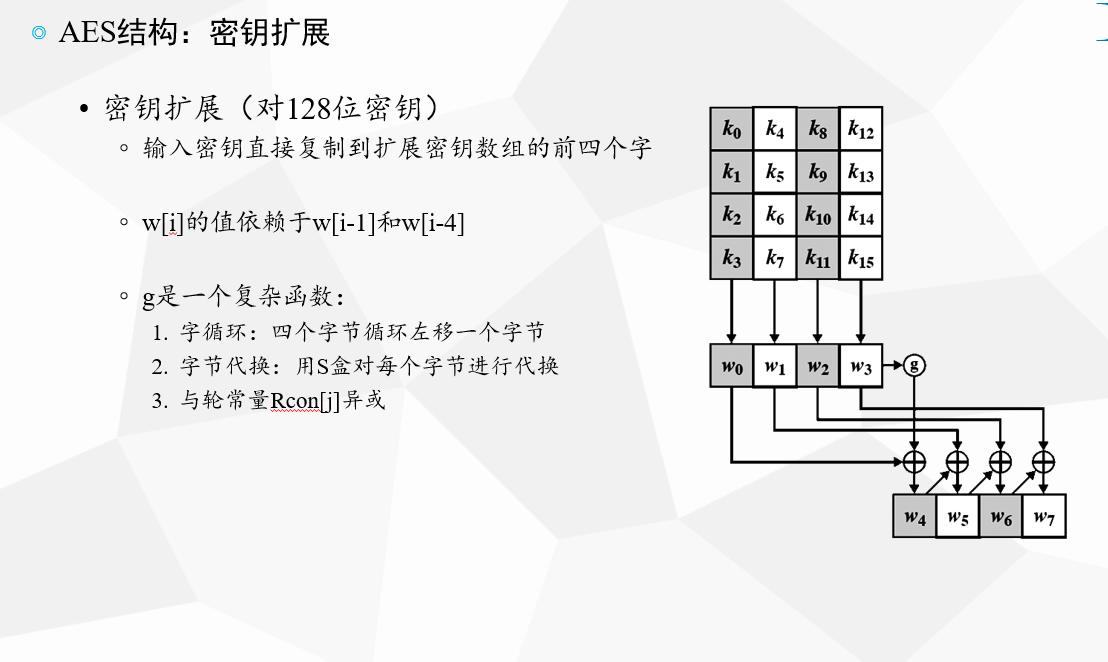


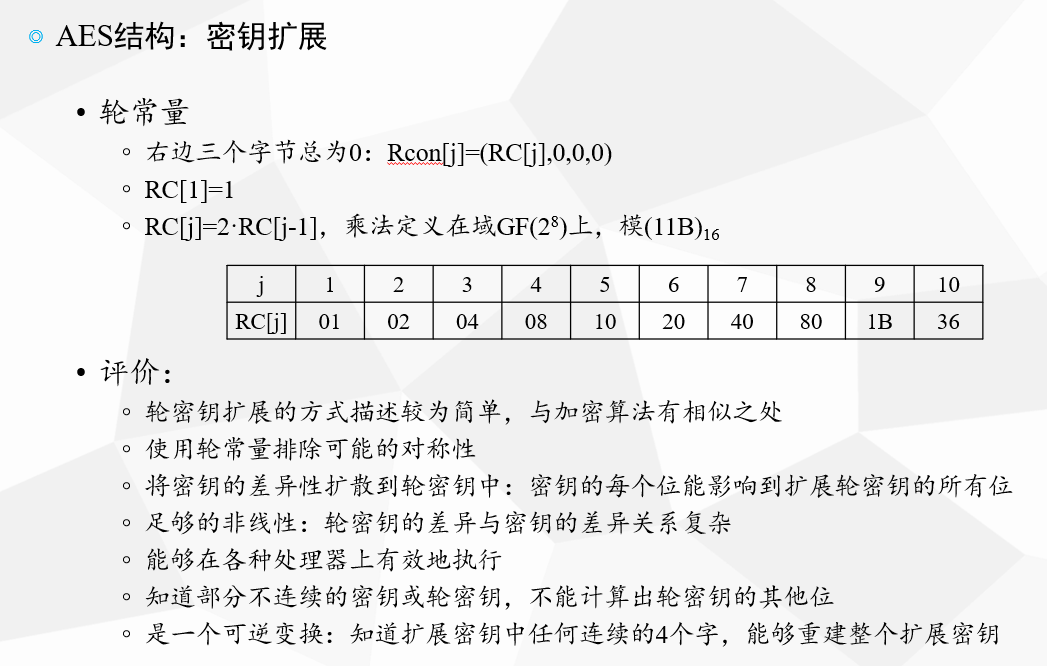
本程序里的明文分组、密钥分组、密文分组均以4\*4矩阵表示，以一个字节为单位。



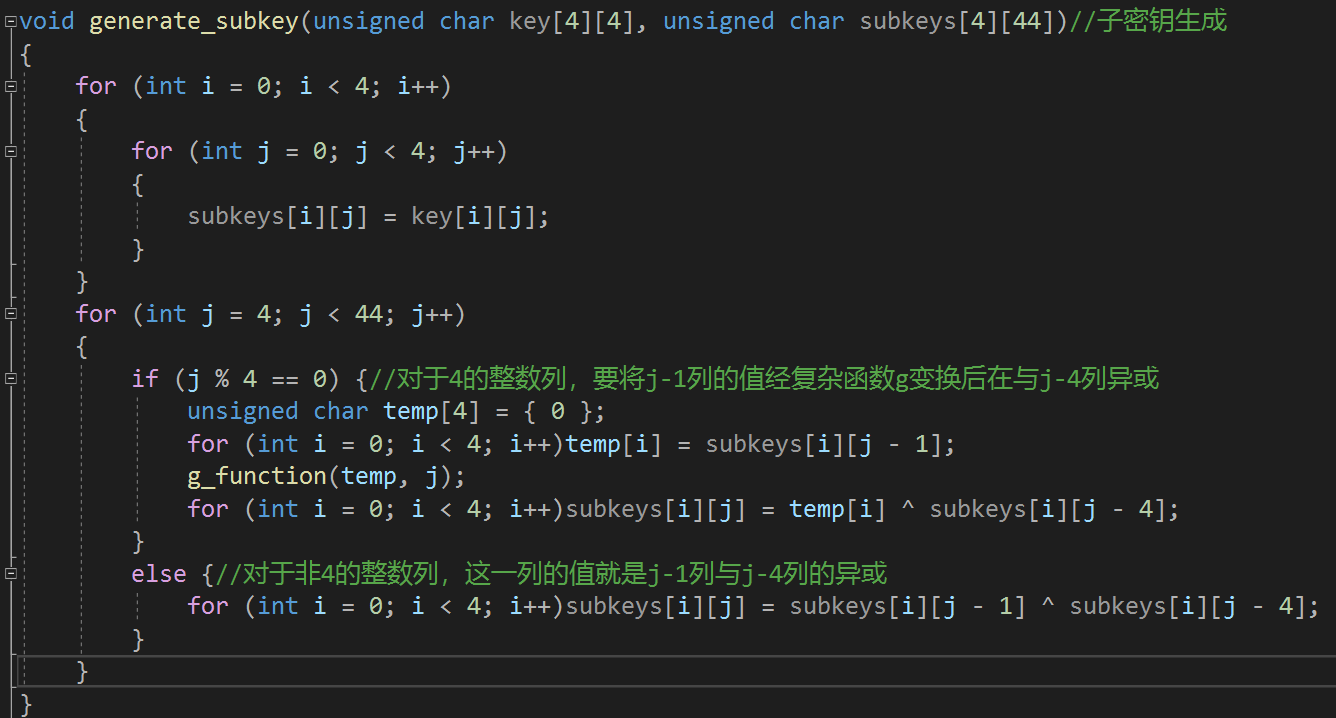
AES算法子密钥生成：





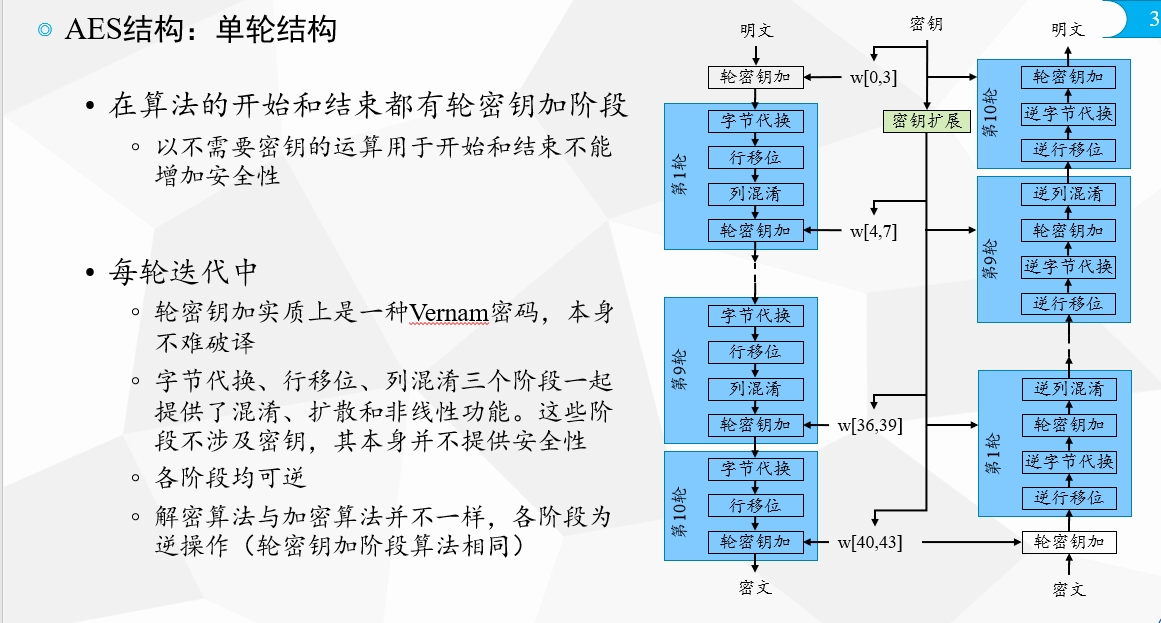


代码实现：



AES的具体结构：

以下代码在encrypt.h文件中得到了实现



void encrypt(unsigned char plaintext[4][4], unsigned char subkeys[4][44], unsigned char cipher[4][4])

{

for (int i = 0; i < 4; i++)

{

for (int j = 0; j < 4; j++)

{

cipher[i][j] = plaintext[i][j];

}

}

Add\_subkey(cipher, subkeys, 0);

for (int i = 1; i <= 9; i++)

{

changebytes(cipher);

shiftrows(cipher);

mixColumn(cipher);

Add\_subkey(cipher, subkeys, i);

}

changebytes(cipher);

shiftrows(cipher);

Add\_subkey(cipher, subkeys, 10);

}

Add\_subkey(cipher, subkeys, 0);实现明文密钥相加

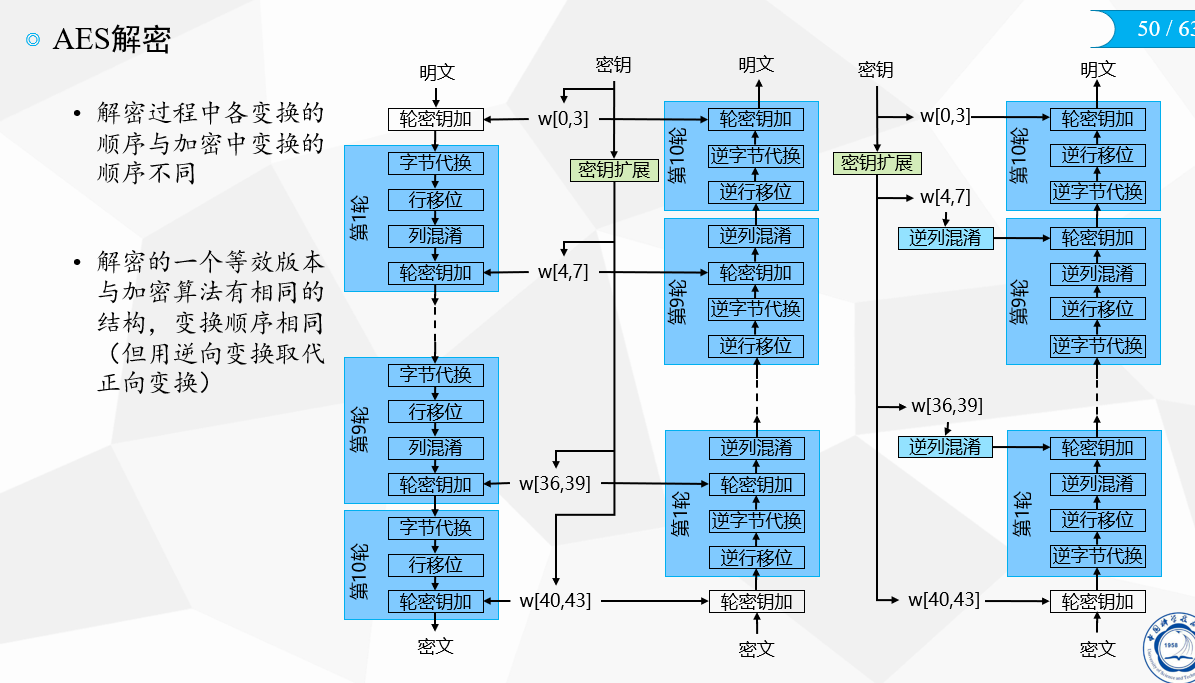
changebytes(cipher);实现字节代换（sbox代换）

shiftrows(cipher);mixColumn(cipher);实现行移位和列混淆

Add\_subkey(cipher, subkeys, i);在进行一次密钥相加

这样经行9轮后，最后在进行第十轮不需要轮密钥相加

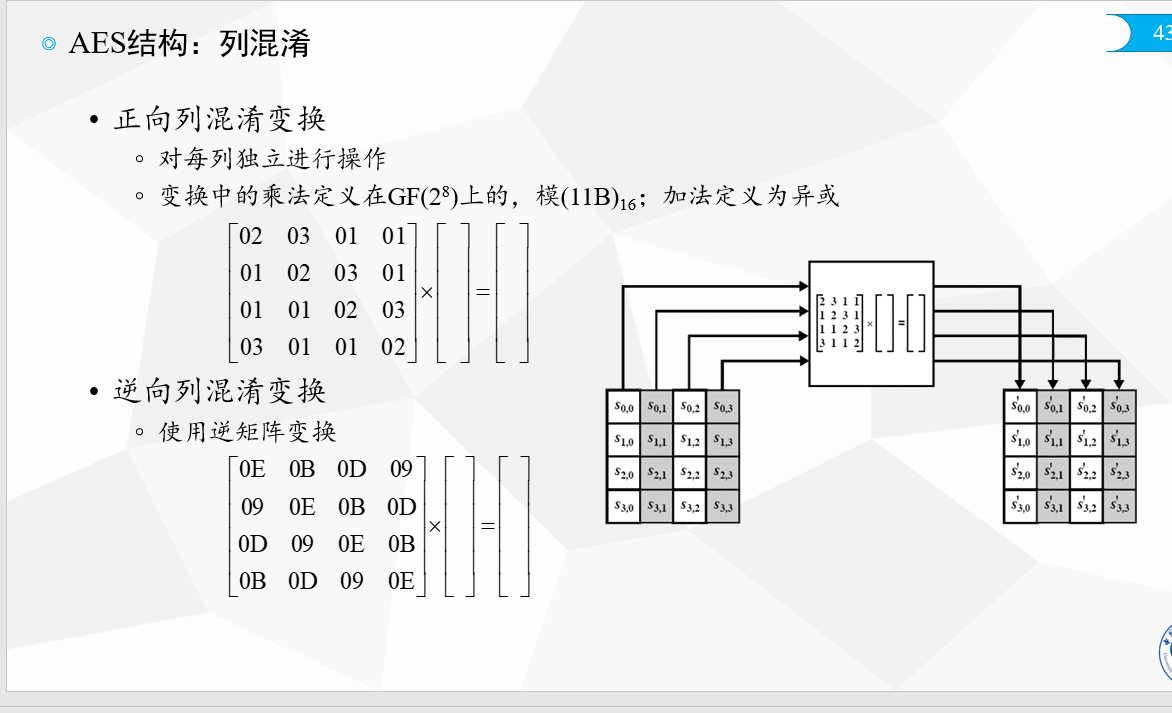
AES解密：



AES解密与加密算法有很多相同的部分，解密在decrypt.h中实现，只需要将很多变换改成加密的逆变换就可以进行解密了

一些算法的具体实现细节：

列混淆：



列混淆使用了GF(2^8)上运算，x2time（y）表示在GF(2^8)上将y与2相乘，这一部分实际上也可以用打表的方法来替代，会更加简单高效，但是我还是直接使用函数来求解了。

