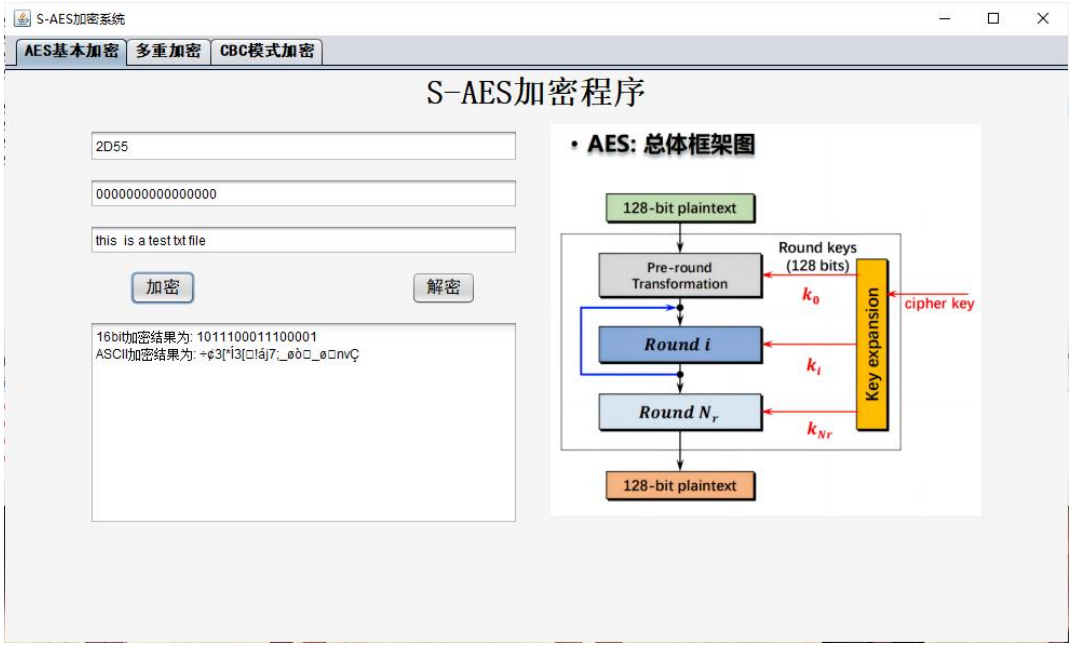
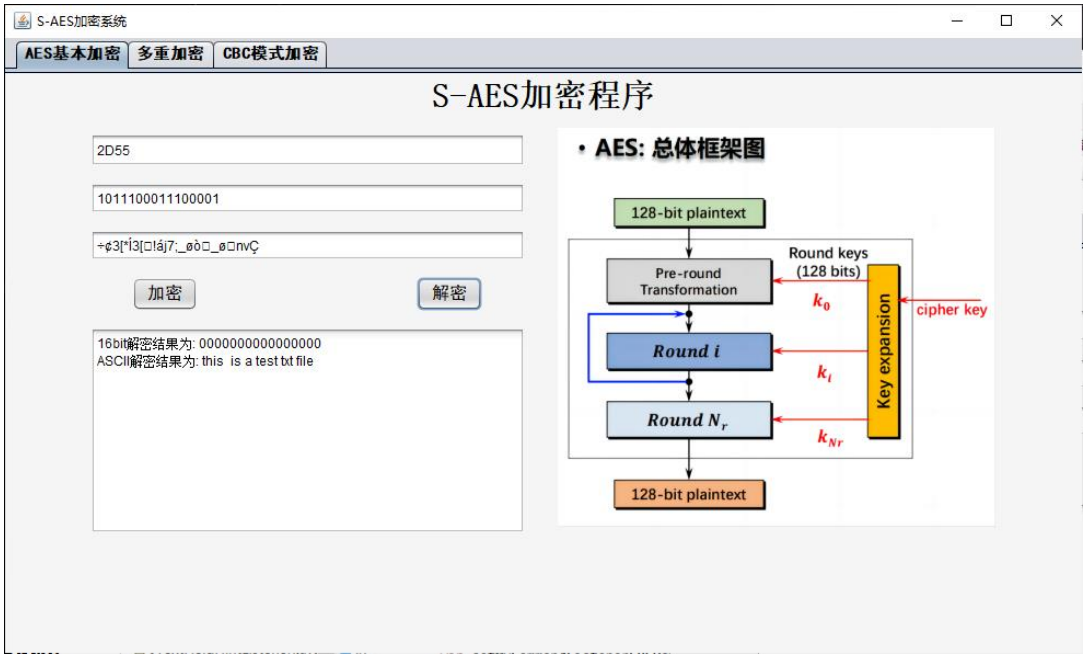
测试结果

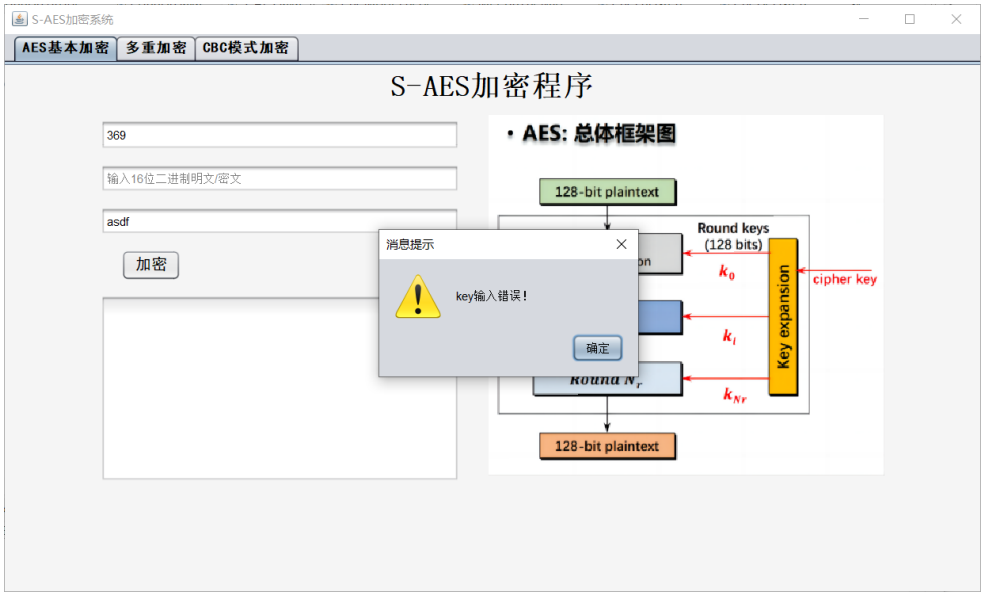
3.1 与 3.3

根据 S-AES 算法编写和调试程序，提供 GUI 解密支持用户交互。输入可以是 16bit 的数据和 16bit 的密钥，输出是 16bit 的密文。考虑到向实用性扩展，加密算法的数据输入可以是 ASII 编码字符串(分组为 2 Bytes)，对应地输出也可以是 ACII 字符串(很可能是乱码)。以下为加密解密结果：





输入错误时会给出相应提示：



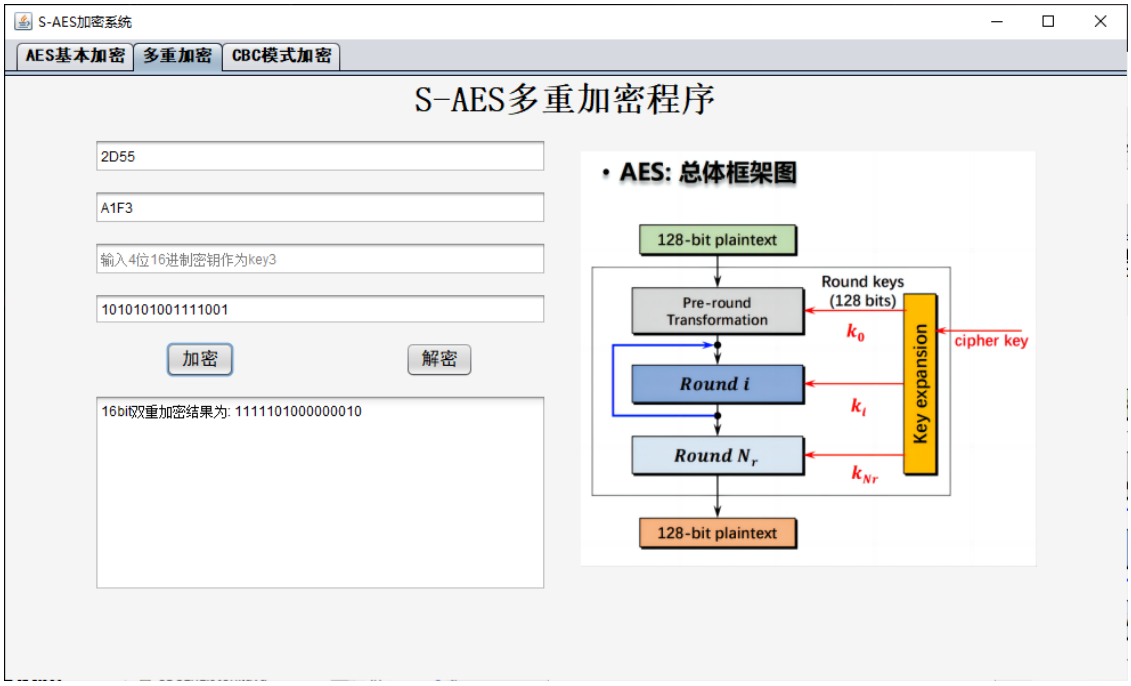
3.2

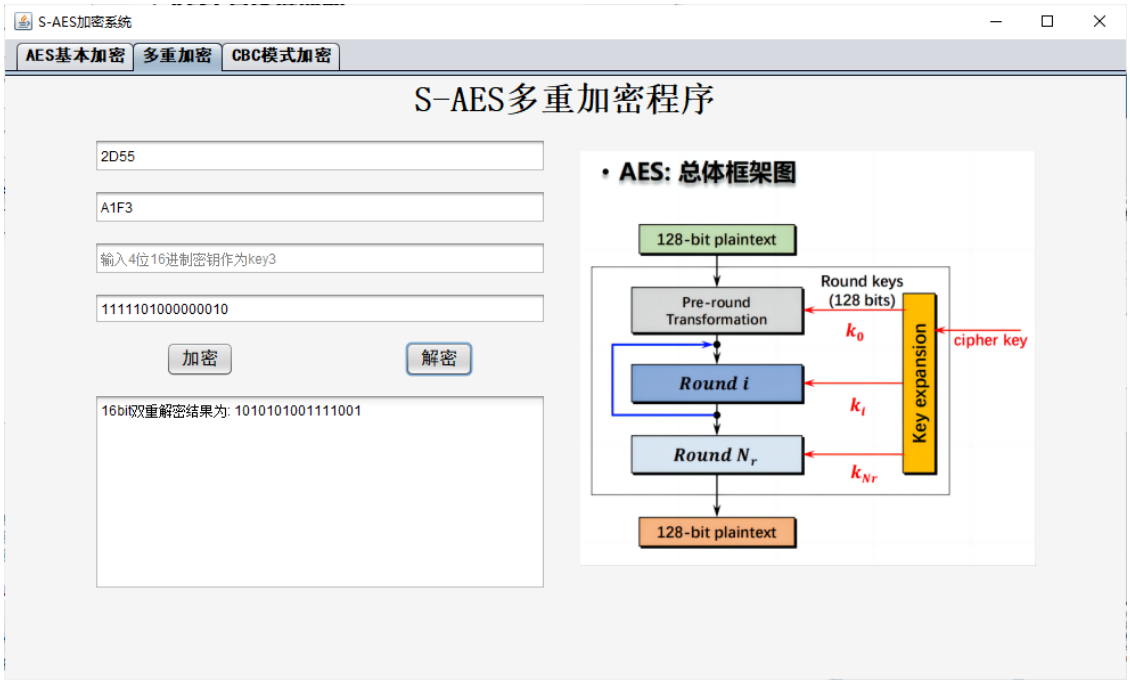
已与熊孝宇、蒋中豪、方珩、朱清扬、韩晓璐组进行了测试，检验通过

3.4.1 与 3.4.3

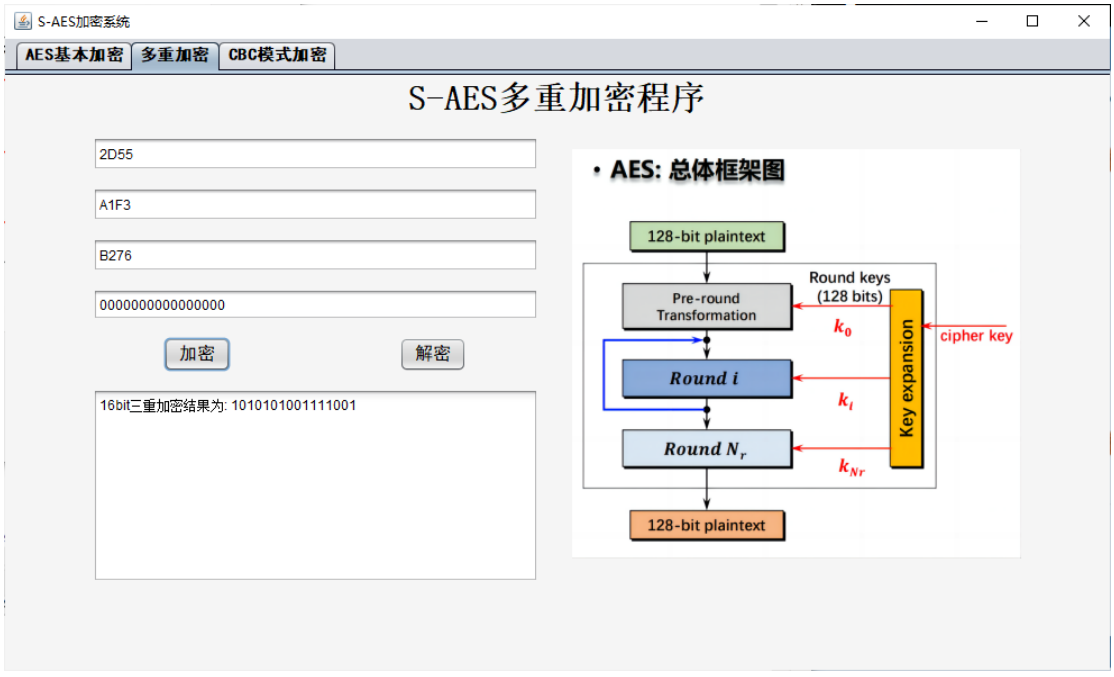
将 S-AES 算法通过双重加密进行扩展，分组长度仍然是 16 bits，但密钥长度为 32bits，将 S-AES 算法通过三重加密进行扩展。

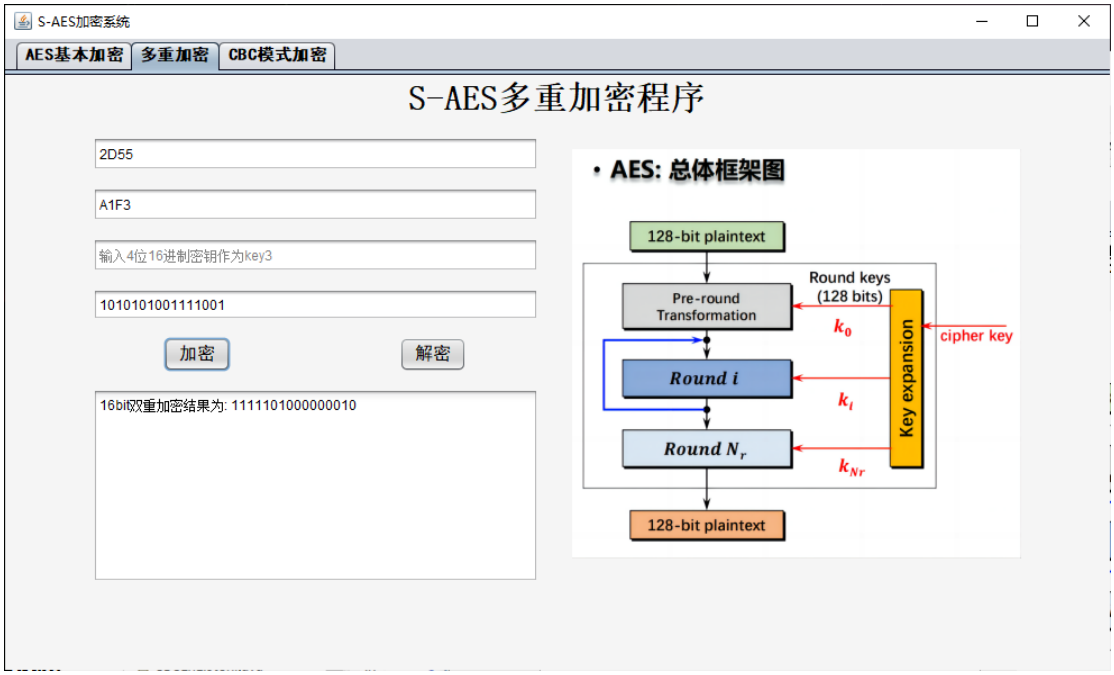
双重加密与解密：




S-AES加密系统
AES基本加密
多重加密
CBC模式加密
S-AES多重加密程序
2D55
A1F3
输入4位16进制密钥作为key3
1111101000000010
加密
解密
16bit双重解密结果为: 1010101001111001
• AES: 总体框架图
128-bit plaintext
Round keys
(128 bits)
Pre-round
Transformation
k_0
cipher key
Round i
k_i
Key expansion
Round N_r
k_{Nr}
128-bit plaintext

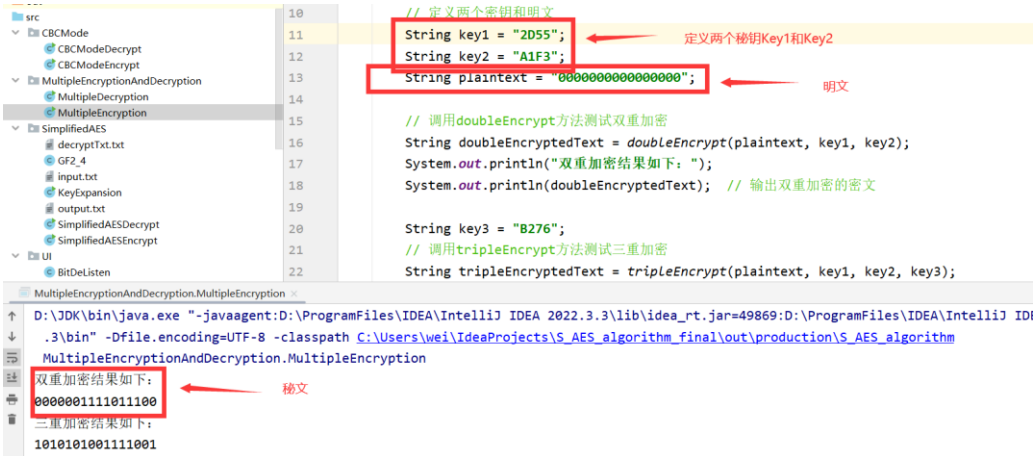
三重加密与解密：

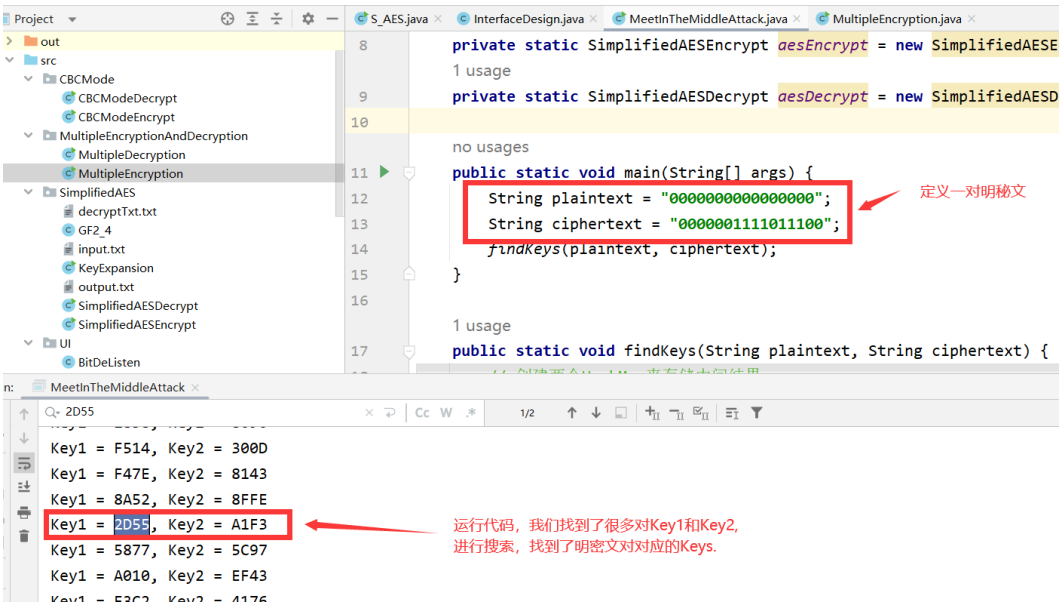

S-AES加密系统
AES基本加密
多重加密
CBC模式加密
S-AES多重加密程序
2D55
A1F3
B276
0000000000000000
加密
解密
16bit三重加密结果为: 1010101001111001
• AES: 总体框架图
128-bit plaintext
Round keys
(128 bits)
Pre-round
Transformation
k_0
cipher key
Round i
k_i
Key expansion
Round N_r
k_{Nr}
128-bit plaintext



3.4.2

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥 Key(K1+K2)。

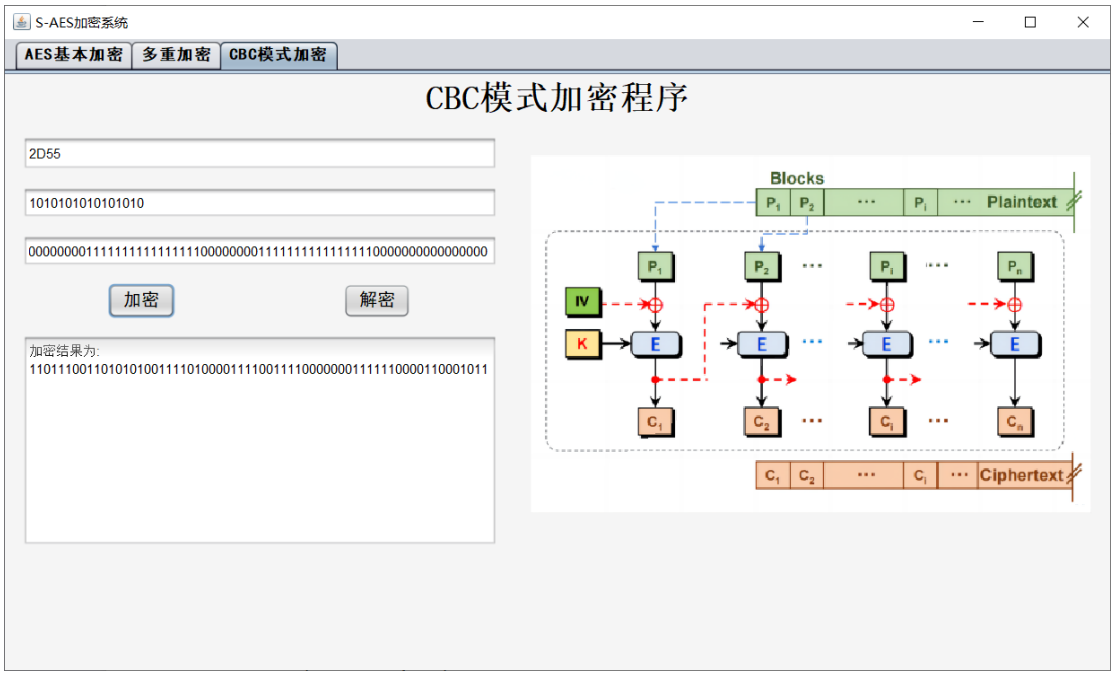


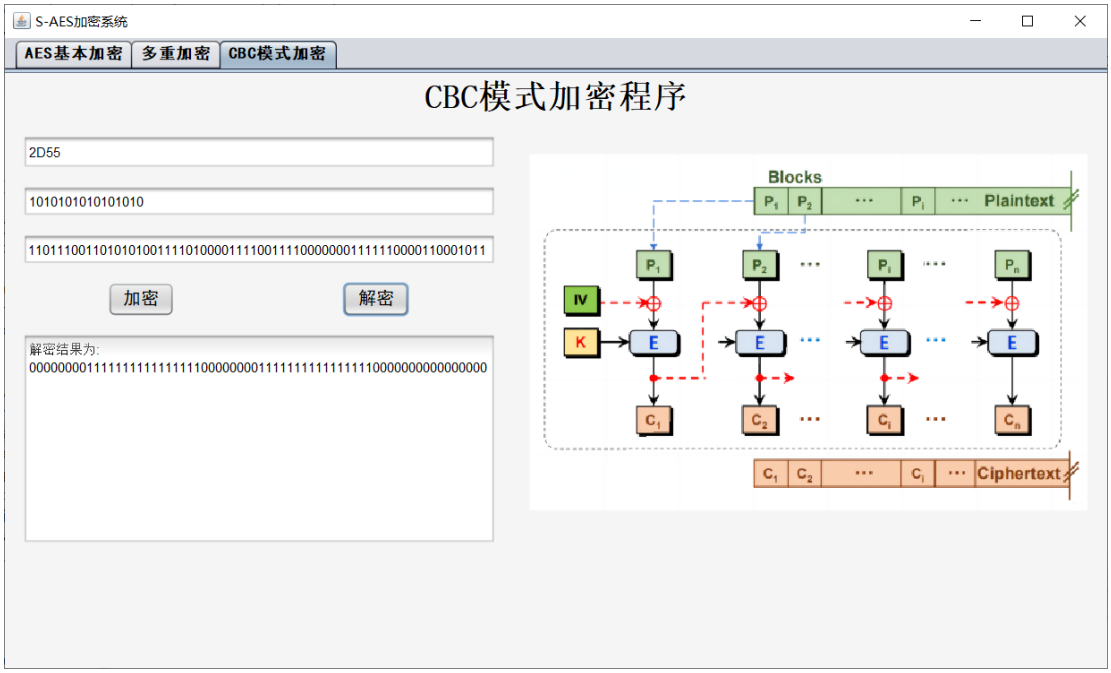


3. 5

在 CBC 模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密，请对比篡改密文前后的解密结果。

基本加密与解密：





替换分组后的加密，可以看见在 CBC 模式下修改明文后，密文只有在原明文修改后的部分有所改变，未修改部分仍相同：

1101110011010101001111010000111 1 00111100000001111111000011000101 1

1101110011010101001111010000111 1 10111100000011001111000110000100