通关情况测试

3.1 第1关：基本测试

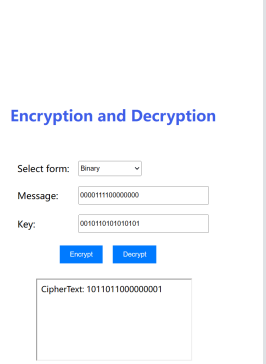
在"加解密"标签页中,可以进行以下操作:

- 输入16进制的明文和密钥,点击"加密"按钮进行加密,点击"解密"按钮进行解

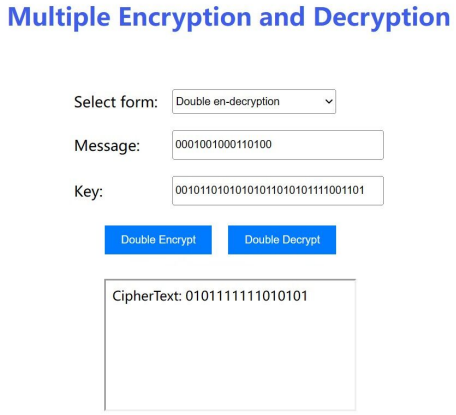
加密	解密
	

3.2 第2关：交叉测试

基本加密:

我们组	其他组
	
密钥：2d55 明文：0f00 密文：b601	密钥：0010110101010101 明文：0000111100000000 密文：1011011000000001

双重加密:

我们组	其他组
	
密钥：2d55abcd 明文：1234 密文：5fd5	密钥： 00101101010101011010101111001101 明文：0001001000110100 密文：0101111111010101

三重加密：

我们组	其他组
	
密钥：B39ADECDBA27 明文：D72C 密文：1911	密钥： 101100111001101011011110110011011011101000100111 明文：1101011100101100 密文：0001100100010001

3.3 第3关：扩展功能

- 选择"ASCII"选项,可以输入任意长度的ASCII字符串进行加密和解密

ASCII加密	解密
	

3.4 第4关：多重加密

3.4.1 双重加密

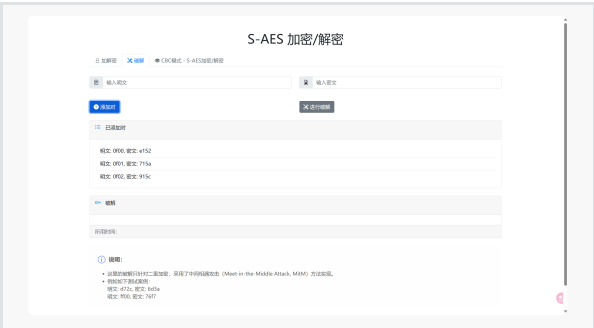
- 选择"双重加密",可以输入16进制明文和32位十六进制密钥,进行双重加密和解密

双重加密	解密
	

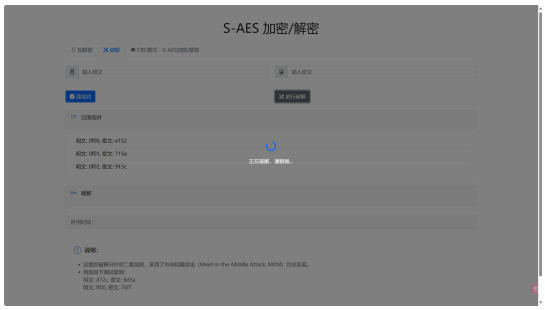
3.4.2 中间相遇攻击

在“破解”标签页中,可以进行中间相遇攻击,步骤如下:

- 输入明文和密文组成一对,点击"添加对"按钮
- 重复上述步骤,添加多个明密文对



- 点击“进行破解”按钮,会显示破解得到的密钥 `K1` 和 `K2` ,以及破解耗时

等待破解	成功破解
	

3.4.3 三重加密

使用48bits(K1+K2+K3)的模式进行三重加解密

- 选择“三重加密”,可以输入16进制明文和48位十六进制密钥,进行三重加密和解密

三重加密	解密
	

3.5 第5关：工作模式

在“CBC模式”标签页中,可以进行CBC模式的加解密:

- 输入16进制密钥和初始向量`IV`
- 在长明文输入框中输入要加密的明文
- 点击“CBC加密”按钮进行加密,结果会显示在结果区域

- 可以点击展开按钮,添加或者修改密文

- 点击“CBC解密”按钮进行解密,查看修改前后解密结果的比较

篡改前	进行篡改测试
	

讨论:

Key Used for Encryption: `0x1234`
Initialization Vector (IV): `0x5678`

Tampering	Original Ciphertext	Tampered Ciphertext	Decrypted Tampered Ciphertext
None	0xf2cf10e25b8dfd0a	N/A	0x9abc9abcdef01234
4 bits	0xf2cf10e25b8dfd0a	0x02cf10e25b8dfd0a	0x6abe6abcdef01234
8 bits	0xf2cf10e25b8dfd0a	0x0dcf10e25b8dfd0a	0x675e65bcdef01234
12 bits	0xf2cf10e25b8dfd0a	0x0d3f10e25b8dfd0a	0x6d7e654cdef01234
16 bits	0xf2cf10e25b8dfd0a	0x0d3010e25b8dfd0a	0x4d716543def01234
32 bits	0xf2cf10e25b8dfd0a	0x0d30ef1d5b8dfd0a	0x4d719659210f1234

分析如下:

1. **错误传播特性**:从结果中,我们可以看到CBC模式的一个显著特点,即一个加密块的篡改会影响到解密的该块和下一个块。这称为错误传播特性。比如当我们篡改第一个块时,解密的第一个块和第二块都受到了影响。
2. **一致性的缺失**:尽管错误传播到后续块,但篡改加密的块并不能以有意义的方式影响解密的块。换句话说,一个小小的篡改(例如4比特)可能会导致完全不同的解密输出,而不是仅仅4比特的差异。这也是为什么篡改加密消息是危险的,因为它会导致完全不可预测的输出。
3. **影响的持续性**:当我们篡改32位时,尽管第一个块和第二块都受到了影响,但从第三块开始,解密的输出与原始明文相同。这证明了CBC模式中错误传播的“有限”特性,即一个错误只会影响其本身和下一个块。
4. **安全性与篡改检测**:CBC模式本身并不提供明文的完整性或篡改检测。从结果中,我们可以看到,即使对加密文本进行了小小的篡改,也可能不容易被接收者察觉,除非他们期望的解密输出与实际的解密输出存在显著差异。
5. **篡改与噪声**:篡改在真实世界中可能被视为噪声或数据损坏。CBC模式对于随机噪声具有某种“弹性”,因为噪声只影响两个块,而不是整个消息。

总之,CBC模式提供了一种方式,使篡改的加密消息在解密时产生不可预测的输出,并且篡改会传播到后续的块,但其影响是有限的。为了提高安全性,应该考虑使用其他机制来确保数据的完整性和篡改检测。