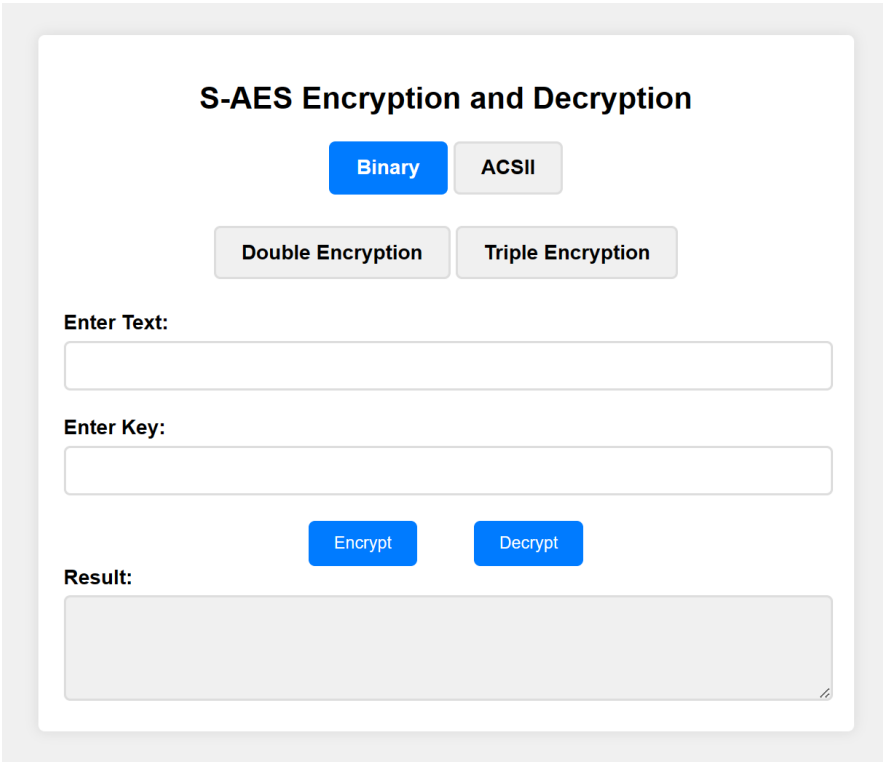


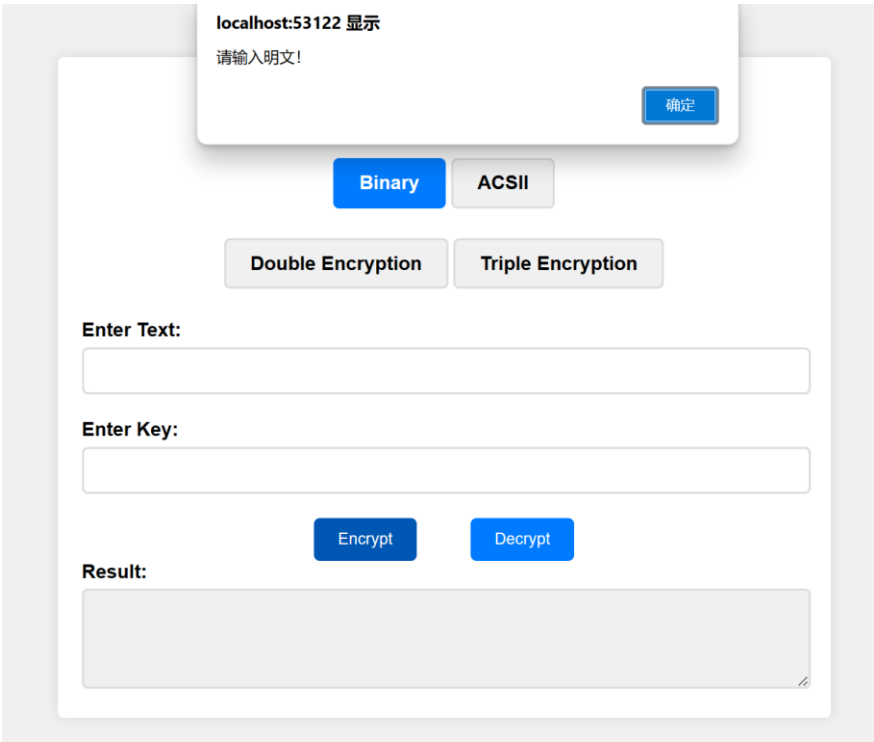
第一关 基本测试

界面设计



图一 用户界面

当 text 为空时，提示“请输入明文！”或“请输入密文！”



图二 提示输入明文

当选择 Binary、Double Encryption 或者 Triple Encryption 后，输入的 text 不是二进制数时，提示“请输入二进制数据！”

请输入二进制数据!

确定

Binary ASCII

Double Encryption Triple Encryption

Enter Text:

abc

Enter Key:

1010101010101010

Encrypt Decrypt

Result:

图三 提示输入二进制数

当选择 Binary 或者 ASCII 时输入的密钥长度不是 16bit 位，则提示“密钥应为 16bit 位！”

密钥应为16位二进制位!

确定

Binary ASCII

Double Encryption Triple Encryption

Enter Text:

1010101010101010

Enter Key:

11110000

Encrypt Decrypt

Result:

图四 提示密钥为 16bit 位

测试明文: 0110111101101011

密钥: 1010011100111011

生成密文: 0000011100111000

The screenshot shows the 'S-AES Encryption and Decryption' web application. At the top, there are two tabs: 'Binary' (selected) and 'ASCII'. Below these are two buttons: 'Double Encryption' and 'Triple Encryption'. The 'Enter Text:' field contains the binary string '0110111101101011'. The 'Enter Key:' field contains the binary string '1010011100111011'. Below the input fields are two buttons: 'Encrypt' and 'Decrypt'. The 'Result:' section shows the output: '密文为: 0000011100111000'.

图五 加密成功

测试密文: 0000011100111000

密钥: 1010011100111011

生成明文: 0110111101101011

The screenshot shows the 'S-AES Encryption and Decryption' web application. At the top, there are two tabs: 'Binary' (selected) and 'ASCII'. Below these are two buttons: 'Double Encryption' and 'Triple Encryption'. The 'Enter Text:' field contains the binary string '0000011100111000'. The 'Enter Key:' field contains the binary string '1010011100111011'. Below the input fields are two buttons: 'Encrypt' and 'Decrypt'. The 'Result:' section shows the output: '明文为: 0110111101101011'.

图六 解密成功

加解密结果均匹配成功。

结果: 基本测试通过。

第二关 交叉测试

二进制单重加密

测试明文: 0000111100001111

密钥: 0010110101010101

测试密文: 1110011000000000

Encryption and Decryption

Select form: Binary

Message:

Key:

Encrypt Decrypt

CipherText: 1110011000000000

图七 另一组二进制单重加密

二进制单重解密

S-AES Encryption and Decryption

Binary ASCII

Double Encryption Triple Encryption

Enter Text:

Enter Key:

Encrypt Decrypt

Result:

明文为: 0000111100001111

图八 二进制单重解密

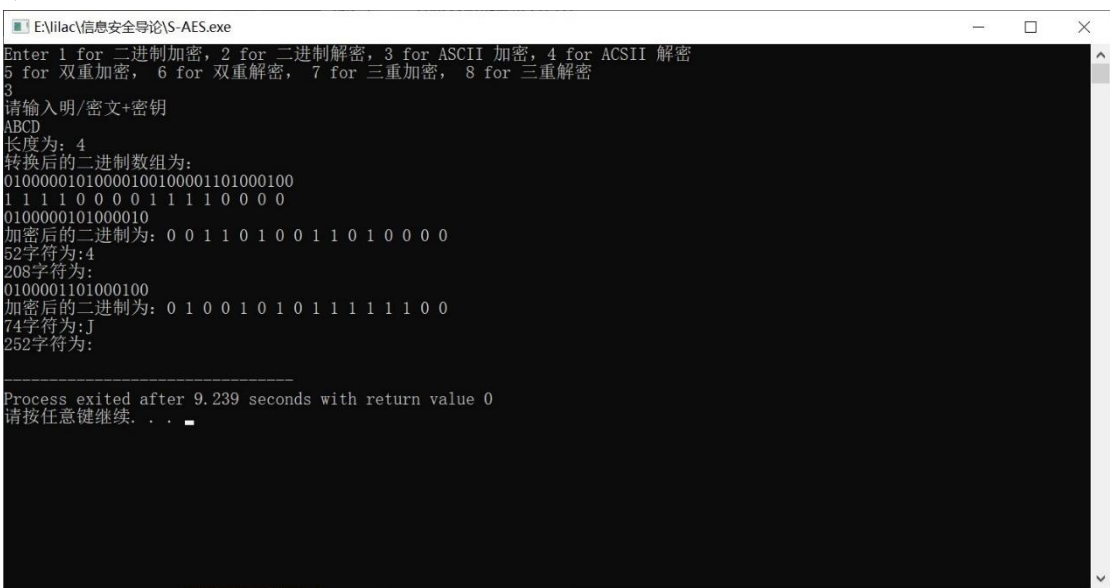
匹配成功!

ACSII 加密
测试明文: ABCD
密钥: 1111000011110000



图九 另一组 ACSII 加密

由于加密得到的密文为乱码无法在网页中正常显示, 所以我们采用命令行形式进行验证。根据加密后得到的 ACSII 值对照 ACSII 码表进行查询, 得到所对应的 ACSII 码与另一组的一致。



图十 我们组 ACSII 加密

匹配成功!

双重加密

测试明文: 1001010101110001

密钥: 11110000101010010001101010101001

测试密文: 1111000011001011

Multiple Encryption and Decryption

Select form: Double en-decryption

Message: 1001010101110001

Key: 11110000101010010001101010101010

Encrypt Decrypt

CipherText: 1111000011001011

图十一 另一组双重加密结果

S-AES Encryption and Decryption

Binary ACSII

Double Encryption Triple Encryption

Enter Text: 1111000011001011

Enter Key: 11110000101010010001101010101001

Encrypt Decrypt

Result: 明文为: 1001010101110001

图十二 我们组双重解密结果

匹配成功!

结果: 交叉测试通过

第三关 拓展功能

由于 ACSII 编码中第 0~31 以及第 127 个字符都是不可见的，并且存在部分字符与浏览器不兼容的问题，所以有部分密文无法在网页中正确显示。

输入明文：ER

密钥：1111000011110000

输出密文：?b

S-AES Encryption and Decryption

Binary

ACSII

Double Encryption

Triple Encryption

Enter Text:

ER

Enter Key:

1111000011110000

Encrypt

Decrypt

Result:

密文为：?b

图十三 ACSII 字符串加密

S-AES Encryption and Decryption

Binary

ACSII

Double Encryption

Triple Encryption

Enter Text:

?b

Enter Key:

1111000011110000

Encrypt

Decrypt

Result:

明文为：ER

图十四 ACSII 字符串解密

匹配成功!

第四关 多重加密

4.1 双重加密

测试明文: 0100101001110100

密钥: 10100111001110111010011100111011

测试密文: 0110111101101011

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

Enter Key:

Encrypt

Decrypt

Result:

密文为: 0110111101101011

图十五 双重加密成功

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

Enter Key:

Encrypt

Decrypt

Result:

明文为: 0100101001110100

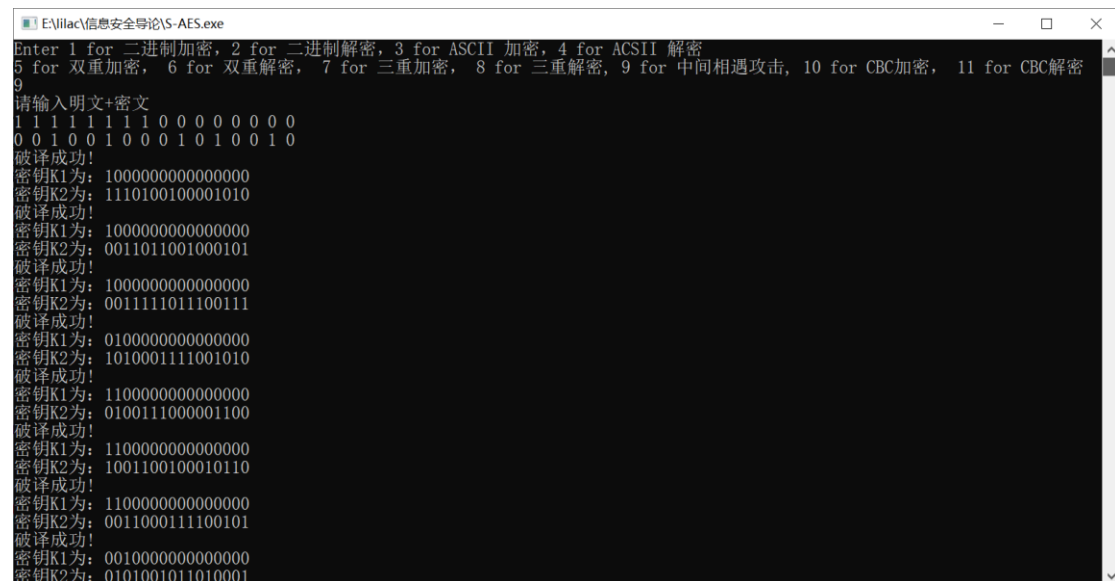
图十六 双重解密成功

4.2 中间相遇攻击

测试明文：1111111100000000

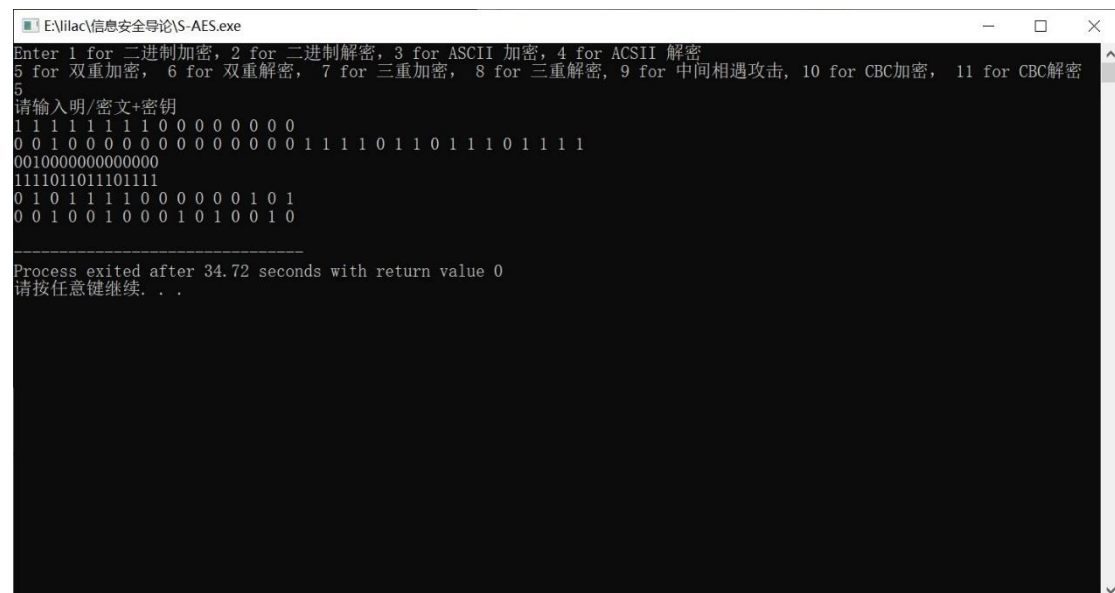
测试密文：0010010001010010

通过中间相遇攻击方法，获得可能的密钥为（数据量较大，仅截取部分数据进行展示）：



图十七 中间相遇攻击

取密钥 K1：1100000000000000，K2：0011000111100101 进行验证，以密钥 110000000000000011000111100101 对明文 1111111100000000 进行双重加密，得到加密后的密文为 0010010001010010，结果一致，中间相遇攻击成功！



图十八 验证中间相遇攻击是否成功

4.3 三重加密

测试明文: 0110111101101011

密钥: 101001110011101110100111001110111010011100111011

测试密文: 0011000011111011

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

0110111101101011

Enter Key:

101001110011101110100111001110111010011100111011

Encrypt

Decrypt

Result:

密文为: 0011000011111011

图十九 三重加密成功

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

0011000011111011

Enter Key:

101001110011101110100111001110111010011100111011

Encrypt

Decrypt

Result:

明文为: 0110111101101011

图二十 三重解密成功

第五关 工作模式

基于 S-AES 算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。注意初始向量(16 bits) 的生成，并需要加解密双方共享。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。

S-AES CBC Work Mode

Enter Text

Enter Key

Enter IV (leave empty for random)

Encrypt

Decrypt

Result:

图二十一 CBC 模式界面

在选择加密时，会自动隐藏初始向量 IV 的输入框，系统将随机生成唯一的初始向量 IV，并随着加密结果一同输出；在选择解密时，会自动显示初始向量 IV 的输入框，用户将之前系统给出的初始向量 IV 与密文、密钥一同进行输入，即可得到解密后的明文。

CBC 模式加密

测试明文：10101010101010101111000011110000

密钥：0000111100001111

测试密文：01111100101110011001101001111001

随机生成的初始向量 (IV): 1100110100100010

S-AES CBC Work Mode

10101010101010101111000011110000

0000111100001111

Encrypt

Decrypt

Result:

随机生成的初始向量 (IV): 1100110100100010

密文为: 01111100101110011001101001111001

图二十二 CBC 模式加密成功

CBC 模式解密

S-AES CBC Work Mode

01111100101110011001101001111001

0000111100001111

1100110100100010

EncryptDecrypt

Result:

明文为: 10101010101010101111000011110000

图二十三 CBC 模式解密成功

当密文分组被替换或修改时，我们仍采用以下测试用例：

测试明文：10101010101010101111000011110000

密钥：0000111100001111

测试密文：01111100101110011001101001111001

随机生成的初始向量 (IV): 1100110100100010

将密文修改为 11111100101110011001101001111001，其余条件保持不变。

解密后得到的明文为 01111010101000110111000011110000

S-AES CBC Work Mode

11111100101110011001101001111001

0000111100001111

1100110100100010

EncryptDecrypt

Result:

明文为: 01111010101000110111000011110000

图二十四 替换密文后的解密结果

对比前后明文可得，两次生成的明文不一致，密文被篡改后无法得到正确的明文。