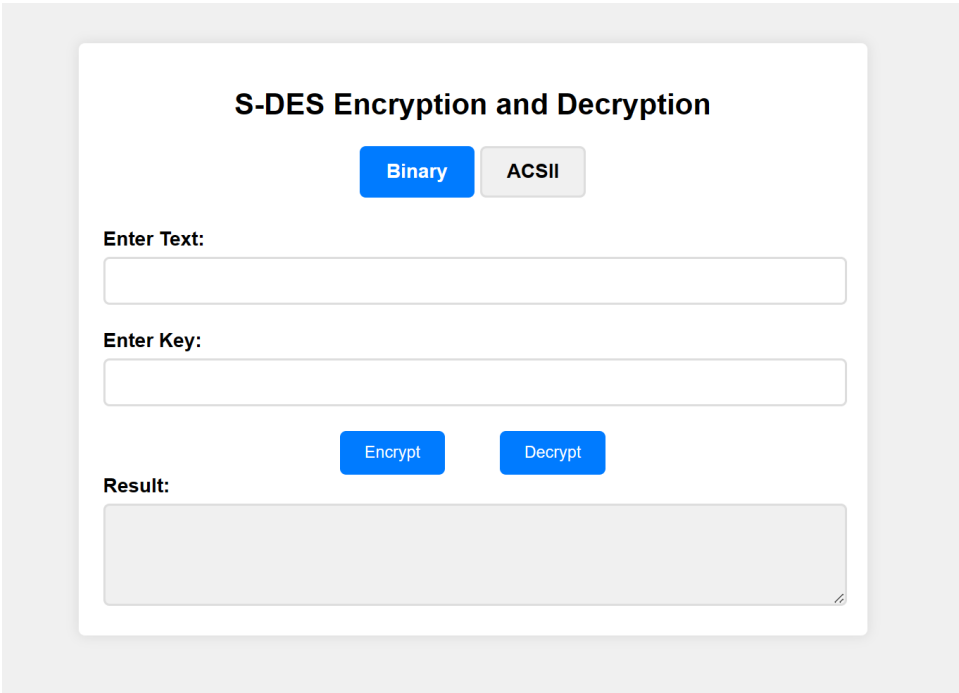


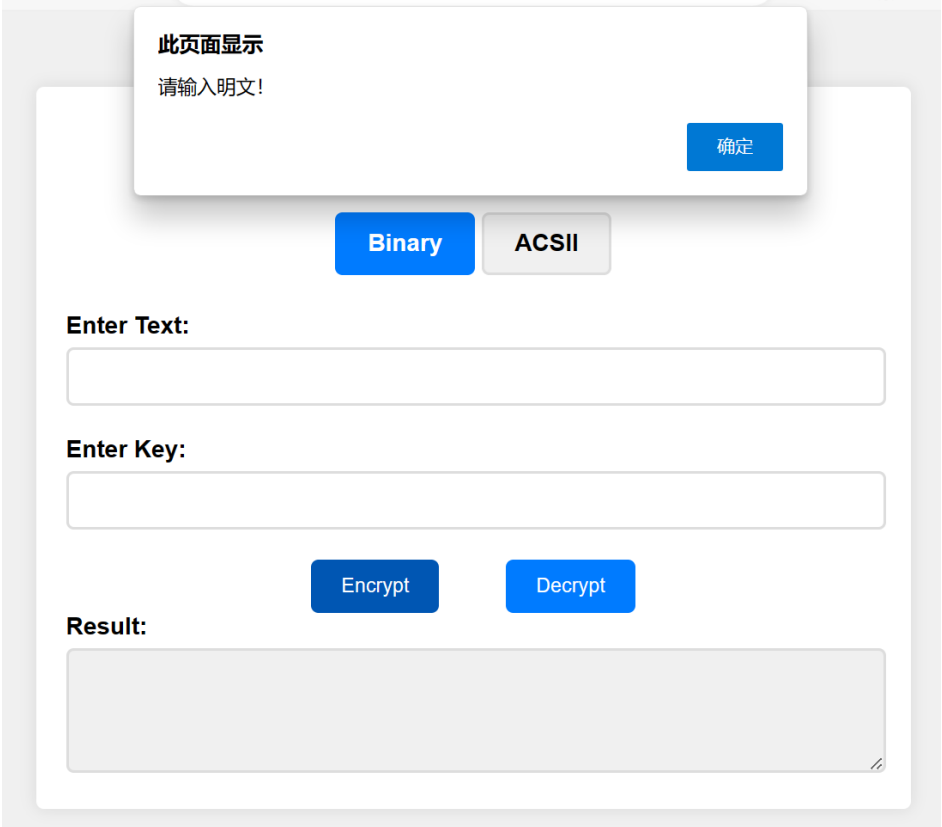
第一关 基本测试

界面设计



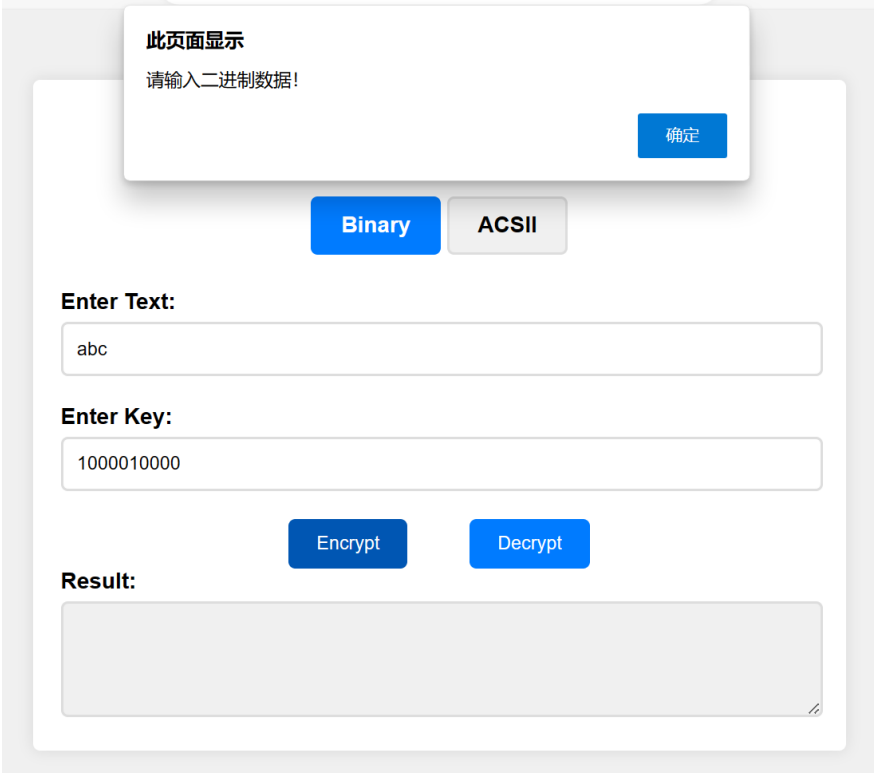
图一 用户界面

当 text 为空时，提示“请输入明文！”或“请输入密文！”



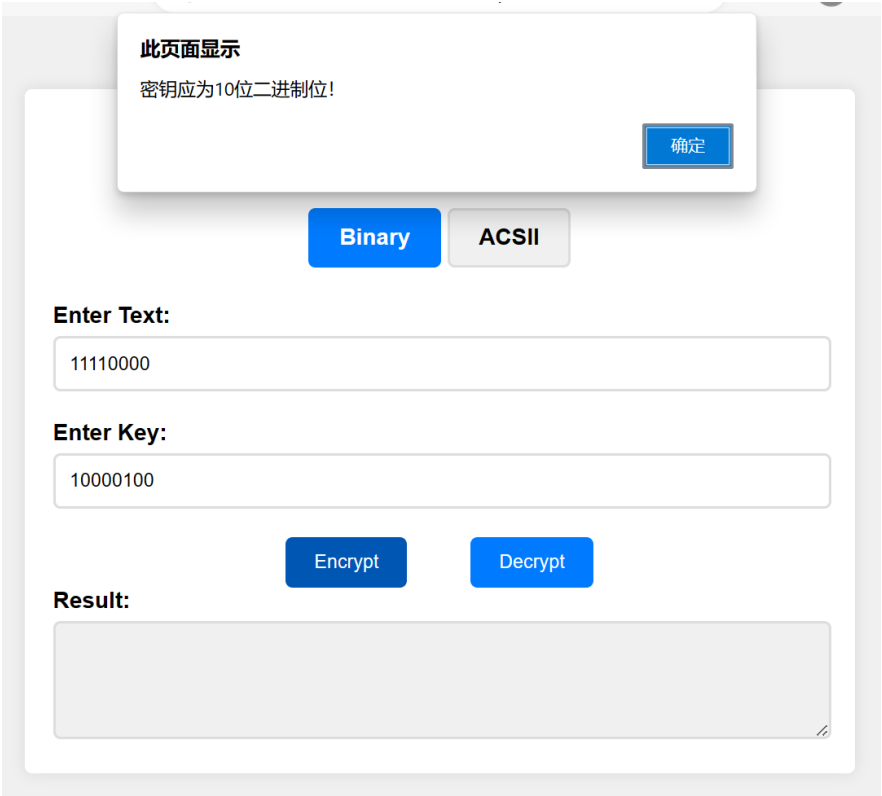
图二 提示输入明文

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



图三 提示输入二进制数

当输入密钥不是 10bit 位时，提示“密钥应为 10bit 位！”



图四 提示密钥为 10bit 位

测试明文：10101010
密钥：1111100000
生成密文：00011011

S-DES Encryption and Decryption

Binary

ASCII

Enter Text:

10101010

Enter Key:

1111100000

Encrypt

Decrypt

Result:

密文为: 00011011

图五 加密成功

测试密文：00011011
密钥：1111100000
生成明文：10101010

S-DES Encryption and Decryption

Binary

ASCII

Enter Text:

00011011

Enter Key:

1111100000

Encrypt

Decrypt

Result:

明文为: 10101010

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

二进制加密

测试明文: 10101010

密钥: 1111100000

测试密文: 00011011

Encryption and Decryption

Select form: Binary ▼

Message:

Key:

Encrypt Decrypt

密文为: 00011011

图七 另一组二进制加密

二进制解密

S-DES Encryption and Decryption

Binary ASCII

Enter Text:

Enter Key:

Encrypt Decrypt

Result:

明文为: 10101010

图八 二进制解密

匹配成功!

ACSII 加密

测试明文: Hello

密钥: 0100010001

测试密文: &Xkk)

S-DES Encryption and Decryption

Binary

ACSII

Enter Text:

Hello

Enter Key:

010001000

Encrypt

Decrypt

Result:

密文为: &Xkk)

图九 ACSII 加密

ACSII 解密

S-DES 加密解密

明文 (8位二进制):

密文 (8位二进制):

&Xkk|

密钥 (10位二进制):

0100010001

生成密钥

加密

解密

解密结果: Hello

导出

图十 另一组 ACSII 解密

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：CjkR

密钥：1100010110

输出密文：iS*r

S-DES Encryption and Decryption

Binary

ACSII

Enter Text:

CjkR

Enter Key:

1100010110

Encrypt

Decrypt

Result:

密文为：iS*r

图十一 ACSII 字符串加密

S-DES Encryption and Decryption

Binary

ACSII

Enter Text:

iS*r

Enter Key:

1100010110

Encrypt

Decrypt

Result:

明文为：CjkR

图十二 ACSII 字符串解密

匹配成功!

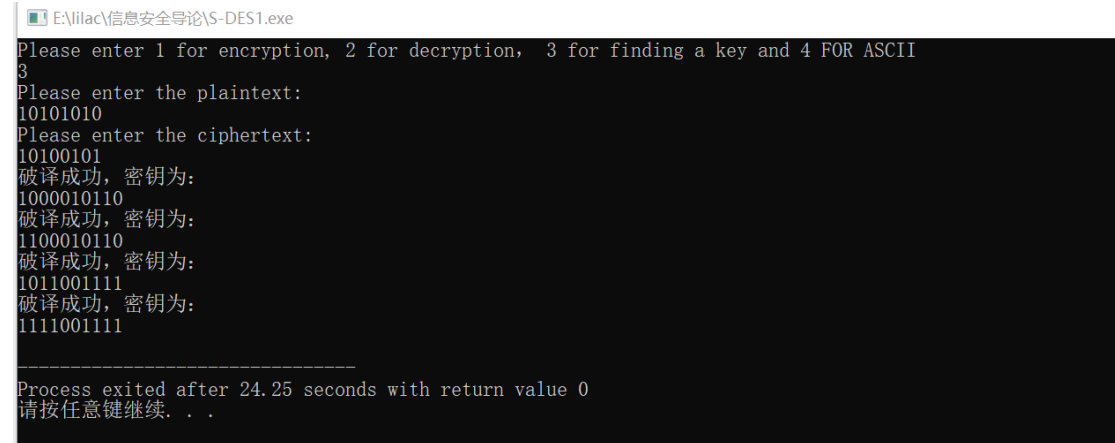
第四关 暴力破解

明文: 10101010

密文: 10100101

测试结果: ['1000010110','1100010110','1011001111','1111001111']

暴力破解用时: 24.25s



```
E:\lilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
3
Please enter the plaintext:
10101010
Please enter the ciphertext:
10100101
破译成功, 密钥为:
1000010110
破译成功, 密钥为:
1100010110
破译成功, 密钥为:
1011001111
破译成功, 密钥为:
1111001111

-----
Process exited after 24.25 seconds with return value 0
请按任意键继续. . .
```

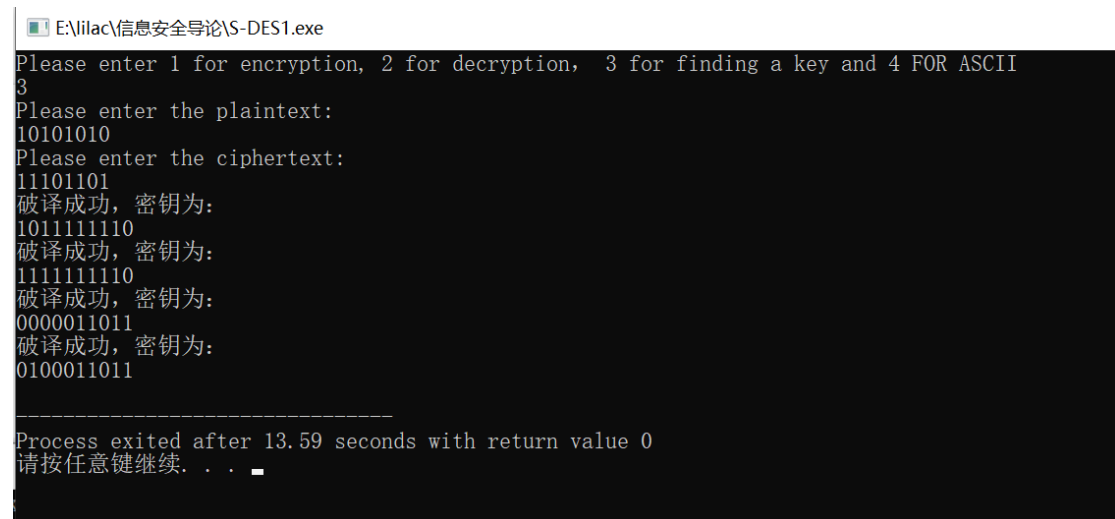
图十三 暴力破解示例一

明文: 10101010

密文: 11101101

测试结果: ['1011111110','1111111110','0000011011','0100011011']

暴力破解用时: 13.59s



```
E:\lilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
3
Please enter the plaintext:
10101010
Please enter the ciphertext:
11101101
破译成功, 密钥为:
1011111110
破译成功, 密钥为:
1111111110
破译成功, 密钥为:
0000011011
破译成功, 密钥为:
0100011011

-----
Process exited after 13.59 seconds with return value 0
请按任意键继续. . .
```

图十四 暴力破解示例二

明文: 10101010

密文: 00011001

测试结果: ['0010100000','0110100000','0011101010','0111101010']

暴力破解用时: 10.94s

```
E:\lilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
3
Please enter the plaintext:
10101010
Please enter the ciphertext:
00011001
破译成功, 密钥为:
0010100000
破译成功, 密钥为:
0110100000
破译成功, 密钥为:
0011101010
破译成功, 密钥为:
0111101010
-----
Process exited after 10.94 seconds with return value 0
请按任意键继续. . .
```

图十五 暴力破解示例三

第五关 封闭测试

根据第四关结果分析得到, 对于我们随机选择的一个明密文对有不只一个密钥 key。

接下来我们进一步讨论, 对应明文空间任意给定的明文分组 $P_{\{n\}}$, 是否会出现选择不同的密钥 $K_{\{i\}} \neq K_{\{j\}}$ 加密得到相同密文 C_n 的情况。

通过第四关, 我们发现, 对于一个明文可以找到几个使其加密成相同密文的密钥, 由此, 我们以明文 10101010, 密文 10100101 为例, 对暴力破解这对明密文所得到的密钥对 1100010110 和 1000010110 进行测试, 分析其产生的子密钥。

```
E:\lilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
1
1100010110
10101010
子密钥k1为:
10101001
子密钥k2为:
10101010
10100101
_
```

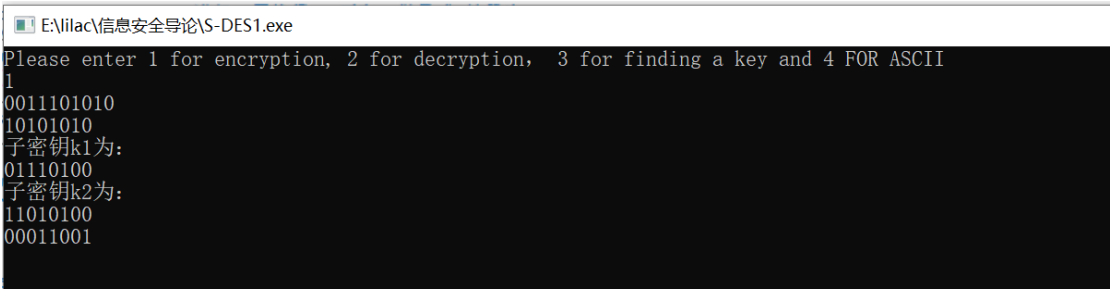
图十六 1100010110 生成的子密钥

```
E:\lilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and
1
1000010110
10101010
子密钥k1为:
10101001
子密钥k2为:
10101010
10100101
```

图十七 1000010110 生成的子密钥

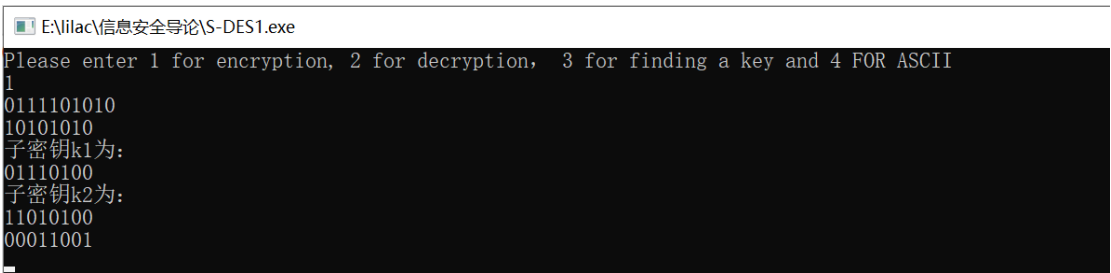
结果: 1100010110 和 1000010110 产生的两个子密钥一致, 加密结果一致

以明文 10101010，密文 00011001 为例，对其密钥对 0011101010 和 0111101010 进行测试分析。



```
E:\ilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
1
0011101010
10101010
子密钥k1为:
01110100
子密钥k2为:
11010100
00011001
```

图十八 0011101010 生成的子密钥

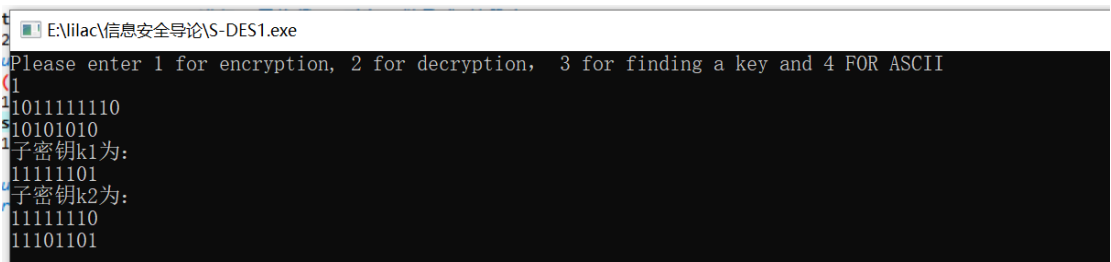


```
E:\ilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
1
0111101010
10101010
子密钥k1为:
01110100
子密钥k2为:
11010100
00011001
```

图十九 0111101010 生成的子密钥

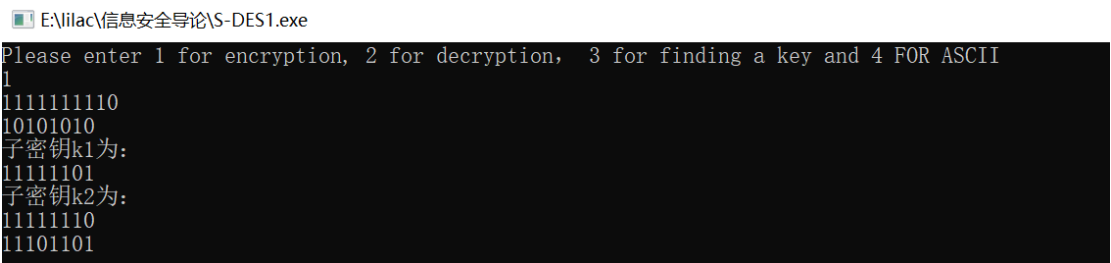
结果：0011101010 和 0111101010 产生的两个子密钥一致，加密结果一致

以明文 10101010，密文 11101101 为例，对其密钥对 1011111110 和 1111111110 进行测试分析。



```
E:\ilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
1
1011111110
10101010
子密钥k1为:
11111101
子密钥k2为:
11111110
11101101
```

图二十 1011111110 生成的子密钥



```
E:\ilac\信息安全导论\S-DES1.exe
Please enter 1 for encryption, 2 for decryption, 3 for finding a key and 4 FOR ASCII
1
1111111110
10101010
子密钥k1为:
11111101
子密钥k2为:
11111110
11101101
```

图二十一 1111111110 生成的子密钥

结果：1011111110 和 1111111110 产生的子密钥一致，加密结果一致

进一步分析发现，当两个 10bit 位的密钥只有第二位不同，其它位都相同时，这个两个密钥的子密钥相同。