S-DES测试结果

**第1关：基本测试**

**测试目标：**验证S-AES算法程序是否能够正确加密和解密16位的数据。

**测试结果：**经过测试，S-AES算法程序能够正确加密和解密16位的数据，并产生准确的密文。

测试步骤和结果：

（1）加密：

明文：1001001101111111

密钥：1100111100001111

密文：1011011110100111

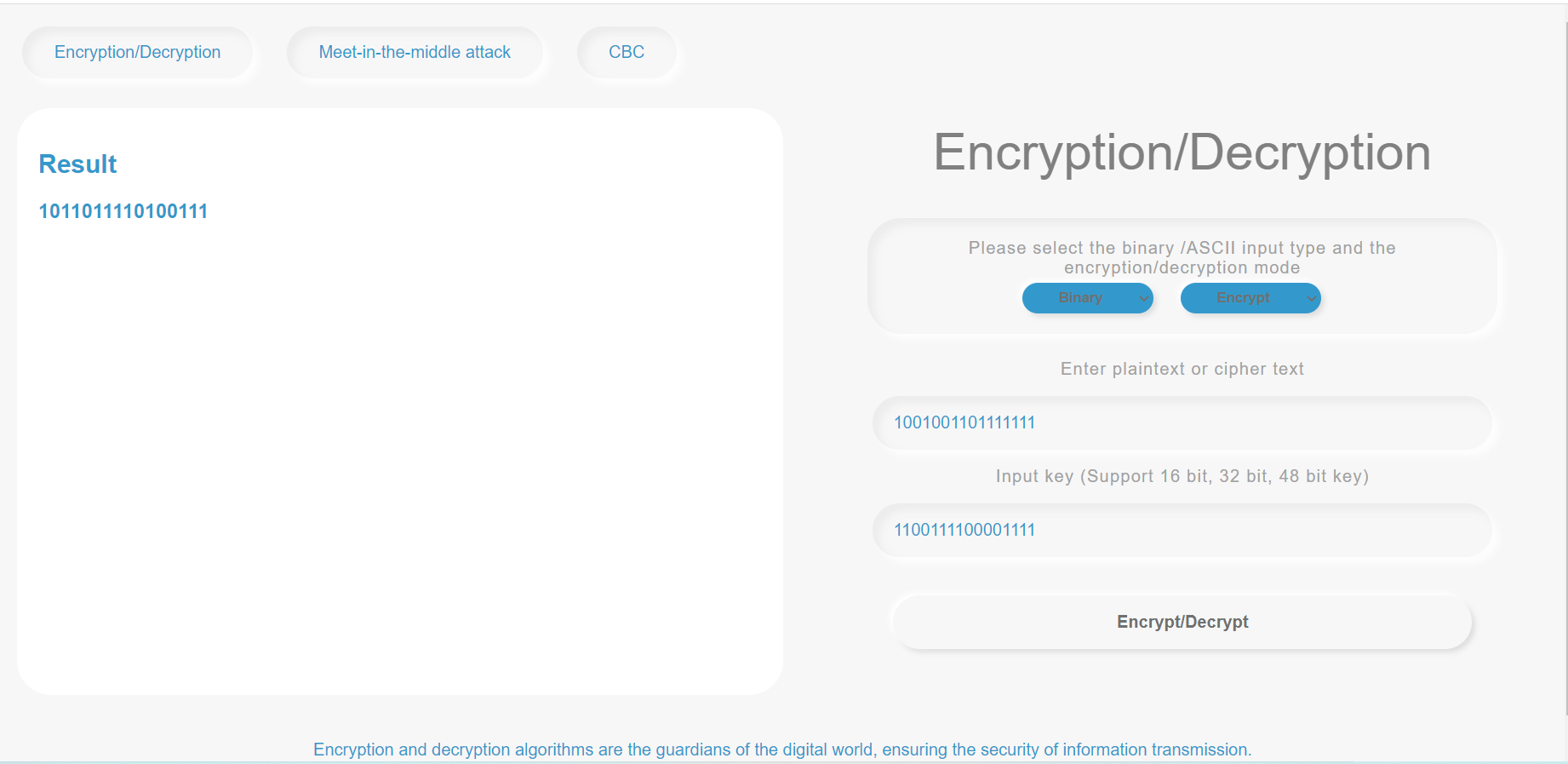


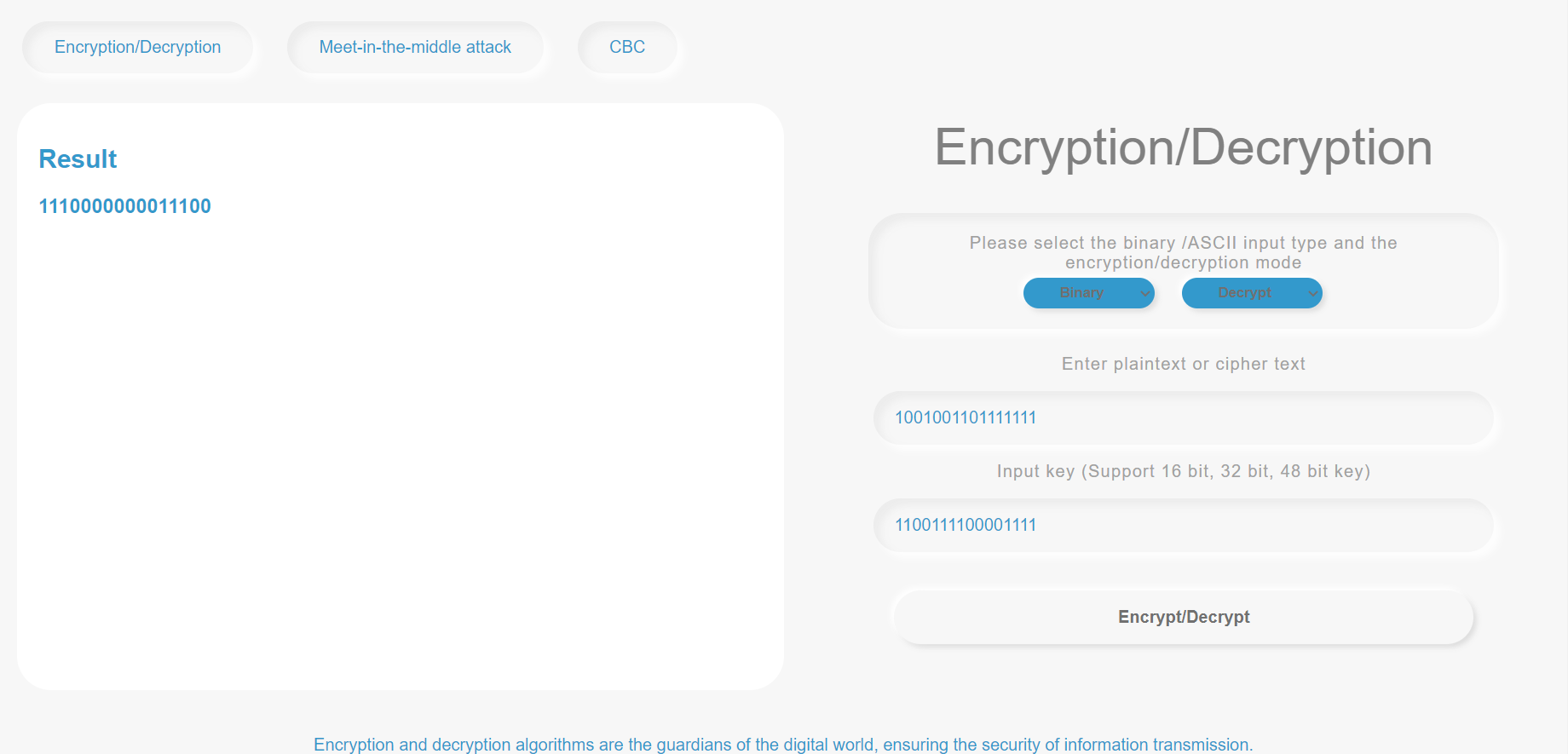
图1.1

（2）解密：

密文：1001001101111111

密钥：1100111100001111

明文：1110000000011100



**第2关：交叉测试**

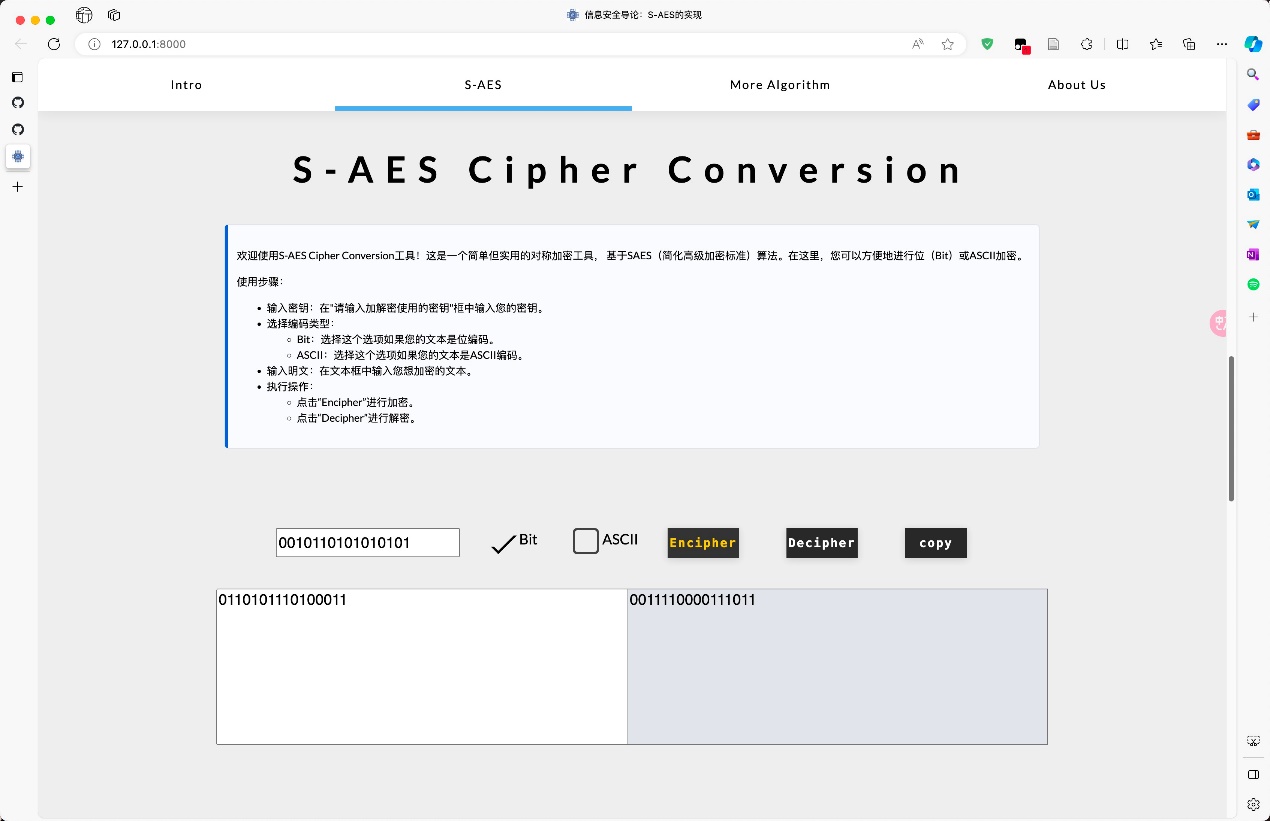
**测试目标：**验证不同人员编写的S-DES算法程序使用相同的密钥和明文时，能够得到相同的密文。

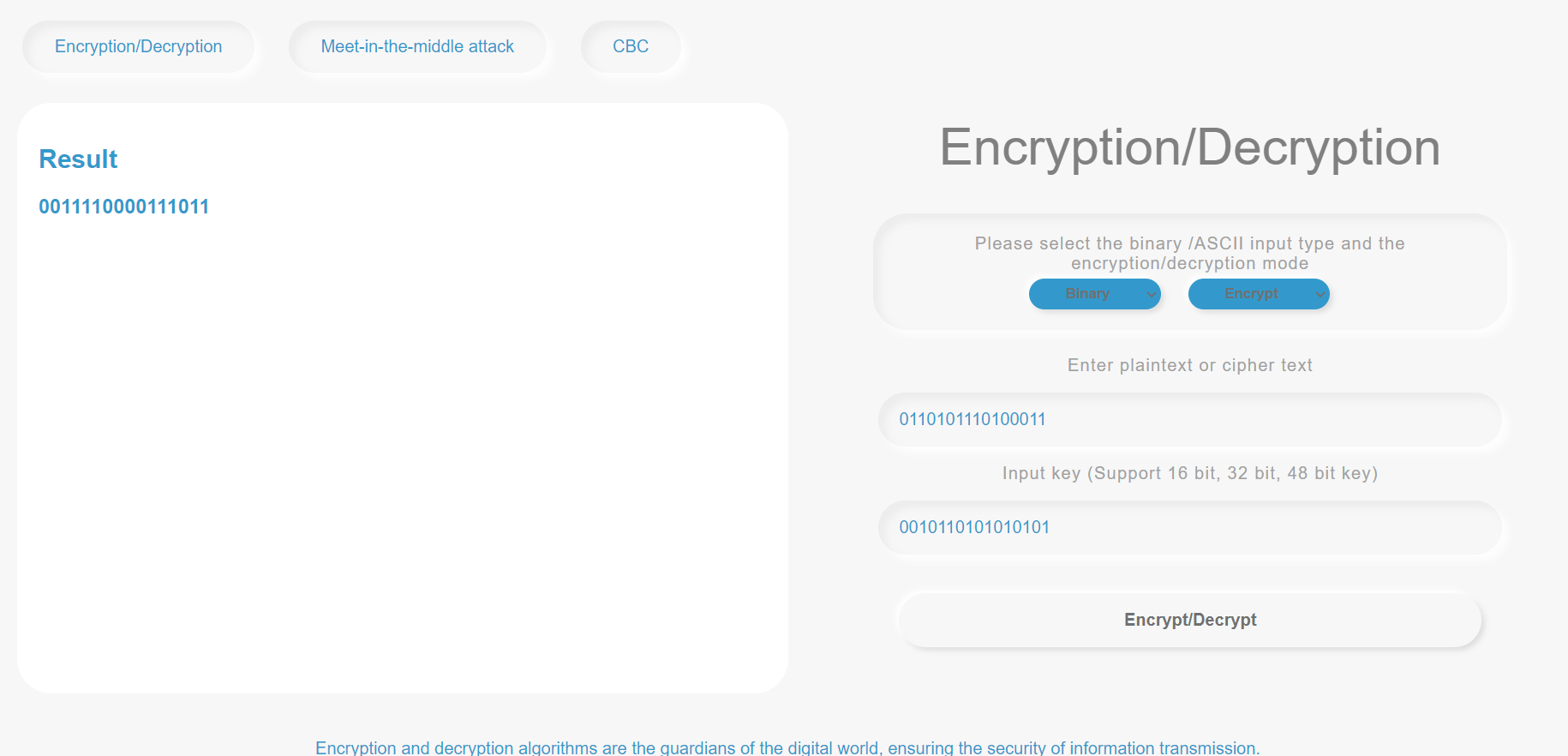
**测试结果：**经过交叉测试，不同编写的S-DES算法程序能够使用相同的密钥和明文得到相同的密文。

测试步骤和结果：

|  |  |  |
| --- | --- | --- |
| **测试输入** | **程序A输出** | **程序B输出** |
| 明文：0110101110100011  密钥：0010110101010101 | 密文：0010110101010101 | 密文：0010110101010101 |

程序A：



程序B（当前）：  


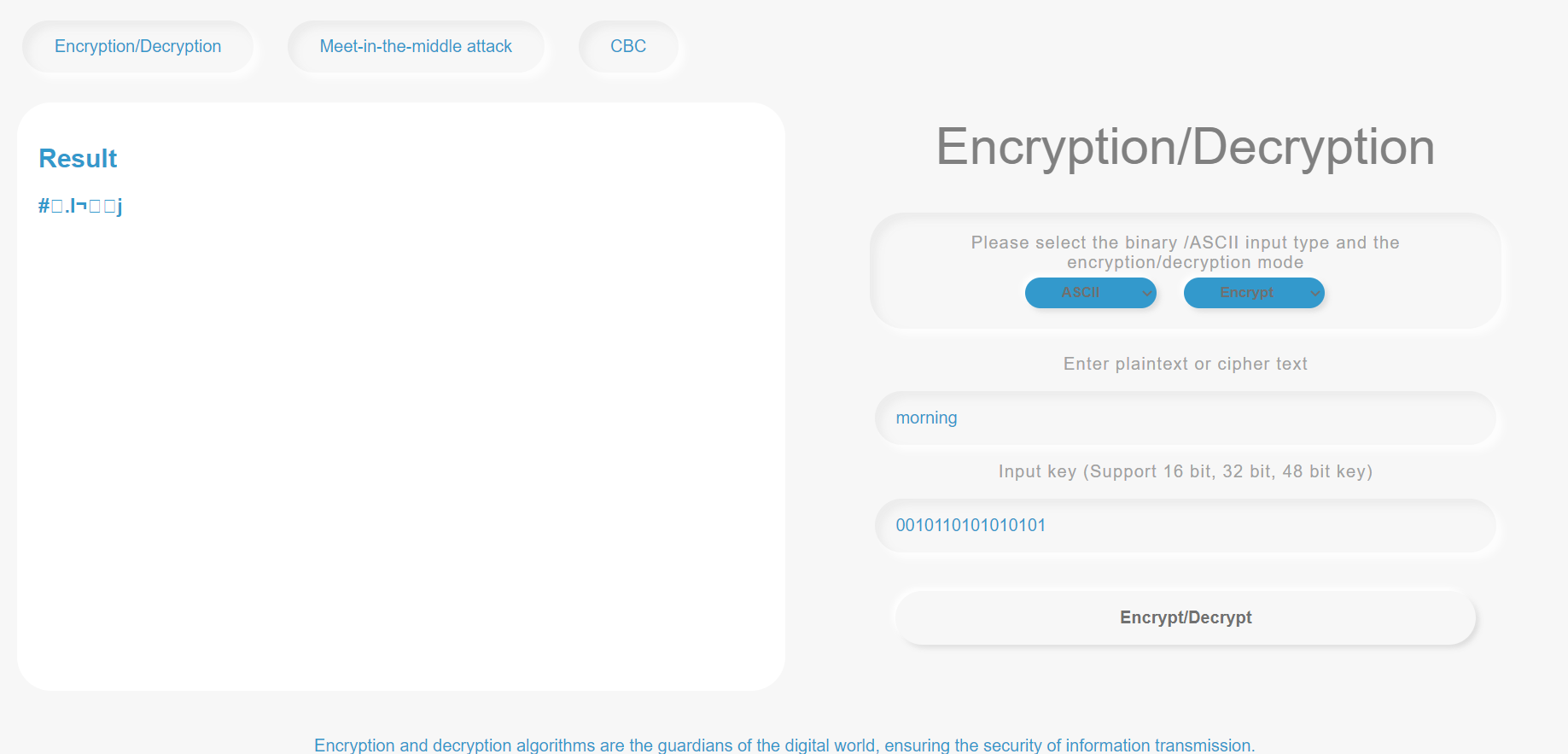
**第3关：扩展功能**

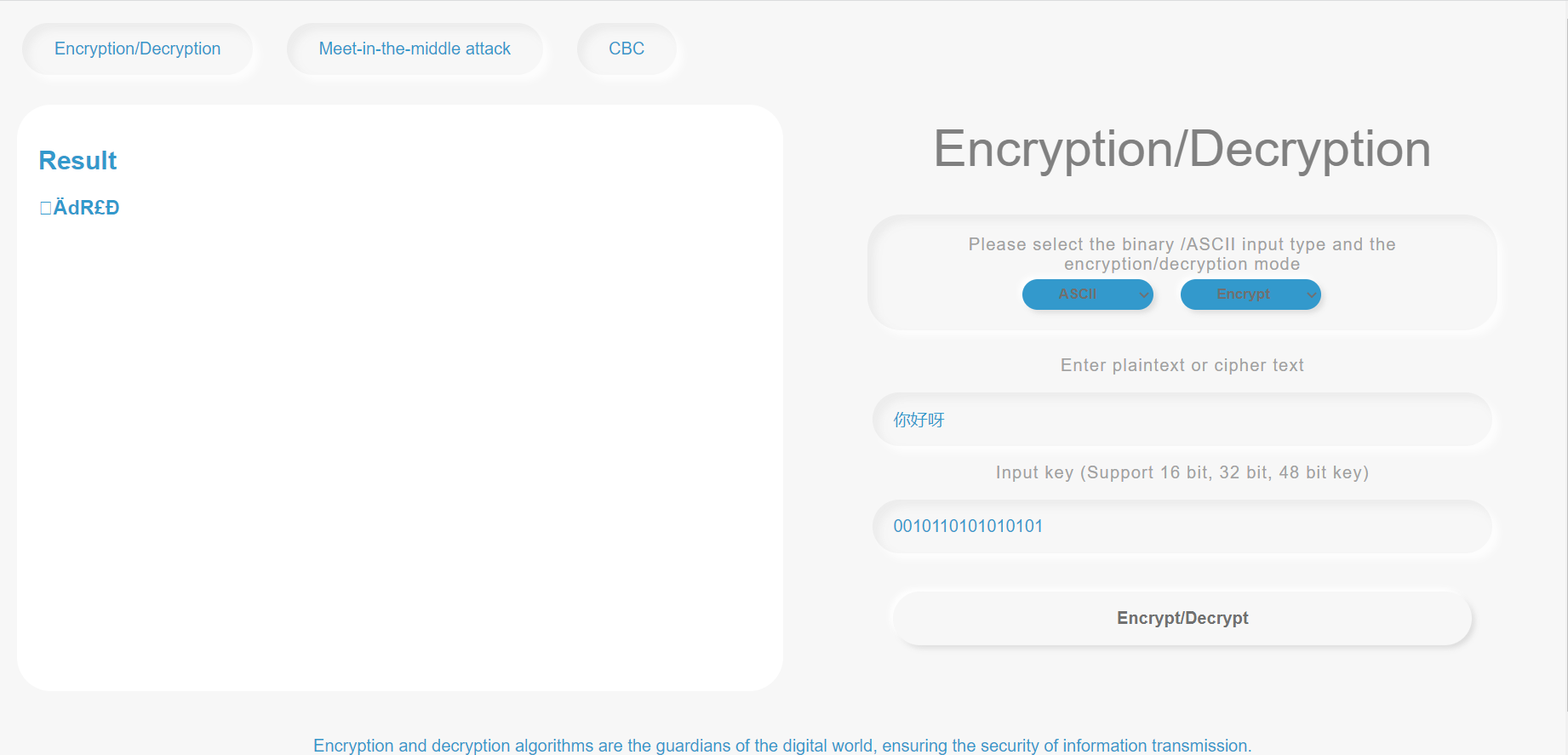
**测试目标：**验证S-AES算法程序是否能够处理ASCII编码字符串的加密和解密。

**测试结果：**经过测试，S-AES算法程序能够处理ASCII编码字符串的加密和解密，并产生相应的ASCII编码的密文。

测试步骤和结果：  
（1）加密

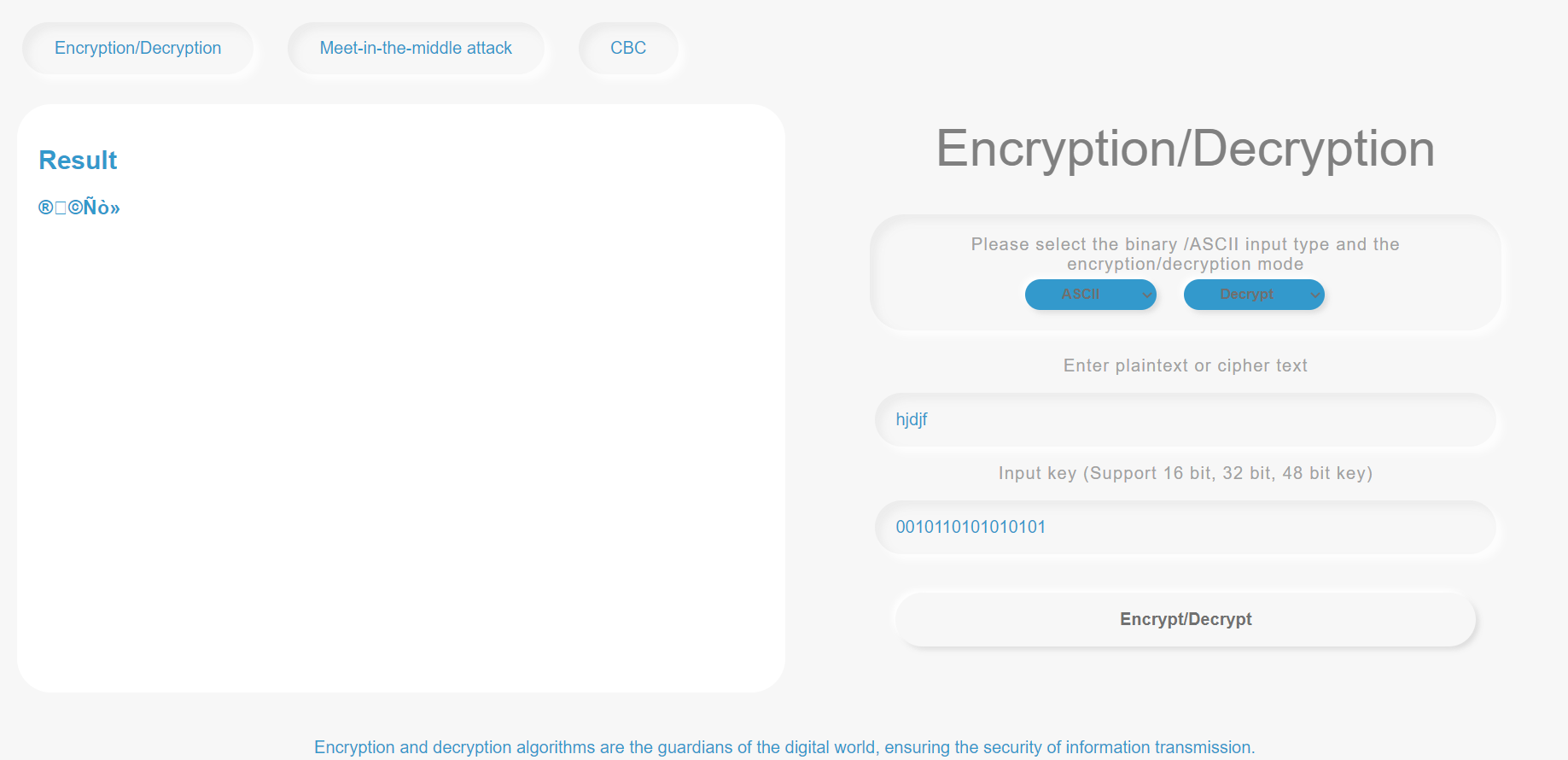
|  |  |
| --- | --- |
| **测试输入** | **输出** |
| 明文：morning 密钥：0010110101010101 | 密文：如图所示 |
| 明文：你好呀 密钥：0010110101010101 | 密文：如图所示 |

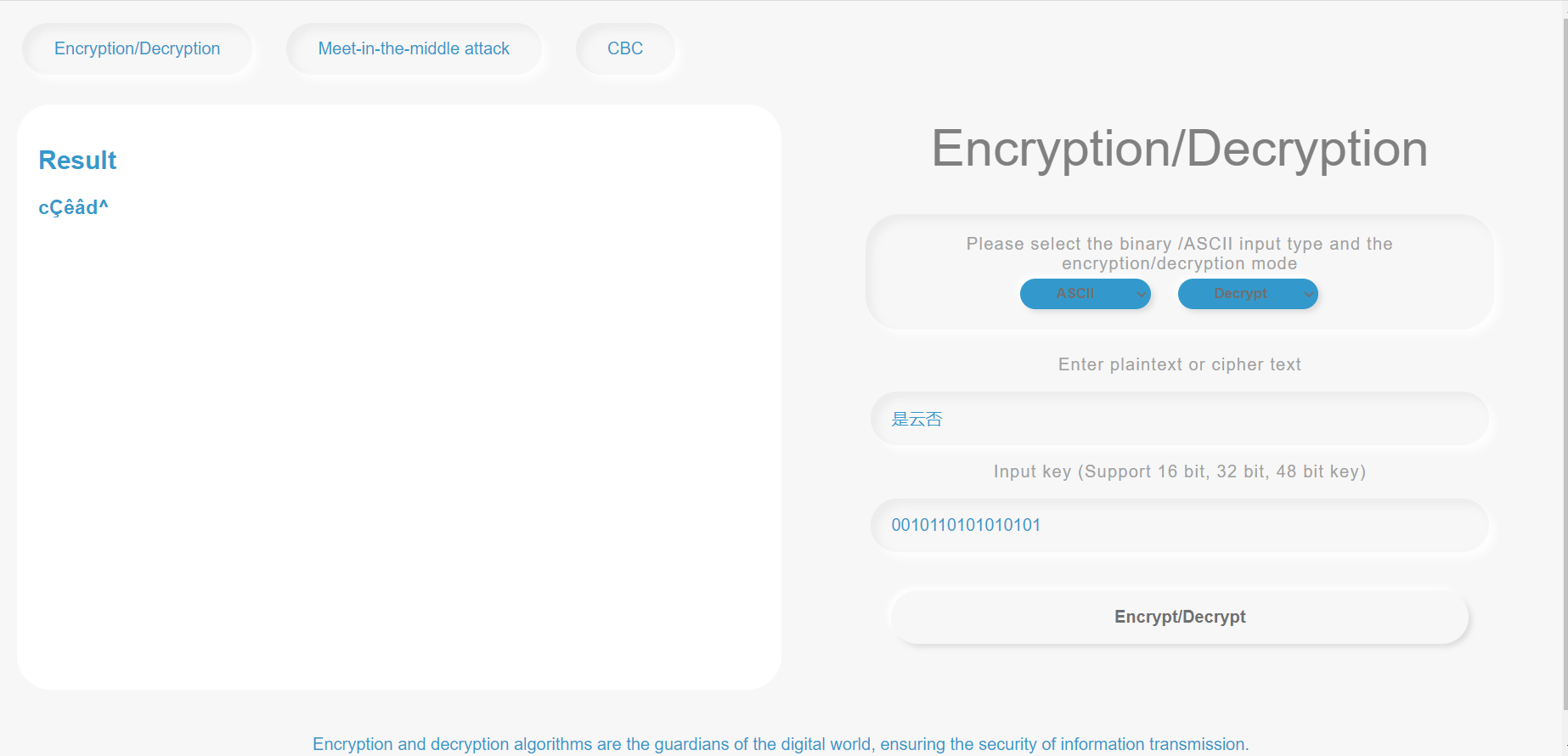




（2）解密

|  |  |
| --- | --- |
| **测试输入** | **输出** |
| 密文：hjdjf 密钥：0010110101010101 | 明文：如图所示 |
| 密文：是云否  密钥：0010110101010101 | 明文：如图所示 |





**第4关：多重加密**

**4.1双重加密**

**测试目标：**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32 bits。

**测试结果：**经过测试， S-AES算法通过双重加密进行扩展能够进行加解密。

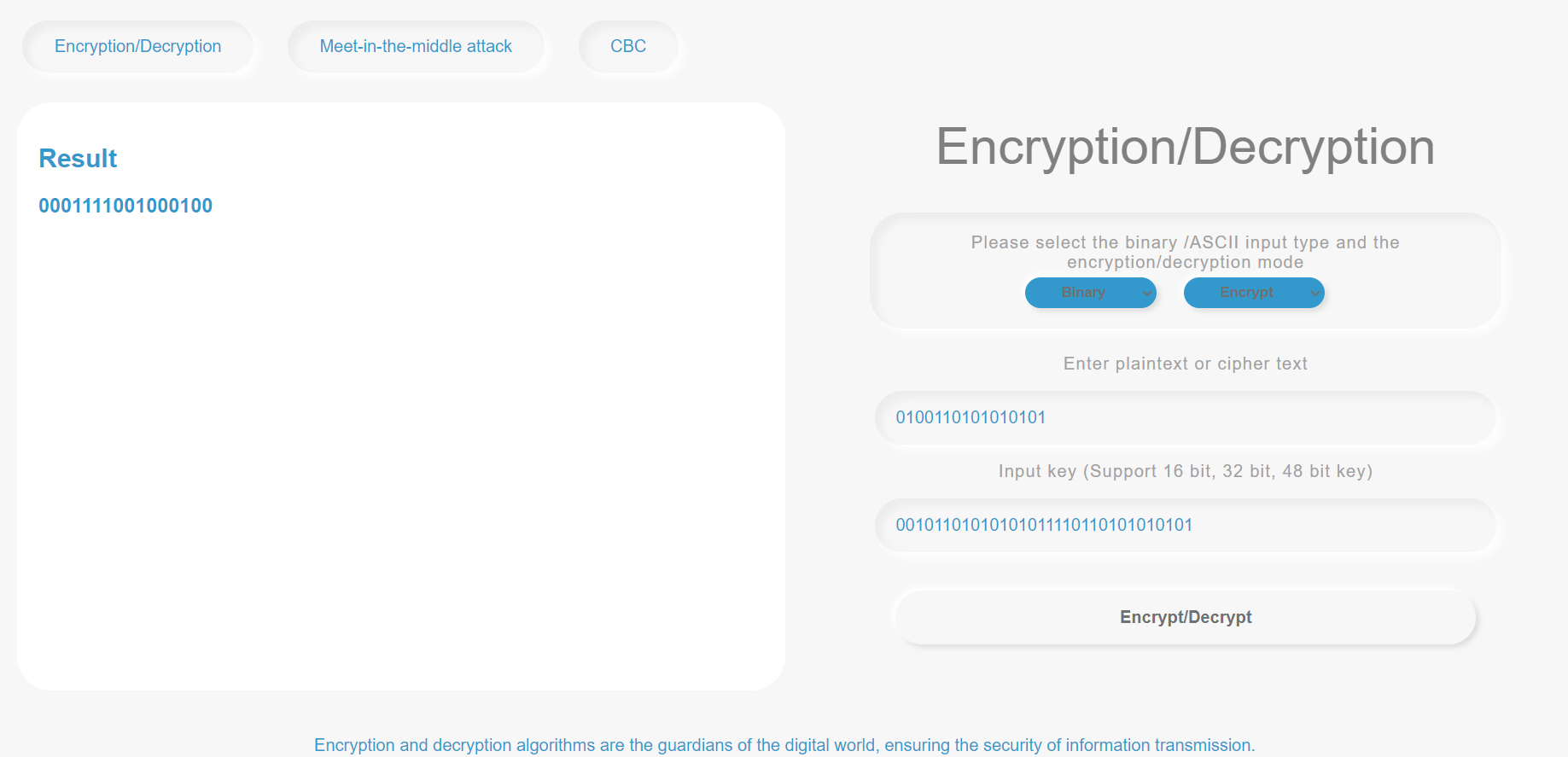


图4.1.1二进制加密

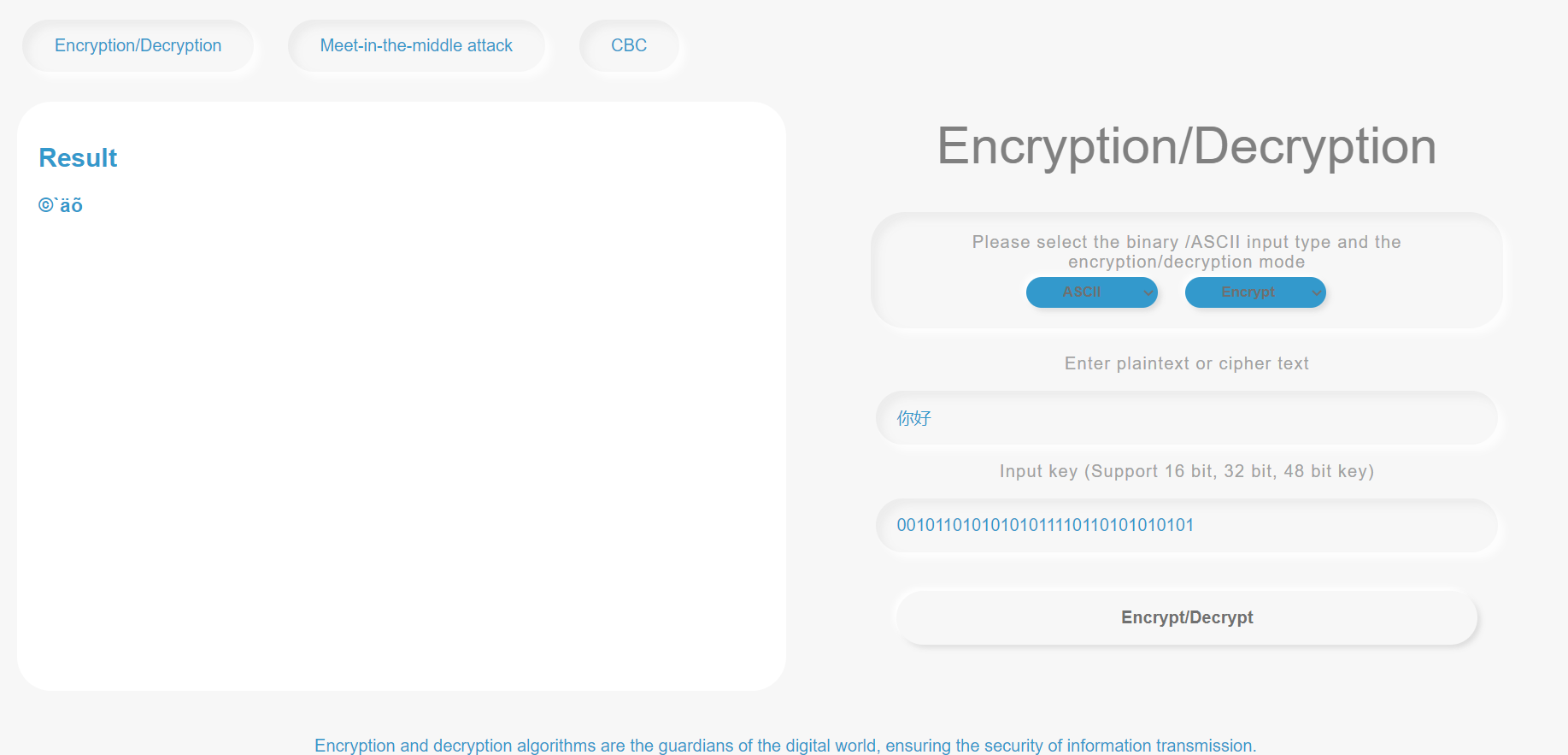


图4.1.2中文加密

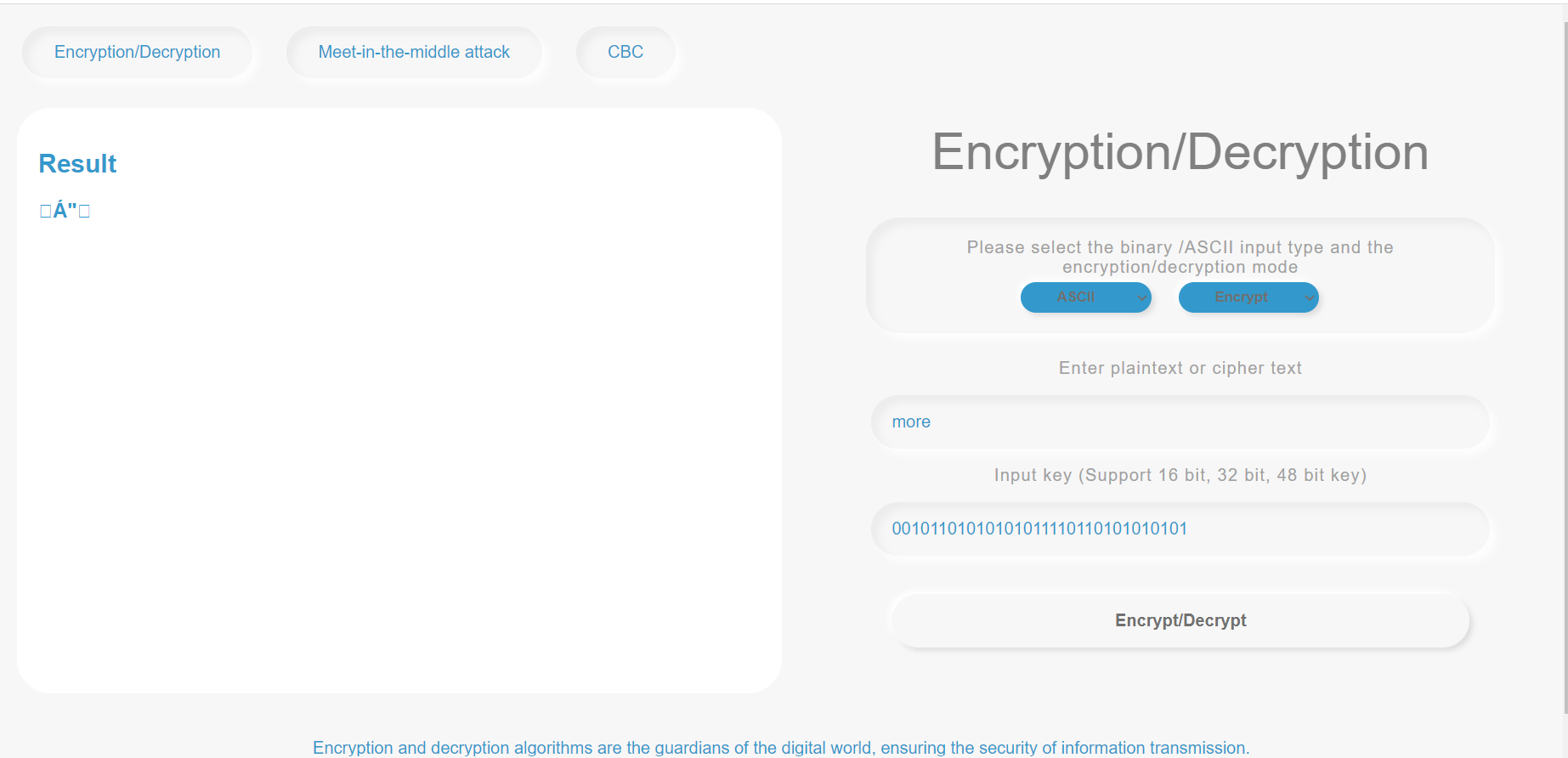


图4.1.3英文加密

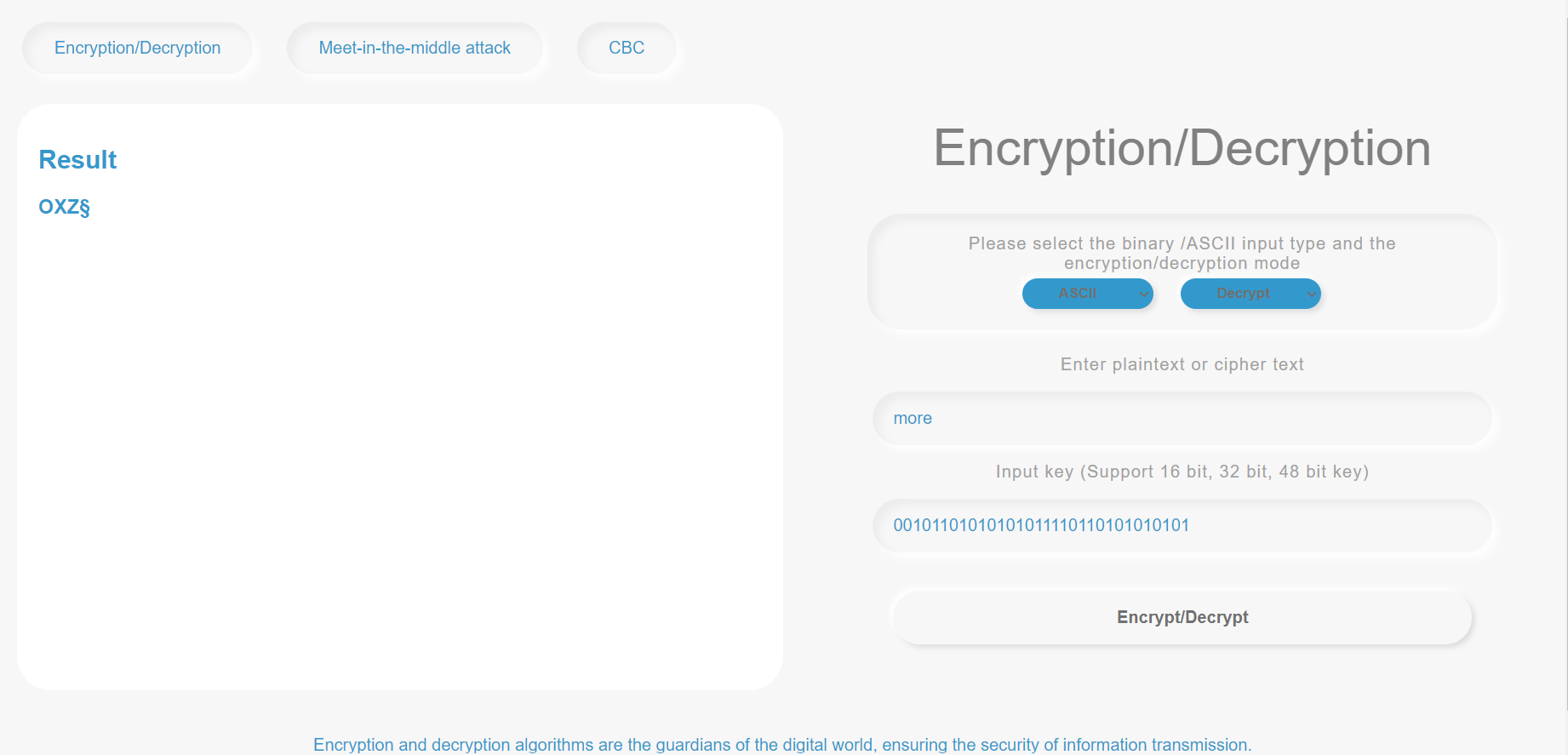


图4.1.4英文解密

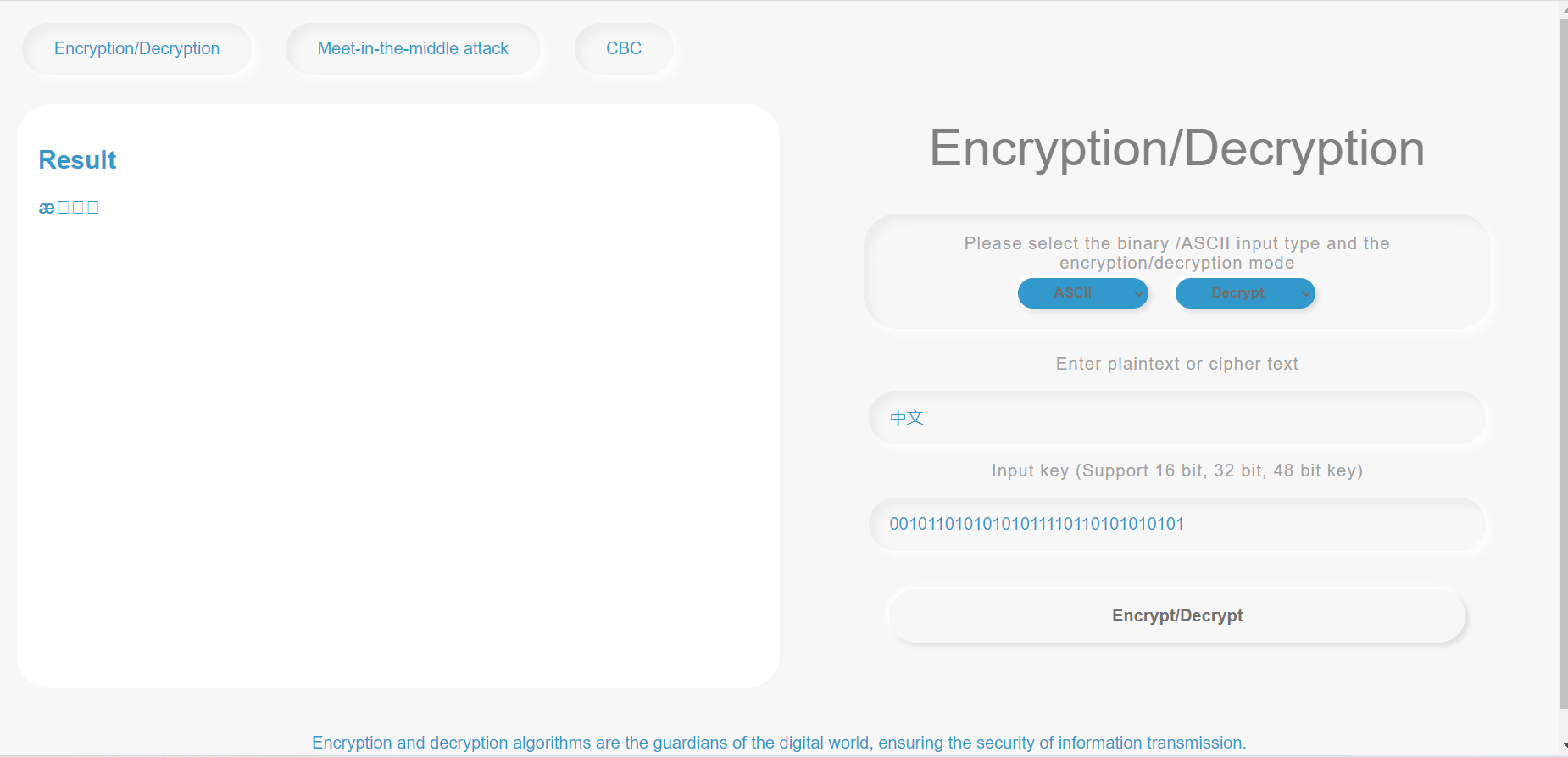


图4.1.5中文解密

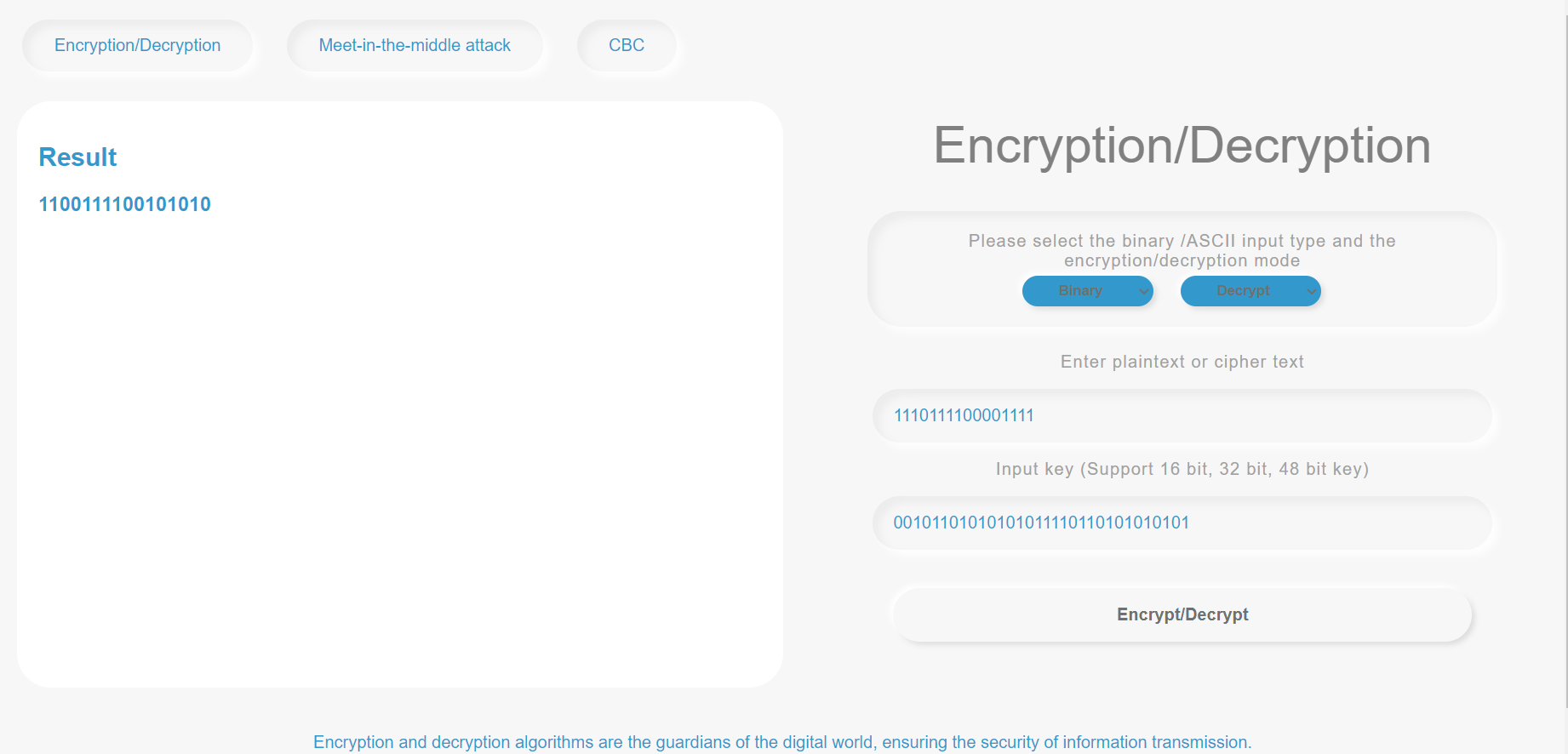


图4.1.6二进制解密

**4.2中途相遇攻击**

**测试目标：**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)。

**测试结果：**经过测试， S-AES算法的双重加密机制能够在中途相遇攻击中找到正确密钥

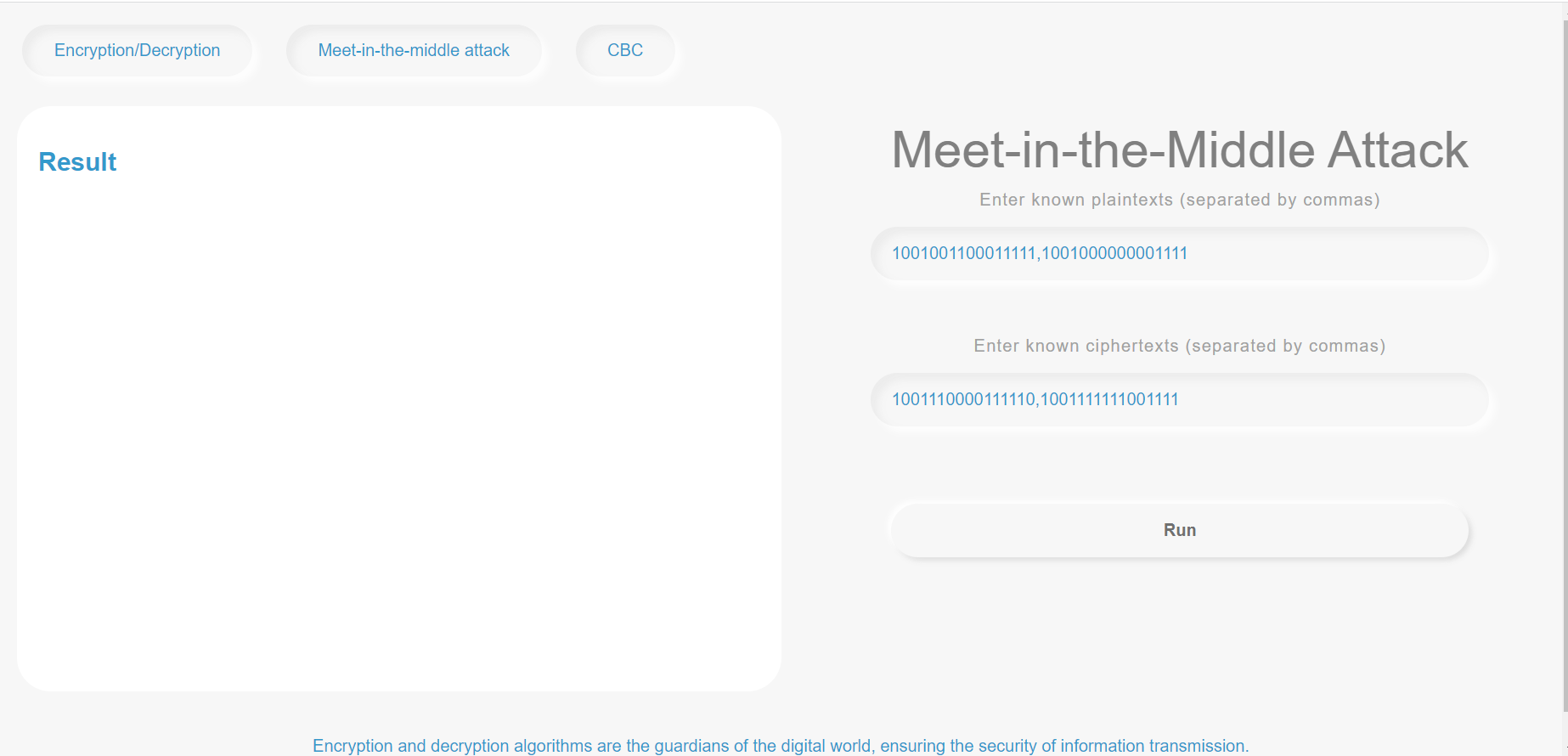


图4.2.1输入明文组、密文组

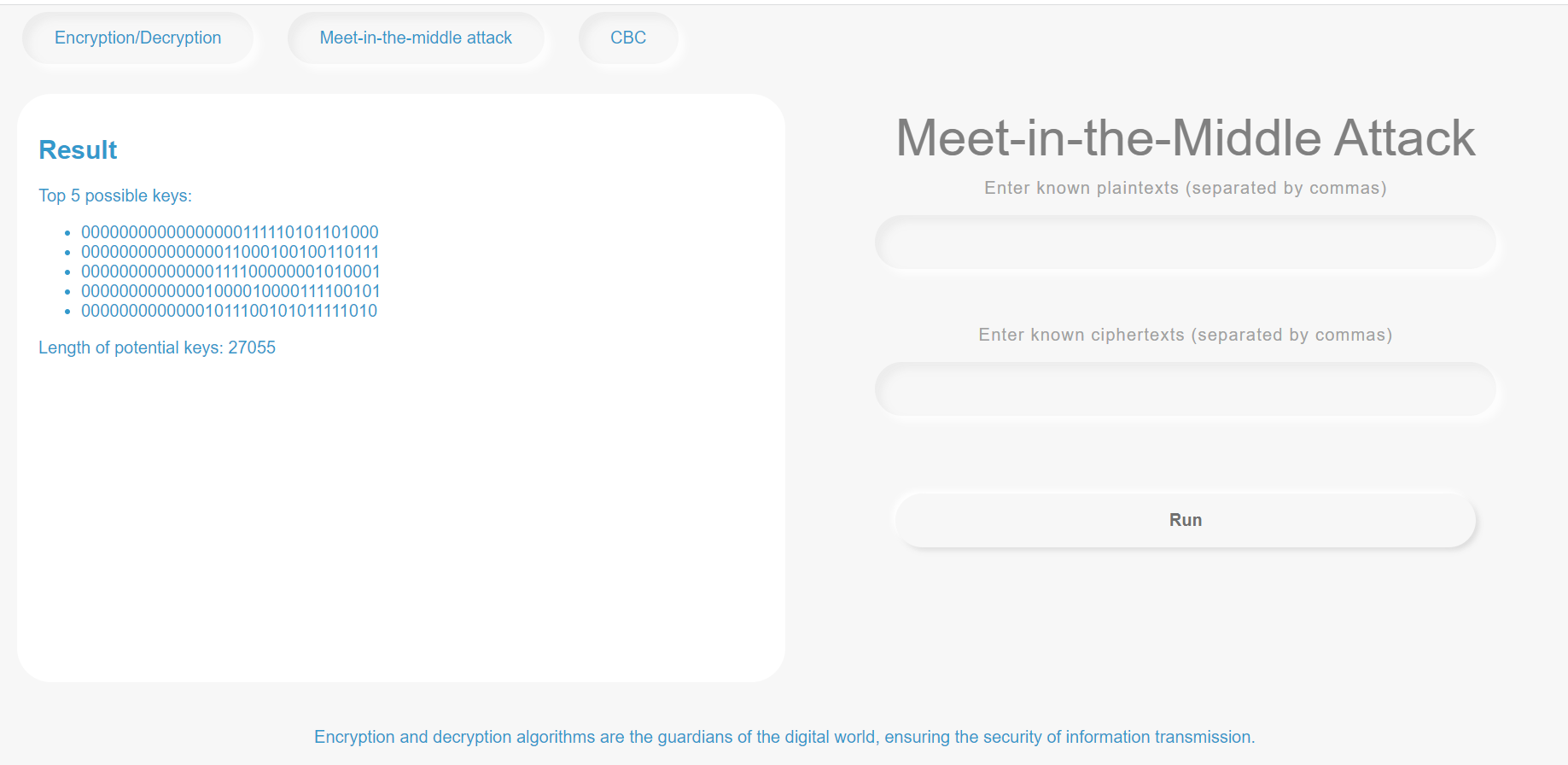


图4.2.2显示密钥

**4.3三重加密（k1,k2,k3）**

**测试目标：**使用48bits(K1+K2+K3)的模式进行三重加解密。

**测试结果：**经过测试， S-AES算法的三重加密机制成功完成。

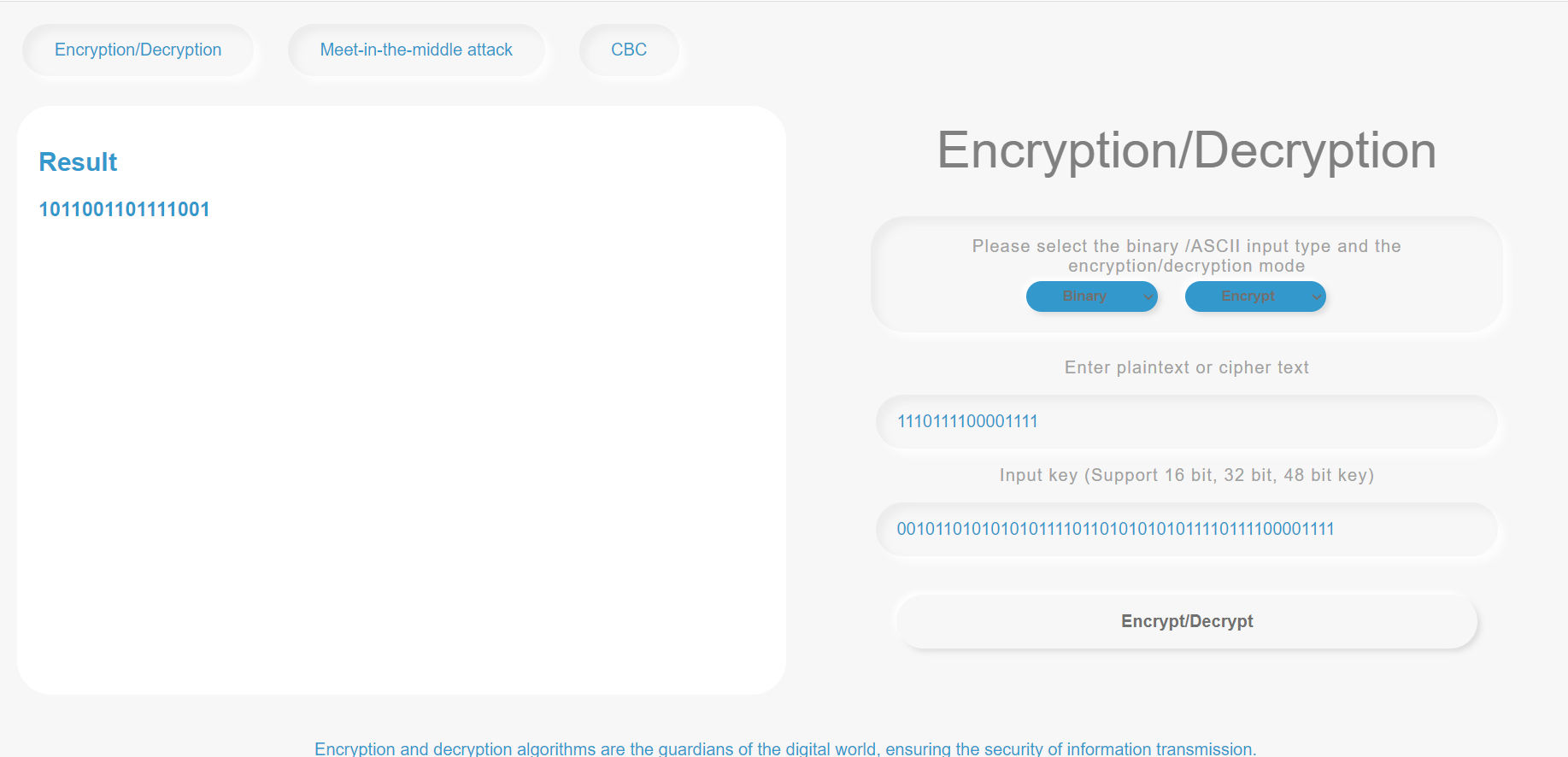


图4.3.1二进制加密

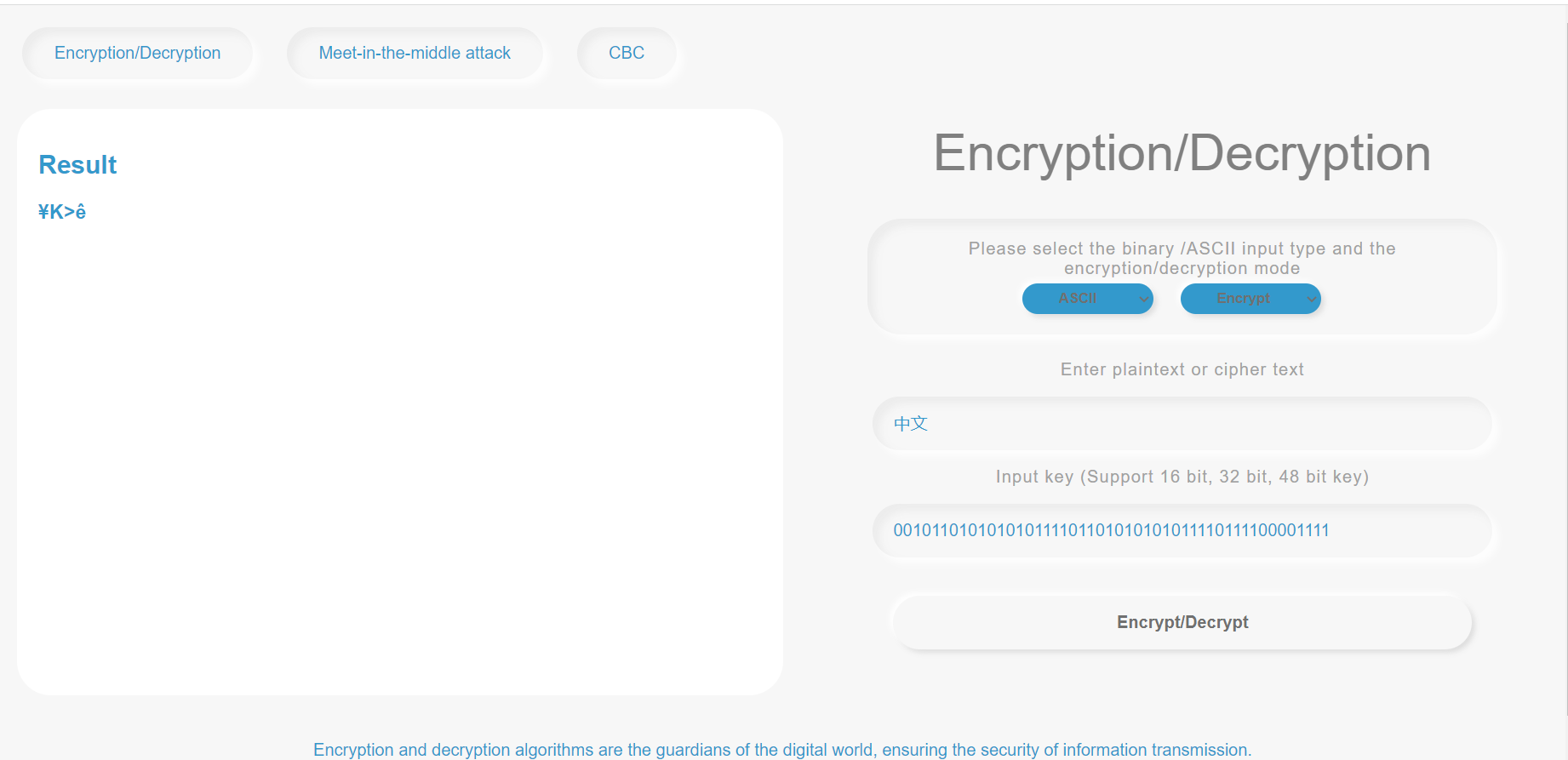


图4.3.2中文加密

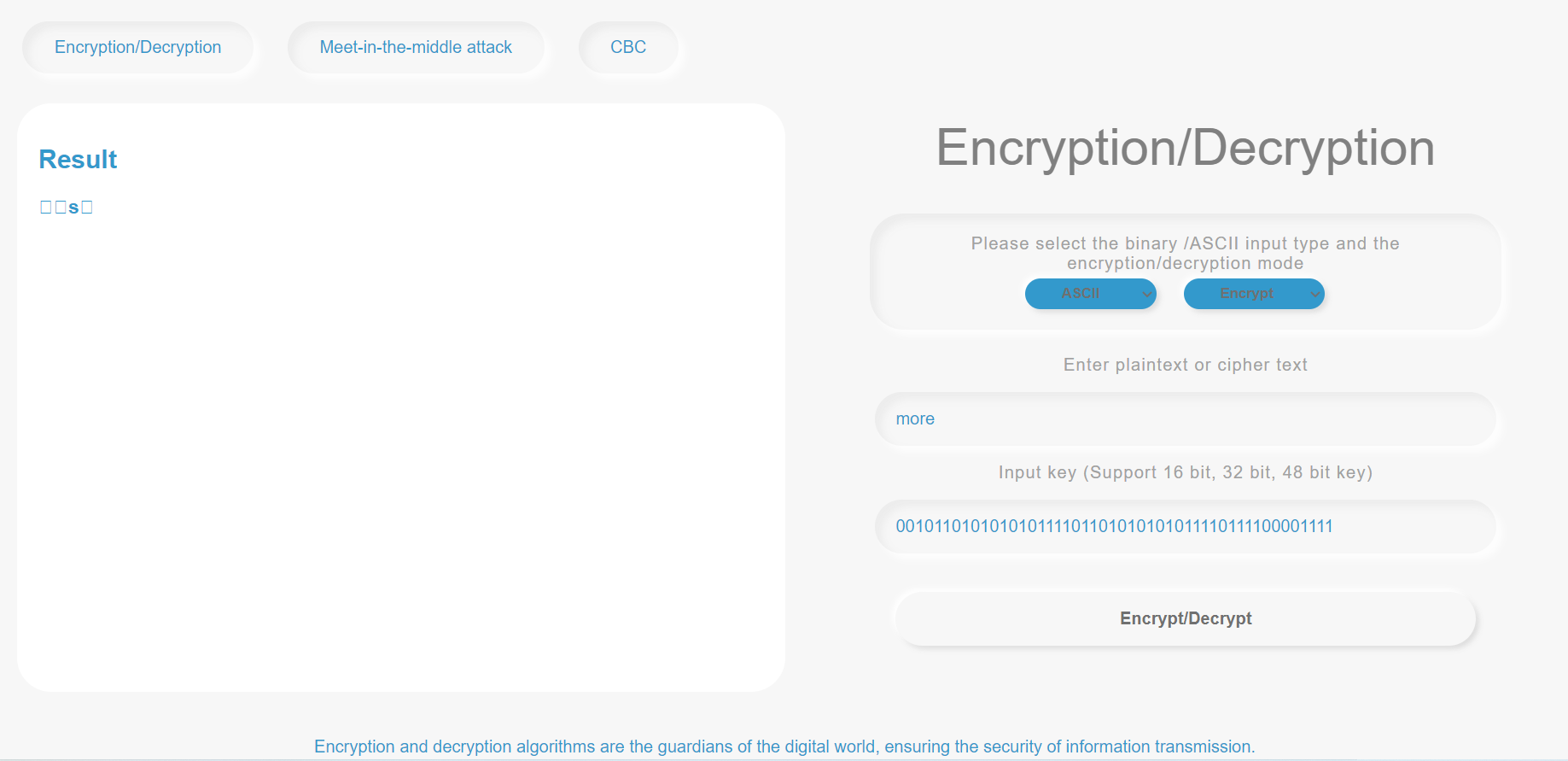


图4.3.3英文加密

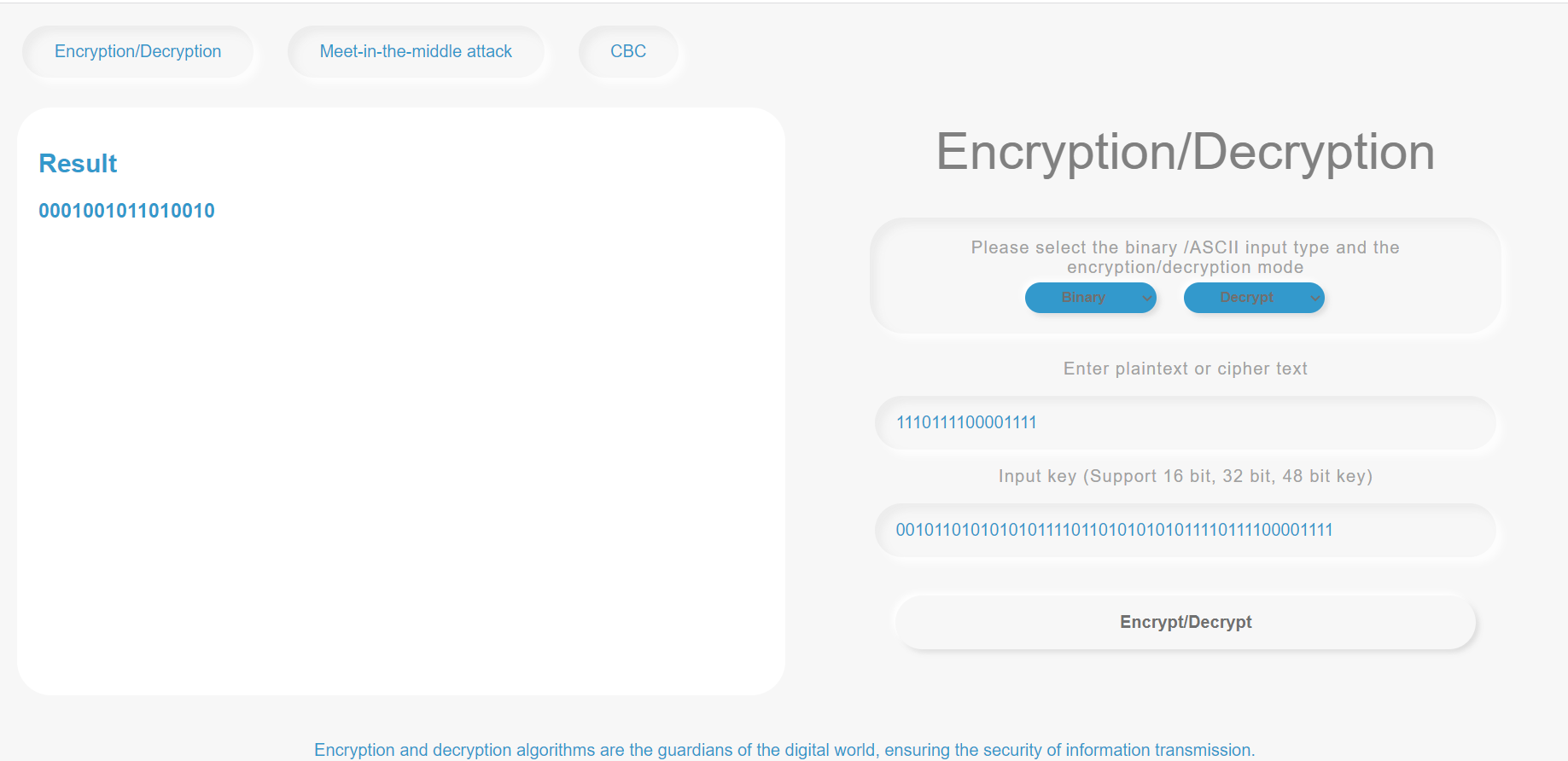


图4.3.4二进制解密

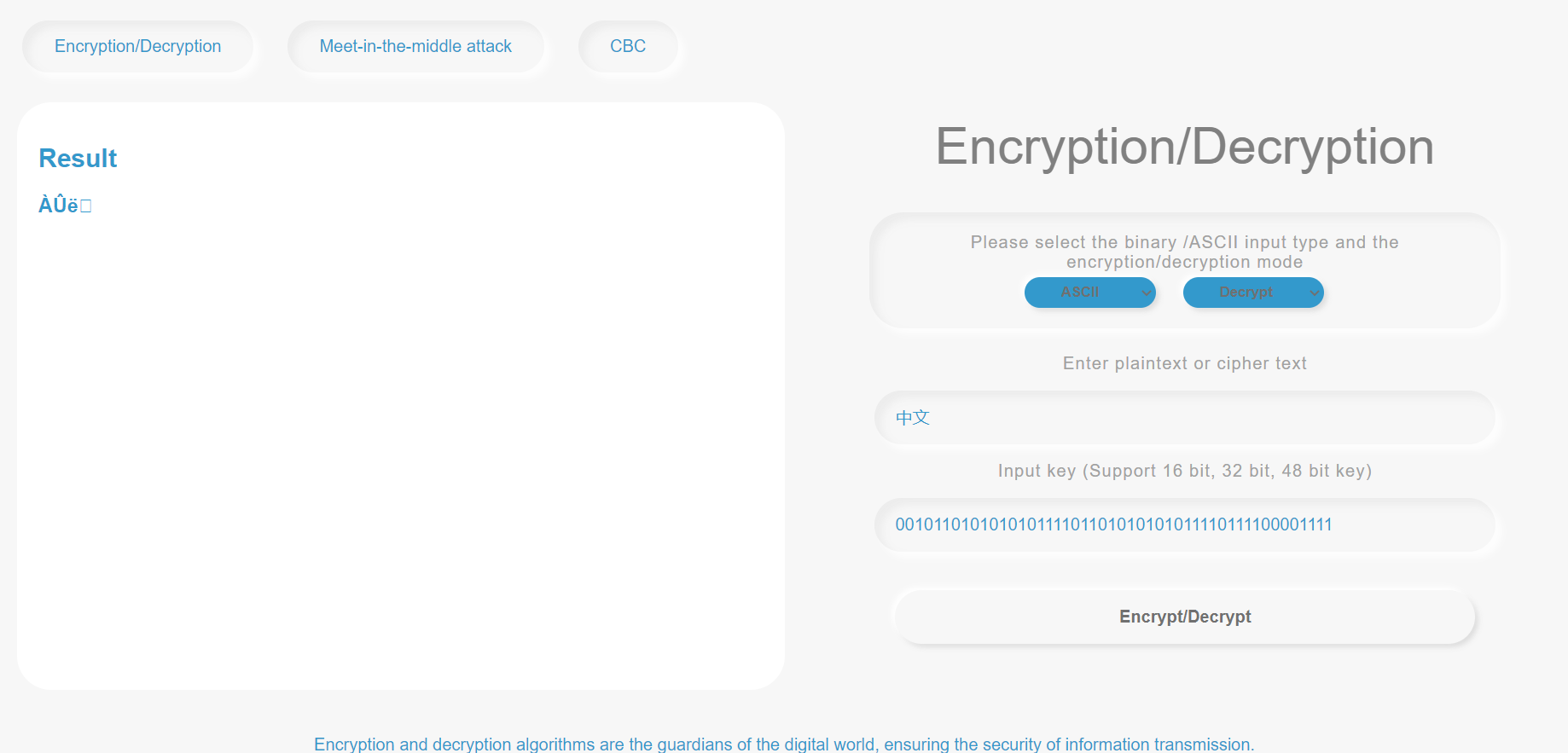


图4.3.5中文解密

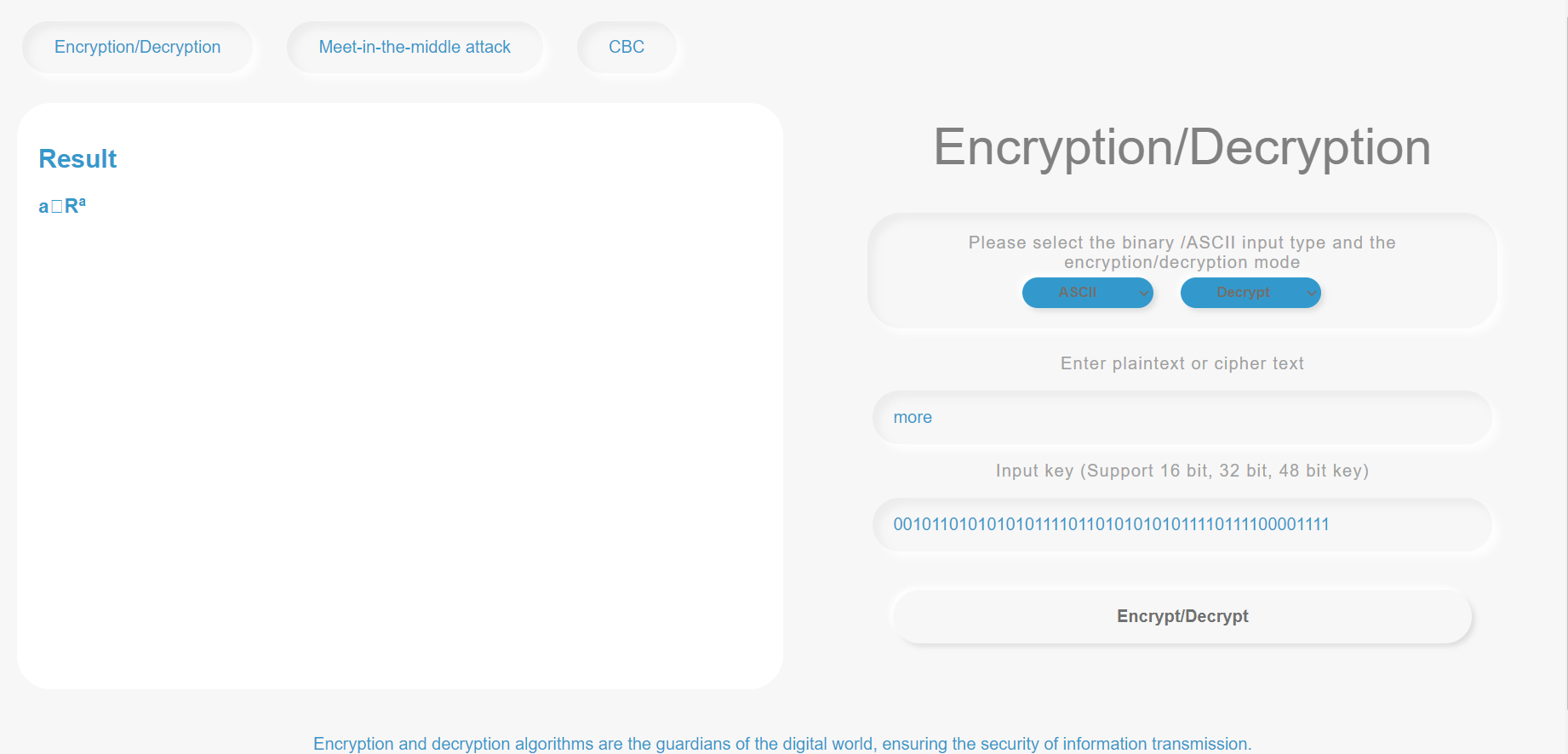


图4.3.6英文解密

**第5关：工作模式**

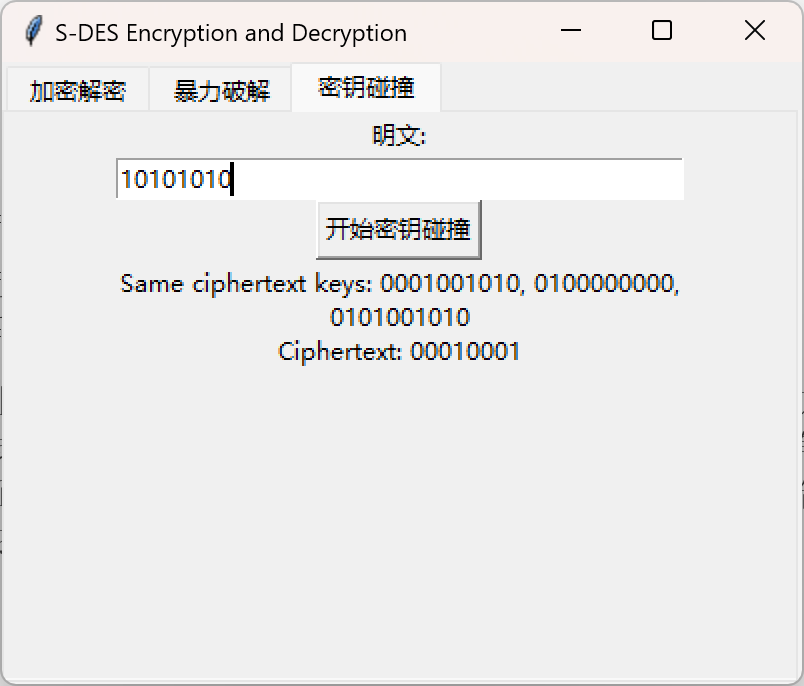
**测试目标：**基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。注意初始向量(16 bits) 的生成，并需要加解密双方共享。

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。

**测试结果：**经过封闭测试，S-DES算法程序中对应明文空间任意给定的明文分组P\_{n}，会出现选择不同的密钥，加密得到相同密文的情况。对于随机选择的一个明密文对，不止一个密钥。

测试步骤和结果：  
A：

|  |  |  |
| --- | --- | --- |
| **明文** | **不同密钥** | **相同密文** |
| 10101010 | 0001001010,0100000000,0101001010 | 00010001 |



B:

|  |  |
| --- | --- |
| **一组明密文** | **密钥** |
| 明文：00000000 密文：11111111 | 0001000100, 0101000100 |

