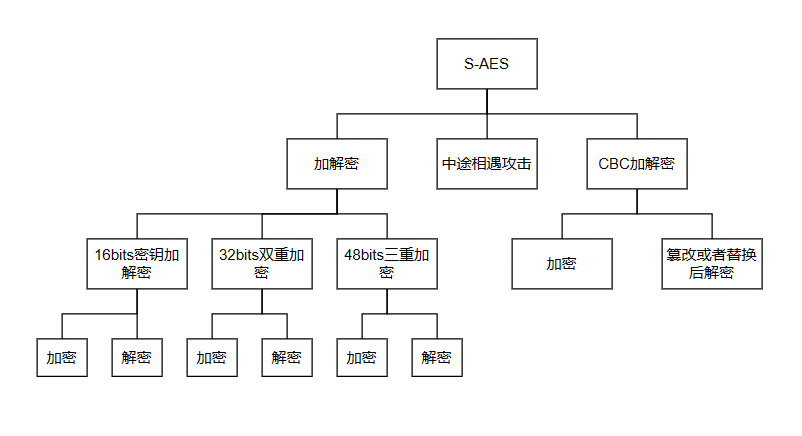
**开发手册**

1. **系统概述**

该系统是一个实现了Simplified Advanced Encryption Standard (S-AES) 算法的加密工具。它提供了一个用户界面，用户可以输入要加密或解密的数据，并选择加密或解密模式、输入类型等选项。它还提供CBC（Cipher Block Chaining）模式加密和解密功能，并包含了中间相遇攻击（meet-in-the-middle attack）算法来破解使用CBC模式加密的数据该程序由app.py，saes.py，cbc.py，middle\_meet\_attack.py四个文件组成。

1. **系统设计**

系统包括S-AES加密解密、中途相遇攻击、CBC模式加密解密模块，其中加密解密又包含二进制加解密、ASCII加解密两个模块，在S-AES加密解密时，根据输入的。



1. **系统生成**

app.py

saes.py

middle\_meet\_attack.py

cbc.py

key.cpython-310.pyc

cbc.cpython-310.pyc

middle\_meet\_attack.cpython-310.pyc

saes.cpython-310.pyc

1. **文件结构和组织方式**

• app.py：负责创建和管理前端用户界面。

• saes.py：实现了S-AES算法的加密和解密功能。

• middle\_meet\_attack.py：提供了中间相遇攻击算法的实现。

• cbc.py：提供了密码分组链模式加密解密算法的实现。

1. **接口文档**

**a. saes.py**

* + - encrypt(input\_data: str, key: str) -> str
* 功能：使用S-AES算法对输入数据进行加密。
* 参数：

input\_data：要加密的数据，可以是二进制或ASCII。

key：加密密钥，必须是16位二进制字符串。

* 返回值：加密后的数据，以二进制字符串形式返回。
  + - decrypt(input\_data: str, key: str) -> str
    - 功能：使用S-AES算法对输入数据进行解密。
    - 参数：

input\_data：要解密的数据，可以是二进制或ASCII。

key：解密密钥，必须是16位二进制字符串。

* + - 返回值：解密后的数据，以二进制字符串形式返回。
    - double\_encrypt(input\_data: str, key: str) -> str
* 功能：使用S-AES算法对输入数据进行加密。
* 参数：

input\_data：要加密的数据，可以是二进制或ASCII。

key：加密密钥，必须是32位二进制字符串。

* 返回值：加密后的数据，以二进制字符串形式返回。
  + - double\_decrypt(input\_data: str, key: str) -> str
    - 功能：使用S-AES算法对输入数据进行解密。
    - 参数：

input\_data：要解密的数据，可以是二进制或ASCII。

key：解密密钥，必须是32位二进制字符串。

* + - 返回值：解密后的数据，以二进制字符串形式返回。
    - triple\_encrypt(input\_data: str, key: str) -> str
* 功能：使用S-AES算法对输入数据进行加密。
* 参数：

input\_data：要加密的数据，可以是二进制或ASCII。

key：加密密钥，必须是48位二进制字符串。

* 返回值：加密后的数据，以二进制字符串形式返回。
  + - triple\_decrypt(input\_data: str, key: str) -> str
    - 功能：使用S-AES算法对输入数据进行解密。
    - 参数：

input\_data：要解密的数据，可以是二进制或ASCII。

key：解密密钥，必须是48位二进制字符串。

* + - 返回值：解密后的数据，以二进制字符串形式返回。

**b. middle\_meet\_attack.py**

* + - meet\_in\_the\_middle\_attack(pairs: List[str]) -> List[str]
      * 功能：使用中间相遇攻击算法破解已知明密文的可能密钥。
      * 参数：

pairs：已知的明文密文对的列表，每个明文或密文必须是16位二进制字符串。

* + - * 返回值：找到的密钥列表，以二进制字符串形式返回。

**c. cbc.py**

* + - cbc\_encrypt(input\_data: str, iv: str, key: str) -> str
* 功能：使用密码分组链CBC模式对输入数据进行加密。
* 参数：

input\_data：要加密的数据，可以是二进制或ASCII。

iv：初始向量，必须是16位二进制字符串。

key：加密密钥，必须是16位二进制字符串。

* 返回值：加密后的数据，以二进制字符串形式返回。
  + - cbc\_decrypt(input\_data: str, iv: str, key: str) -> str
    - 功能：使用密码分组链CBC模式对输入数据进行解密
    - 参数：

input\_data：要解密的数据，可以是二进制或ASCII。

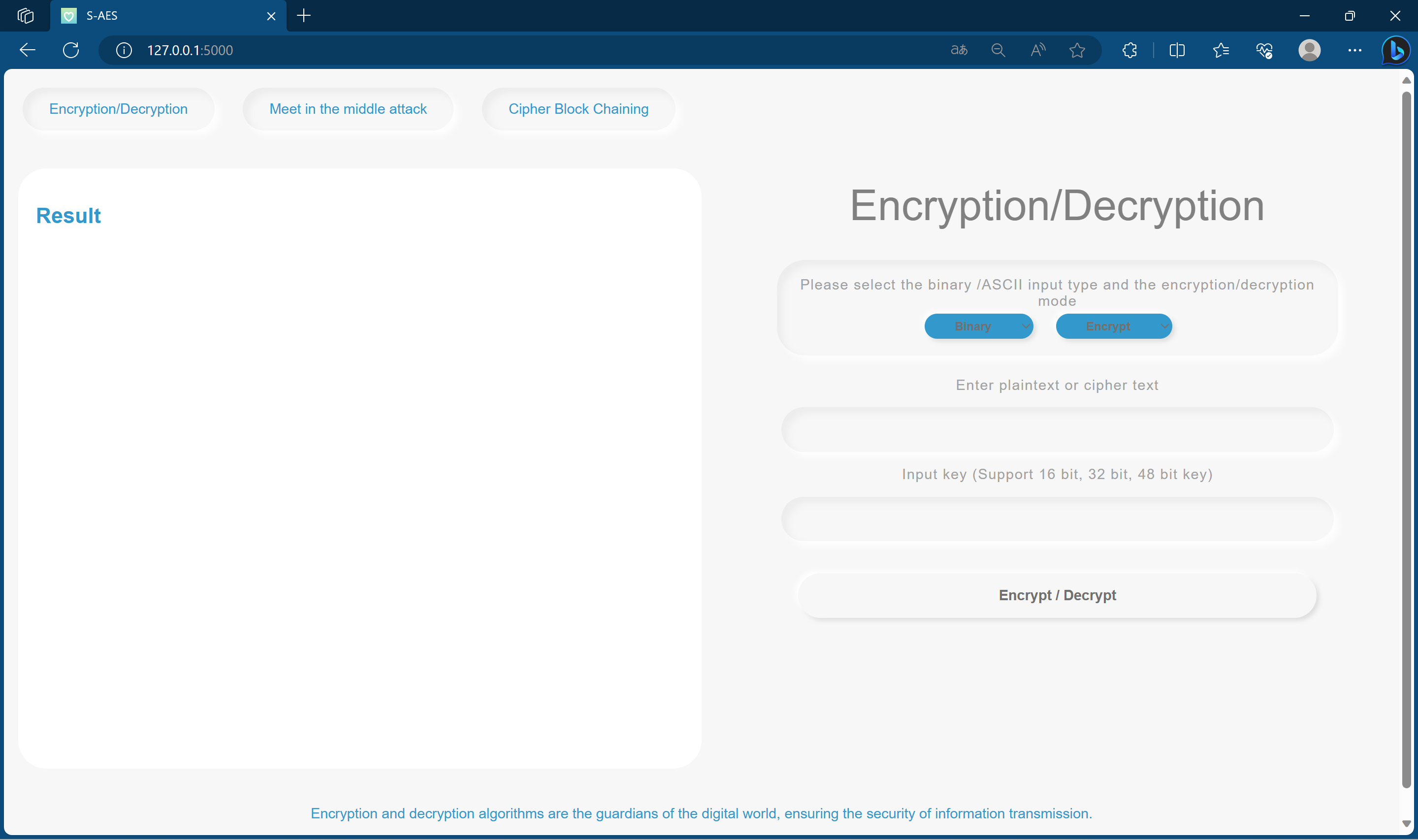
iv：初始向量，必须是16位二进制字符串。

key：解密密钥，必须是16位二进制字符串。

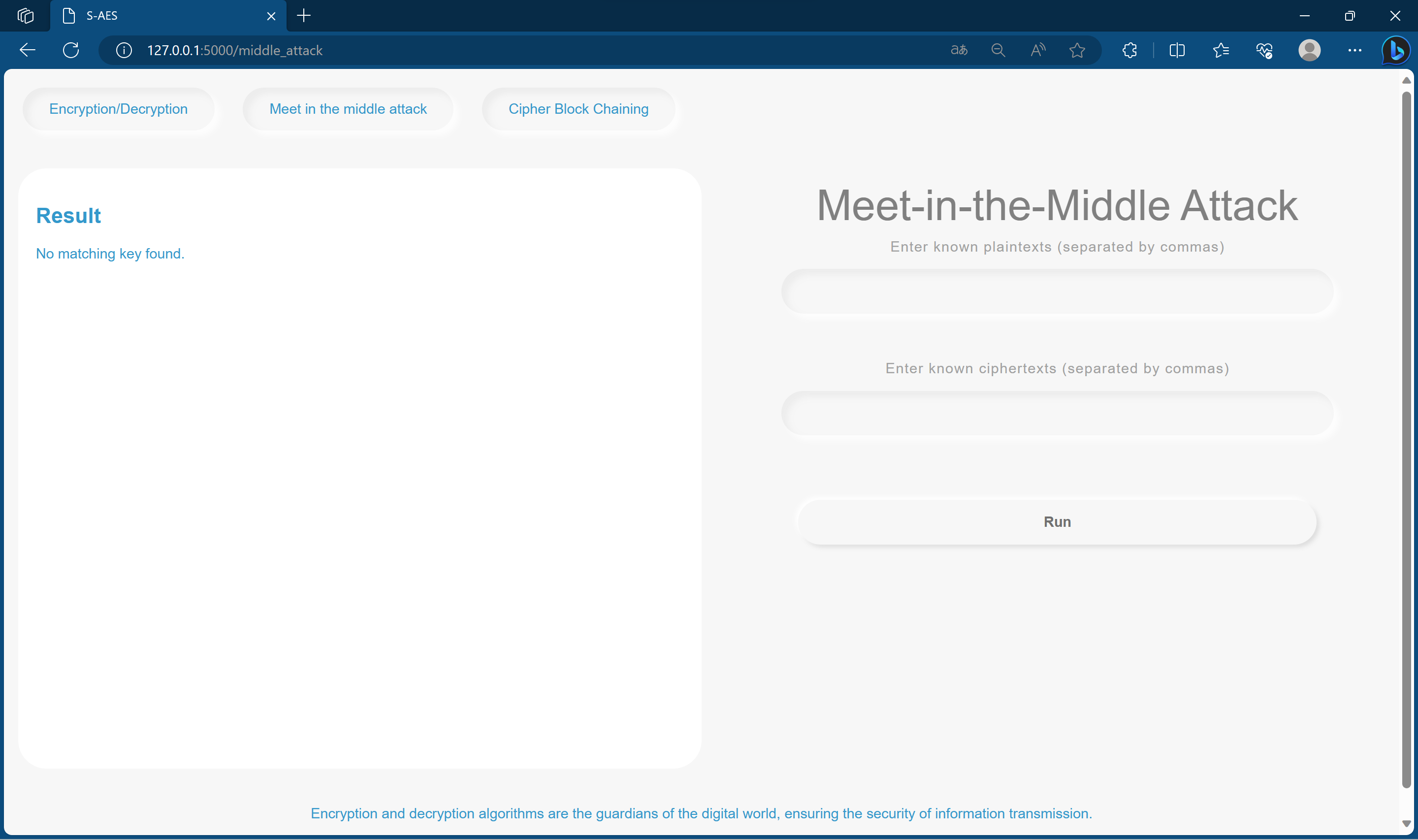
* + - 返回值：解密后的数据，以二进制字符串形式返回。

1. **系统验收**

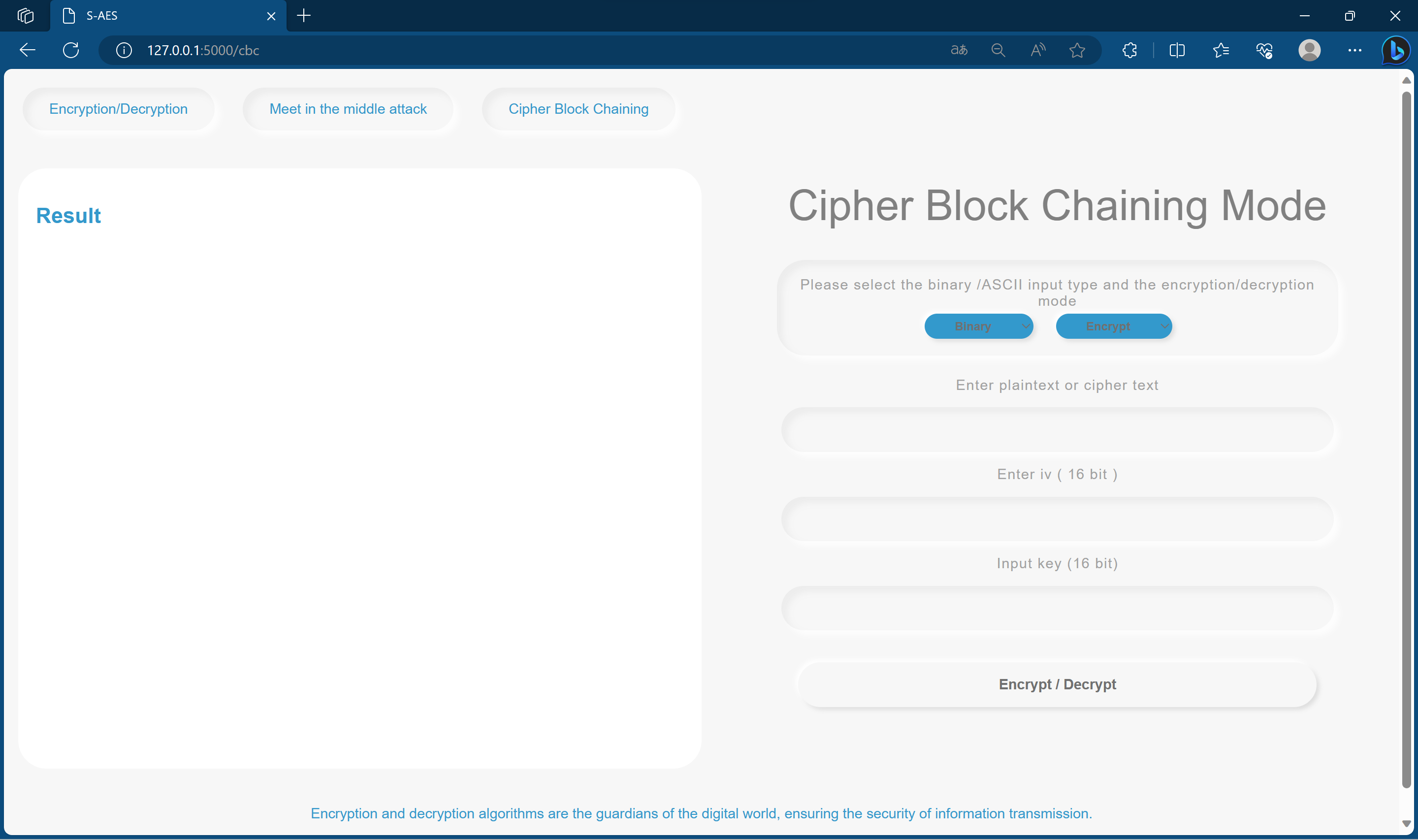
加密解密模块（含双重加密、三重加密）：

****

中间相遇攻击模块：

****

密码分组链(CBC)模块：

****