

用户指南

1. 介绍

1.1 什么是 S-AES 加密算法？

S-AES (Simplified Advanced Encryption Standard) 是一种轻量级的对称加密算法，它是对 AES (Advanced Encryption Standard) 算法的简化版本。S-AES 专门设计用于小规模数据的加密，通常处理 16 位的数据块。与 AES 相比，S-AES 的密钥长度更短，轮数更少，因此适用于资源受限的环境。S-AES 通常用于教育、学术和基础加密概念的演示。

1.2 S-AES 的关键特点

- (1) 密钥长度：S-AES 使用 16 位密钥来进行加密和解密。这是相对较短的密钥，可能不够安全用于高度敏感的数据。
- (2) 数据块大小：S-AES 处理 16 位数据块，其中包括 16 位明文和 16 位密文。这使得它适用于小规模数据的加密需求。
- (3) 两轮加密：S-AES 通常包括两轮加密，每轮使用不同的子密钥。
- (4) 轮密钥生成：S-AES 使用密钥排列算法生成两个轮密钥，这些轮密钥与明文进行轮密钥加操作，以增加加密的安全性。
- (5) 教育性质：S-AES 的安全性相对较低，主要用于教育和理解加密算法的基本概念。

1.3 用户指南概览

欢迎使用 S-AES 加密算法程序，此程序为 Advanced Encryption Standard (AES) 的一个简化版本，本用户指南旨在帮助教育和理解加密算法的基本原理，且由于 S-AES 的限制，该算法不适用于实际的安全应用。

1.4 用户界面

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

Enter Key:

Encrypt

Decrypt

Result:

2. S-AES 算法流程

2.1 S-AES 加密算法流程

- (1) 密钥扩展 (Key Expansion): 使用密钥排列算法, 将 16 位的主密钥扩展为两个轮密钥。
- (2) 初始轮 (Initial Round): 将明文块与主密钥进行 XOR 操作。
- (3) 第一轮
 - ① 半字节代替 (SubBytes): 将数据块中的每个字节分成两部分, 分别通过 S-盒替代, 然后合并。
 - ② 行位移 (ShiftRows): 对数据块的行进行循环位移操作, 以增加混淆度。
 - ③ 列混淆 (MixColumns): 对数据块的列进行混淆操作, 通过矩阵乘法进行。
 - ④ 轮密钥加 (AddRoundKey): 将数据块与第一个轮密钥进行 XOR 操作。
- (4) 第二轮:
 - ① 半字节代替 (SubBytes): 再次进行半字节代替操作。
 - ② 行位移 (ShiftRows): 再次进行行位移操作。
 - ③ 轮密钥加 (AddRoundKey): 将数据块与第二个轮密钥进行 XOR 操作。
- (5) 输出密文 (ciphertext): 最后的数据块即为密文, 长度为 16 位。

2.2 S-AES 解密算法流程

- (1) 初始轮 (Initial Round): 将明文块与第二个轮密钥进行 XOR 操作。
- (3) 第一轮
 - ① 逆行位移 (Inverse ShiftRows): 对数据块的行进行逆循环位移操作, 与加密时相反。
 - ② 逆半字节代替 (Inverse SubBytes): 将数据块中的每个字节分成两部分, 分别通过逆 S-盒替代, 然后合并。
 - ③ 轮密钥加 (AddRoundKey): 将数据块与第一个轮密钥进行 XOR 操作。
 - ④ 逆列混淆 (Inverse MixColumns): 对数据块的列进行逆混淆操作, 通过逆矩阵乘法进行。
- (4) 第二轮:
 - ① 逆行位移 (Inverse ShiftRows): 再次进行逆行位移操作, 与加密时相反。
 - ② 逆半字节代替 (Inverse SubBytes): 再次进行逆半字节代替操作。
 - ③ 轮密钥加 (AddRoundKey): 将数据块与主密钥进行 XOR 操作。
- (5) 输出明文 (plaintext): 最后的数据块即为明文, 长度为 16 位。

3. 使用说明

3.1 二进制加密

3.1.1 单重加密

- (1) 选择 Binary
- (2) 输入二进制明文, 长度为 16bit 位
- (3) 输入密钥, 长度为 16bit 位
- (4) 点击“Encrypt”
- (5) 在 Result 框中得到加密后的密文

示例：明文为 0110111101101011
密钥为 1010011100111011
输出密文为 0000011100111000

S-AES Encryption and Decryption

Binary ACSII

Double Encryption Triple Encryption

Enter Text:
0110111101101011

Enter Key:
1010011100111011

Encrypt Decrypt

Result:
密文为: 0000011100111000

3.1.2 双重加密

- (1) 选择 Double Encryption
- (2) 输入二进制明文，长度为 16bit 位
- (3) 输入密钥，长度为 32bit 位
- (4) 点击“Encrypt”
- (5) 在 Result 框中得到加密后的密文

示例：明文为 0100101001110100
密钥为 10100111001110111010011100111011
输出密文为 0110111101101011

S-AES Encryption and Decryption

Binary ACSII

Double Encryption Triple Encryption

Enter Text:
0100101001110100

Enter Key:
10100111001110111010011100111011

Encrypt Decrypt

Result:
密文为: 0110111101101011

3.1.3 三重加密

- (1) 选择 Triple Encryption
- (2) 输入二进制明文，长度为 16bit 位
- (3) 输入密钥，长度为 48bit 位
- (4) 点击“Encrypt”
- (5) 在 Result 框中得到加密后的密文

示例：明文为 0110111101101011

密钥为 101001110011101110100111001110111010011100111011

输出密文为 0011000011111011

The screenshot shows a web application titled "S-AES Encryption and Decryption". It features two radio buttons at the top: "Binary" (selected) and "ASCII". Below these are two buttons: "Double Encryption" and "Triple Encryption" (selected). The "Enter Text:" field contains the binary string "0110111101101011". The "Enter Key:" field contains the binary string "101001110011101110100111001110111010011100111011". There are "Encrypt" and "Decrypt" buttons. The "Result:" field displays the output: "密文为: 0011000011111011".

3.2 ASCII 字符串加密

- (1) 选择 ASCII
- (2) 输入 ASCII 字符串
- (3) 输入密钥，长度为 16bit 位
- (4) 点击“Encrypt”
- (5) 在 Result 框中得到加密后的密文

示例：明文为 ER

密钥为 1111000011110000

输出密文为 ?b

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

ER

Enter Key:

1111000011110000

Encrypt

Decrypt

Result:

密文为: %b

3.3 二进制解密

3.3.1 单重解密

- (1) 选择 Binary
- (2) 输入二进制密文，长度为 16bit 位
- (3) 输入密钥，长度为 16bit 位
- (4) 点击“Decrypt”
- (5) 在 Result 框中得到解密后的明文

示例：密文为 0000011100111000

密钥为 1010011100111011

输出明文为 0110111101101011

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

0000011100111000

Enter Key:

1010011100111011

Encrypt

Decrypt

Result:

明文为: 0110111101101011

3.3.2 双重解密

- (1) 选择 Double Encryption
- (2) 输入二进制密文，长度为 16bit 位
- (3) 输入密钥，长度为 32bit 位
- (4) 点击“Decrypt”
- (5) 在 Result 框中得到解密后的明文

示例：密文为 0110111101101011

密钥为 10100111001110111010011100111011

输出明文为 0100101001110100

The screenshot shows a web application titled "S-AES Encryption and Decryption". At the top, there are two tabs: "Binary" (selected) and "ASCII". Below the tabs are two buttons: "Double Encryption" (highlighted in blue) and "Triple Encryption" (grey). The "Enter Text:" section has a text input field containing "0110111101101011". The "Enter Key:" section has a text input field containing "10100111001110111010011100111011". Below these are two buttons: "Encrypt" and "Decrypt" (highlighted in blue). The "Result:" section shows a grey box with the text "明文为: 0100101001110100".

3.3.3 三重解密

- (1) 选择 Triple Encryption
- (2) 输入二进制密文，长度为 16bit 位
- (3) 输入密钥，长度为 48bit 位
- (4) 点击“Decrypt”
- (5) 在 Result 框中得到解密后的明文

示例：密文为 0011000011111011

密钥为 101001110011101110100111001110111010011100111011

输出明文为 0110111101101011

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

0011000011111011

Enter Key:

101001110011101110100111001110111010011100111011

Encrypt

Decrypt

Result:

明文为: 0110111101101011

3.4 ASCII 字符串解密

- (1) 选择 ASCII
- (2) 输入 ASCII 字符串
- (3) 输入密钥，长度为 16bit 位
- (4) 点击“Decrypt”
- (5) 在 Result 框中得到解密后的明文

示例：密文为 ?b

密钥为 1111000011110000

输出明文为 ER

S-AES Encryption and Decryption

Binary

ASCII

Double Encryption

Triple Encryption

Enter Text:

?b

Enter Key:

1111000011110000

Encrypt

Decrypt

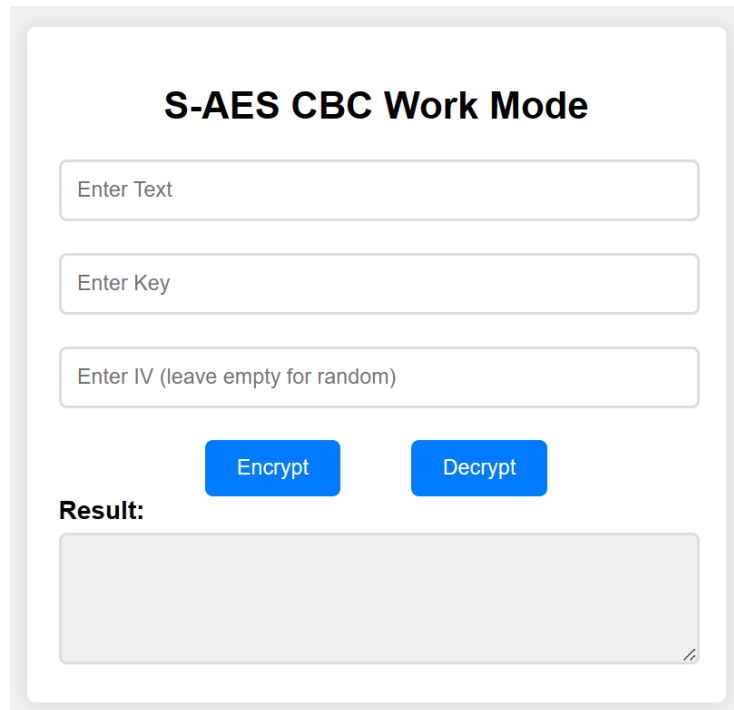
Result:

明文为: ER

3.5 工作模式

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。

界面



CBC 加密

- (1) 打开 S-AES CBC Work Mode 界面
- (2) 输入明文, 明文为任意长度
- (3) 输入密钥, 长度为 16bit 位
- (4) 点击“Encrypt”
- (5) 在 Result 框中得到加密后的密文和随机生成的初始向量 IV

示例: 明文为 10101010101010101111000011110000

密钥为 0000111100001111

输出密文为 01111100101110011001101001111001

随机生成的初始向量 (IV): 1100110100100010

S-AES CBC Work Mode

1010101010101010101111000011110000

0000111100001111

EncryptDecrypt

Result:

随机生成的初始向量 (IV): 1100110100100010
密文为: 01111100101110011001101001111001

CBC 解密

- (1) 打开 S-AES CBC Work Mode 界面
- (2) 输入密文
- (3) 输入密钥，长度为 16bit 位
- (4) 点击“Decrypt”
- (5) 在 Result 框中得到解密后的明文

示例：密文为 01111100101110011001101001111001
密钥为 0000111100001111
初始向量 IV 为 1100110100100010
输出明文为 1010101010101010101111000011110000

S-AES CBC Work Mode

01111100101110011001101001111001

0000111100001111

1100110100100010

EncryptDecrypt

Result:

明文为: 1010101010101010101111000011110000

3.6 操作提示

当明文为空时，提示“请输入明文！”

localhost:53122 显示
请输入明文!

确定

Binary ASCII

Double Encryption Triple Encryption

Enter Text:

Enter Key:

Encrypt Decrypt

Result:

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:

当选择 Binary、Double Encryption 或者 Triple Encryption 后，但输入的 text 不是二进制时，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:

4. 安全注意事项

用户在使用本服务时，请务必创建和定期更改强密码，不要与他人共享密码，启用多因素认证，只在安全连接下操作，小心使用公共 Wi-Fi，安装防病毒和反恶意软件，定期备份重要数据，警惕社交工程攻击，及时安装安全更新，保护个人敏感信息，避免不安全的实践，积极举报不当行为，尊重隐私，使用密码管理工具，并接受网络安全教育，以确保在线安全和隐私。

5. 参考资料

[1] Stallings, William. "Cryptography and Network Security: Principles and Practice." Prentice Hall, 2017.

[2] National Institute of Standards and Technology. (2001). FIPS PUB 197 - Advanced Encryption Standard (AES). NIST

[3] Paar, Christof, and Jan Pelzl. "Understanding Cryptography: A Textbook for Students and Practitioners." Springer, 2010.

6. 支持和反馈

如果您在使用程序时遇到问题或需要进一步帮助，请联系我们：leagueofcat@qq.com

7. 版本历史

版本 v1.0 (2023 年 10 月 28 日)，初始版本。