

S-AES 加密解密程序用户指南

1. 程序简介

S-AES 加密解密是一款基于 AES（高级加密标准）的简化版加密解密程序。AES 是一种广泛使用的对称加密算法，以其高效性、安全性和广泛的适用性而成为许多应用场景的首选加密算法。S-AES 作为 AES 的简化版本，主要特点是只使用 16 位的明文和 16 位的密钥进行加密，这使得它在资源受限的环境中或者对加密算法性能要求较高的场合更为适用。

2. 功能概述

(1) S-AES 加解密：使用 S-AES 算法根据输入的 4bit 十六进制密钥，对输入的 16bits 或 ASCII 类型的明文或密文进行加解密。

(2) 多重加解密：使用 S-AES 算法根据输入的 8bits 十六进制密钥，对输入的 16bits 的明文进行双重加密或密文进行双重解密；根据输入的 12bits 十六进制密钥，对输入的 16bits 的明文进行三重加密或密文进行三重解密；

(3) CBC 模式加解密：输入 4 位 16 进制密钥，16bits 初始向量以及一串长明文进行 CBC 加密。

3. 使用说明

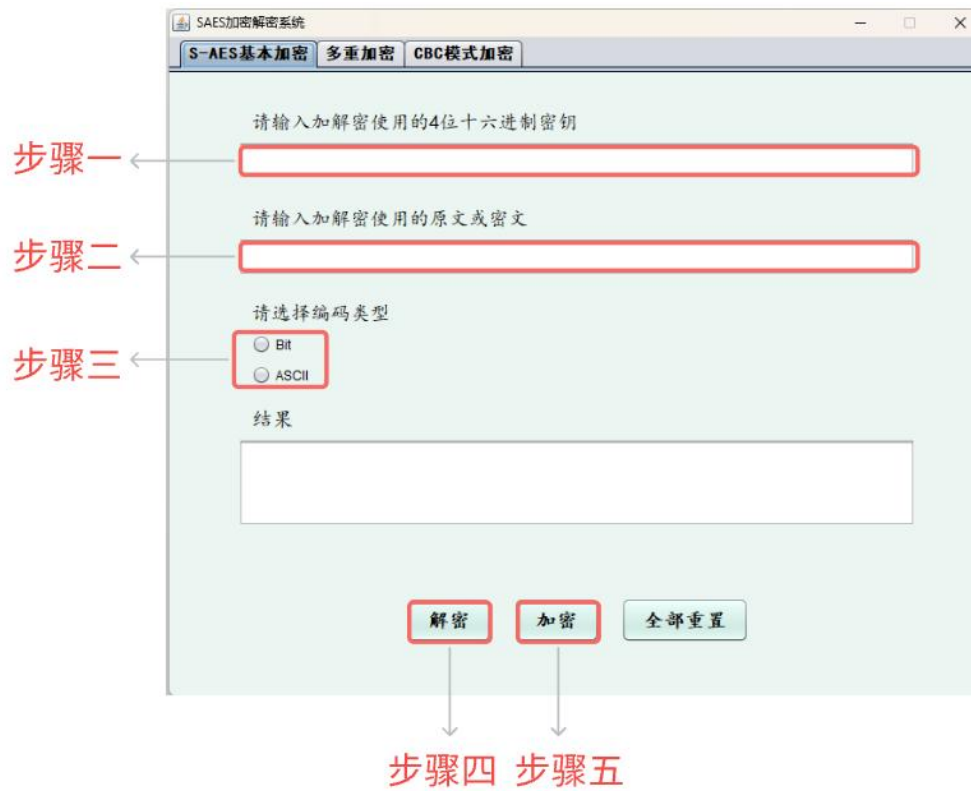


图 1 3.1S-AES 加解密流程



图 2 3.2 多重加解密流程



图 3 3.3CBC 模式加解密

3.1 S-AES 加解密流程

1. 加密：输入 4 位十六进制密钥以及 16bits 明文或偶数长度 String 类型的 ASCII 编码字符串，选择编码类型——Bit 或 ASCII，点击加密按钮，即可在结果的文本框里获得密文。



2. 解密：输入 4 位十六进制密钥以及 16bits 密文或偶数长度 String 类型的 ASCII 编码字符串，选择编码类型——Bit 或 ASCII，点击解密按钮，即可在结果的文本框里获得明文。



3.2 多重加解密流程

3.2.1 二重加解密

1. 加密：输入 8 位十六进制密钥以及 16bits 明文，选择二重加密，点击加密按钮，即可在结果的文本框里获得 16bits 密文。

SAES加密解密系统

S-AES基本加密 多重加密 CBC模式加密

若使用双重加密，请输入8位十六进制密钥
若使用三重加密，请输入16位十六进制密钥

29993777

请输入加解密使用的原文或密文

1011111100001010

请选择多重加密类型

☒ 双重加密
☐ 三重加密

结果

双重加密输出结果: 1010001000101111

解密 加密 全部重置

2. 解密：输入 8 位十六进制密钥以及 16bits 密文，选择二重加密，点击解密按钮，即可在结果的文本框里获得 16bits 明文。

SAES加密解密系统

S-AES基本加密 多重加密 CBC模式加密

若使用双重加密，请输入8位十六进制密钥
若使用三重加密，请输入16位十六进制密钥

29993777

请输入加解密使用的原文或密文

1011111100001010

请选择多重加密类型

☒ 双重加密
☐ 三重加密

结果

双重解密输出结果: 1100000101101100

解密 加密 全部重置

3.2.2 三重加解密

1. 加密：输入 12 位十六进制密钥以及 16bits 明文，选择三重加密，点击加密按钮，即可在结果的文本框里获得 16bits 密文。


The screenshot shows the 'SAES加密解密系统' window with the 'S-AES基本加密' tab selected. The interface includes instructions for key lengths: '若使用双重加密，请输入8位十六进制密钥' and '若使用三重加密，请输入16位十六进制密钥'. A text input field contains the key '299937774888DDDD'. Below it, another text input field contains the plaintext '1011111100001010'. The '请选择多重加密类型' (Please select multiple encryption type) section has two radio buttons: '双重加密' (Double encryption) and '三重加密' (Triple encryption), with '三重加密' selected. The '结果' (Result) section shows the output: '三重加密输出结果: 1011110010011000'. At the bottom, there are three buttons: '解密' (Decrypt), '加密' (Encrypt), and '全部重置' (Reset all).

3. 解密：输入 12 位十六进制密钥以及 16bits 密文，选择三重加密，点击解密按钮，即可在结果的文本框里获得 16bits 明文。

The screenshot shows the same 'SAES加密解密系统' window, but with the '解密' (Decrypt) button highlighted. The inputs remain the same: key '299937774888DDDD' and ciphertext '1011111100001010'. The '三重加密' (Triple encryption) option is still selected. The '结果' (Result) section now shows the output: '三重解密输出结果: 1001000111111111'. The '加密' (Encrypt) and '全部重置' (Reset all) buttons are also visible at the bottom.

3.3 CBC 模式加解密

1. 加密：选择 CBC 加密，输入 4 位十六进制密钥、16bits 初始向量，以及一串长明文，点击加密按钮，即可在结果文本框里获得密文。



The screenshot shows a web-based application titled "SAES加密解密系统". It has three tabs: "S-AES基本加密", "多重加密", and "CBC模式加密", with the last one being active. The interface contains several input fields and buttons:

- A label "请输入加解密使用的4位十六进制密钥" above an input field containing "5C12".
- A label "请输入加解密使用的64bits原文或密文" above an input field containing a long binary string: "1010111100001110101011110000111010101111000011101010111100001110".
- A label "请输入16bits初始向量" above an input field containing "1010111100001111".
- A label "结果" above a large output text area.
- At the bottom, three buttons: "解密" (Decipher), "加密" (Encrypt), and "全部重置" (Reset All).

The output text area displays the result: "CBC模式下加密输出结果:10000001011111111100101000101101110101001000100010101111011101111".

2. 解密：选择 CBC 解密，输入 4 位十六进制密钥以及 16bits 初始向量，以及一串长密文，点击解密按钮，即可在结果文本框里获得明文。

SAES加密解密系统

S-AES基本加密 多重加密 **CBC模式加密**

请输入加解密使用的4位十六进制密钥

5C12

请输入加解密使用的64bits原文或密文

1010111100001110101011110000111010101111000011101010111100001110

请输入16bits初始向量

1010111100001111

结果

CBC模式下解密输出结果:11101101100111111110110110011110110110011110110110110110011110

解密 加密 全部重置

4. 注意事项

4.1 若输入的密钥不满足要求，点击加解密按钮后会弹出错误提示的弹框，要求输入正确密钥。

4.2 当输入的原文或密文不符合要求时，点击加解密按钮会弹出错误提示的弹框，要求输入正确明文或密文。

4.3 数据规模：本程序仅适用于小规模的数据加密需求，不建议用于处理大量或敏感数据。

4.4 仅适用于一次一组输入进行加密或解密，不适用于多组同时进行。