**S-AES用户指南**

1. **系统操作**

打开界面可查看到加解密、中途相遇攻击、CBC三个模块；可以正常进行粘贴、复制等操作；如果系统使用完毕，可以使用右上方的“-”或者“×”进行最小化或退出。

1. **常用功能**
2. **加解密**
3. **普通加解密****（16 bits密钥）**

在“input”框中输入明文二进制（16 bits），输入Key（密钥），选择Binary类型和Encrypt/Decrypt类型，点击“Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

在“input”框中输入明文ASCII码、中文、英文，输入Key（密钥），选择ASCII类型和Encrypt/Decrypt类型，点击 “Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

1. **双重加密（32 bits密钥）**

在“input”框中输入明文二进制（16 bits），输入Key（密钥），选择Binary类型和Encrypt/Decrypt类型，点击“Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

在“input”框中输入明文ASCII码、中文、英文，输入Key（密钥），选择ASCII类型和Encrypt/Decrypt类型，点击 “Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

1. **三重加密（48 bits密钥）**

在“input”框中输入明文二进制（16 bits），输入Key（密钥），选择Binary类型和Encrypt/Decrypt类型，点击“Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

在“input”框中输入明文ASCII码、中文、英文，输入Key（密钥），选择ASCII类型和Encrypt/Decrypt类型，点击 “Encrypt/Decrypt”按钮，在左侧方形区域显示result（二进制 16 bits）。

1. **中途相遇攻击**

分别输入明文组和密文组，组内以英文逗号分隔，点击“Run”按钮，显示前五个结果和密钥数量。

1. **CBC加密**
2. **安全功能**

本系统的目的是为了对信息进行加密，从而确保信息安全；其中，中途相遇攻击与CBC加密模块是对算法的安全性进行测试与评估，双重加密与三重加密是对算法安全性进一步提高。