**用户指南**

**1.基础加解密**  
此功能用于对单组16位的二进制数据进行加密或解密。

1. 切换到[基本加解密]标签页。
2. 在“明/密文(16位二进制)”框中，输入16位数据。
3. 在“密钥(16位二进制)”框中，输入16位密钥。
4. 点击“加密”或“解密”按钮。
5. 结果将显示在下方的“输出结果”框中。

**2.ASCII加解密**

此功能用于对任意长度的文本字符串进行加密或解密。

1. 切换到[ASCII加解密]标签页。
2. 在“ASCII文本”框中，输入你想要处理的字符串。
3. 在“密钥(16位二进制)”框中，输入16位密钥。
4. 点击“加密ASCII”或“解密ASCII”按钮。
5. 结果将显示在“ASCII输出”框中（加密后可能为乱码）。

**3.双重加密与攻击**

**3.1双重加密与解密**

1. 切换到[双重加密]标签页。
2. 在“明/密文(16位)”框中，输入16位数据。
3. 在“密钥(32位二进制)”框中，输入32位密钥(K1+K2)。
4. 点击“双重加密”或“双重解密”按钮。

**3.2中间相遇攻击**

1. 在“中间相遇攻击”区域，输入“已知明文”和“已知密文”。
2. 点击“中间相遇攻击”按钮。
3. 程序将遍历所有可能，请耐心等待。
4. 所有找到的(K1,K2)密钥对将显示在“双重加密输出”框中。

**4.三重加密**

此功能使用48位密钥(K1+K2+K3)进行E-D-E模式的三重加密。

1. 切换到[三重加密]标签页。
2. 在“明/密文”框中，输入16位数据。
3. 在“密钥(48位二进制)”框中，输入48位密钥。
4. 点击“三重加密”或“三重解密”按钮。
5. 结果将显示在“三重加密输出”框中。

**5.CBC工作模式**

1. 切换到[CBC模式]标签页。
2. 在“长明/密文”框中，输入文本。
3. 在“密钥(16位二进制)”框中，输入16位密钥。
4. 在“初始向量IV(16位)”框中，输入16位IV。
5. 点击“CBC加密”或“CBC解密”执行操作。
6. 点击“篡改测试”按钮，将自动执行一次密文篡改并对比解密前后的结果，用于分析CBC的错误传播特性。